The p-Adic Numbers

Evan P. Dummit

Northeastern University

Northeastern Math Club

November 4th, 2022

Outline of Talk

I will start by motivating the p-adic numbers with some curious, and totally illegal, infinite sum calculations.

Then I will give the actual definition of the p-adic numbers, and illustrate various kinds of calculations with them.

Next, I will talk about some of the unusual and neat analytical and topological properties of the p-adic numbers.

Finally, time permitting, I will try to describe some uses of the p-adic numbers in number theory.

How To Sum Geometric Series, I

Consider the geometric series

$$S = 1 + \frac{1}{2} + \frac{1}{4} + \frac{1}{8} + \cdots .$$

- As we all presumably remember, this series converges and its sum is 2. To (re)determine this, just note that

  $$\frac{1}{2}S = \frac{1}{2} + \frac{1}{4} + \frac{1}{8} + \frac{1}{16} + \cdots$$

  and so subtracting and cancelling common terms yields

  $$S - \frac{1}{2}S = 1$$

  from which we see $S = 2$.

How To Sum Geometric Series, II

The same approach works for the more general geometric series

$$S = 1 + r + r^2 + r^3 + \cdots$$

Namely, just multiply it by r and then subtract from the original. Explicitly, we have

$$\begin{aligned} S &= 1 + r + r^2 + r^3 + r^4 + \cdots \\ rS &= \phantom{1 + {}} r + r^2 + r^3 + r^4 + \cdots \end{aligned}$$

and so subtracting and cancelling yields $S - rS = 1$ from which $S = 1/(1 - r)$.

How To Sum Geometric Series, III

Of course, these manipulations are only valid under the assumption that the original series

$$S = 1 + r + r^2 + r^3 + \cdots$$

converges[1].

- Since (as one may check) the geometric series S only converges when $|r| < 1$, the derivation of the formula $1 + r + r^2 + r^3 + \cdots = 1/(1 - r)$ is only valid for $|r| < 1$.
- In particular, it is completely illegal to do something like setting $r = 2$, or $r = 10$, in that formula.

[1] Actually, to do the cancellations without changing the value requires absolute convergence, but geometric series converge only when they converge absolutely, so it's fine.

How NOT To Sum Geometric Series, I

So let's set $r = 2$ in that formula: it yields

$$1 + 2 + 4 + 8 + 16 + \cdots = 1/(1 - 2) = -1.$$

[Pause here for the audience to express shock and horror.]

How NOT To Sum Geometric Series, I

So let's set $r = 2$ in that formula: it yields

$$1 + 2 + 4 + 8 + 16 + \cdots = 1/(1 - 2) = -1.$$

[Pause here for the audience to express shock and horror.]

- This is clearly nonsense for several reasons: first, the left-hand side is a sum of a bunch of positive integers (which goes to $+\infty$) while the right-hand side is negative!
- Completely ridiculous! There is absolutely no scenario in which this calculation could possibly be correct.

How NOT To Sum Geometric Series, I

So let's set $r = 2$ in that formula: it yields

$$1 + 2 + 4 + 8 + 16 + \cdots = 1/(1 - 2) = -1.$$

[Pause here for the audience to express shock and horror.]

- This is clearly nonsense for several reasons: first, the left-hand side is a sum of a bunch of positive integers (which goes to $+\infty$) while the right-hand side is negative!
- Completely ridiculous! There is absolutely no scenario in which this calculation could possibly be correct.
- Except... the whole point of this talk is to demonstrate how this calculation can be made meaningful and valid.

How NOT To Sum Geometric Series, II

To give some motivation, let's instead take $r = 10$: it yields

$$1 + 10 + 100 + 1000 + 10000 + \cdots = 1/(1 - 10) = -1/9.$$

[Pause here for audience to express slightly more shock and horror.]

How NOT To Sum Geometric Series, II

To give some motivation, let's instead take $r = 10$: it yields

$$1 + 10 + 100 + 1000 + 10000 + \cdots = 1/(1 - 10) = -1/9.$$

[Pause here for audience to express slightly more shock and horror.]

- This one is even worse than the one with $r = 2$, because now the right-hand side isn't even an integer.
- Somehow, that seems even less reasonable than the sum coming out to be negative. To fix that, let's multiply it by 9. That gives

$$9 + 90 + 900 + 9000 + 90000 + \cdots = -1.$$

How NOT To Sum Geometric Series, III

So let's see if we can make any sense out of

$$9 + 90 + 900 + 9000 + 90000 + \cdots = -1.$$

- Being as charitable as possible, try imagining that the sum on the left actually makes sense. If we just add up a few terms, we get numbers like 9, 99, 999, 9999, 99999, ...
- So the limit would then be a number whose base-10 expansion (all 9s) just keeps going, like this:

How NOT To Sum Geometric Series, III

So let's see if we can make any sense out of

$$9 + 90 + 900 + 9000 + 90000 + \cdots = -1.$$

- Being as charitable as possible, try imagining that the sum on the left actually makes sense. If we just add up a few terms, we get numbers like 9, 99, 999, 9999, 99999, ...
- So the limit would then be a number whose base-10 expansion (all 9s) just keeps going, like this:

$$\ldots 99999999999999999999999999999999999999999999999999999999999$$

- Now, the ludicrous claim is that this weird number equals -1. So let's try adding 1 to it.

How NOT To Sum Geometric Series, IV

Here we go, adding:

$$
\begin{array}{r}
\ldots 99999999999999999999999999999999999 \\
+ \qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad 1 \\
\hline
\end{array}
$$

How NOT To Sum Geometric Series, IV

Here we go, adding:

$$
\begin{array}{r}
1 \\
\ldots 999999999999999999999999999999 \\
+ \hspace{22em} 1 \\
\hline
0
\end{array}
$$

How NOT To Sum Geometric Series, IV

Here we go, adding:

$$
\begin{array}{r}
11 \\
\ldots 999999999999999999999999999999 \\
+ \qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad 1 \\
\hline
00
\end{array}
$$

How NOT To Sum Geometric Series, IV

Here we go, adding:

$$\begin{array}{r} {\scriptstyle 111} \\ \ldots 999999999999999999999999999999 \\ +1 \\ \hline 000 \end{array}$$

How NOT To Sum Geometric Series, IV

Let's jump ahead about ten steps:

$$
\begin{array}{r}
1111111111111 \\
\ldots 999999999999999999999999999999 \\
+ \qquad\qquad\qquad\qquad\qquad\qquad\qquad 1 \\
\hline
0000000000000
\end{array}
$$

How NOT To Sum Geometric Series, IV

The pattern is pretty clear, right? Just keep going forever:

$$\begin{array}{r} 11111111111111111111111111111 \\ \ldots 999999999999999999999999999999 \\ +\qquad\qquad\qquad\qquad\qquad\qquad 1 \\ \hline \ldots 000000000000000000000000000000 \end{array}$$

How NOT To Sum Geometric Series, V

So what does this tell us?

- It sure looks like if we add 1 to the number $\ldots 99999999999999$, we get the number $\ldots 00000000000000$.
- And if a string of a bunch of zeroes means anything, that last number is just 0.
- So to summarize, if we add 1 to $9 + 90 + 900 + 9000 + 90000 + \cdots$, we get 0.
- Thus subtracting 1 yields the conclusion $9 + 90 + 900 + 9000 + 90000 + \cdots = -1$, as claimed.

How NOT To Sum Geometric Series, V

So what does this tell us?

- It sure looks like if we add 1 to the number $\ldots 99999999999999$, we get the number $\ldots 00000000000000$.
- And if a string of a bunch of zeroes means anything, that last number is just 0.
- So to summarize, if we add 1 to $9 + 90 + 900 + 9000 + 90000 + \cdots$, we get 0.
- Thus subtracting 1 yields the conclusion $9 + 90 + 900 + 9000 + 90000 + \cdots = -1$, as claimed.

Mental exercise for you: redo this calculation but with base-2 expansions to "explain" why $1 + 2 + 4 + 8 + 16 + \cdots = -1$.

Towards the p-adics, I

In order to make calculations like the ones we just did meaningful, we need to describe a place in which the infinite sum $1 + 2 + 4 + 8 + 16 + \cdots$, actually converges in a meaningful way.

- Going with this idea, recall[2] that an infinite series can converge only if its terms eventually become small.
- So we are looking for a way to measure the "size" of an integer, in such a way that the powers of 2 become small in size as we take higher and higher powers of 2.
- Of course, we could just define an arbitrary "size" function on integers, but we want this size function to behave nicely.
- So, what conditions do we want?

[2] More formally, this is sometimes called the "nth term test for divergence": if the terms a_n do not have limit zero as $n \to \infty$, then the infinite sum $a_1 + a_2 + a_3 + \cdots$ cannot converge.

Towards the p-adics, II

We can take some cues from a size function that already exists: the usual absolute value $|n|$.

- Of course, this absolute value doesn't have the property that powers of 2 have small size, since $|2^n| = 2^n$ grows large as $n \to \infty$, rather than going to 0.
- But it does have lots of other nice properties. Here are some particularly good ones:
  (1) The absolute value is positive except at 0: $|a| \geq 0$ with equality only for $a = 0$.
  (2) The absolute value is multiplicative: $|ab| = |a||b|$ for any integers a and b.
  (3) The absolute value satisfies the triangle inequality: $|a + b| \leq |a| + |b|$ for any integers a and b.

Towards the p-adics, III

So, let's see if we can cook up an absolute-value-like function $|\cdot|_2$ on integers that has those same three properties

(1) $|a|_2 \geq 0$ with equality only for $a = 0$.

(2) $|ab|_2 = |a|_2|b|_2$ for any integers a and b.

(3) $|a + b|_2 \leq |a|_2 + |b|_2$ for any integers a and b.

and also has the property that $|2^n| \to 0$ as $n \to \infty$.

Towards the p-adics, III

So, let's see if we can cook up an absolute-value-like function $|\cdot|_2$ on integers that has those same three properties

(1) $|a|_2 \geq 0$ with equality only for $a = 0$.

(2) $|ab|_2 = |a|_2|b|_2$ for any integers a and b.

(3) $|a+b|_2 \leq |a|_2 + |b|_2$ for any integers a and b.

and also has the property that $|2^n| \to 0$ as $n \to \infty$.

- Since the absolute value is multiplicative, to make $|2^n|_2 \to 0$ as $n \to \infty$, we want to have $|2|_2 < 1$.
- So let's try, arbitrarily, taking $|2|_2 = 1/2$. Then $|2^n|_2$ would be $1/2^n$, which certainly goes to zero very fast.
- But what should we do with the other integers? By thinking about prime factorizations, it's enough to decide what to do with the other prime numbers.

Towards the p-adics, IV

Here's a really lazy idea: take $|p|_2 = 1$ for all of the other prime numbers aside from $p = 2$.

[Pause to allow audience to appreciate the laziness.]

Towards the p-adics, IV

Here's a really lazy idea: take $|p|_2 = 1$ for all of the other prime numbers aside from $p = 2$.

[Pause to allow audience to appreciate the laziness.]

- Using multiplicativity, if $n = 2^k q$ where q is odd, then we are defining $|n| = 1/2^k$, and also $|0|_2 = 0$. Certainly it has a simplicity to it, but does it satisfy our requirements?

(1) $|a|_2 \geq 0$ with equality only for $a = 0$.

(2) $|ab|_2 = |a|_2 |b|_2$ for any integers a and b.

(3) $|a + b|_2 \leq |a|_2 + |b|_2$ for any integers a and b.

- Certainly (1) and (2) are fine, but what about (3)? Let's try some examples to check.

Towards the p-adics, V

With our absolute value $|n| = 1/2^k$ for $n = 2^k q$ where q is odd, let's try out the triangle inequality $|a+b|_2 \leq |a|_2 + |b|_2$:

- $a = 1,\ b = 3$

Towards the p-adics, V

With our absolute value $|n| = 1/2^k$ for $n = 2^k q$ where q is odd, let's try out the triangle inequality $|a+b|_2 \leq |a|_2 + |b|_2$:

- $a = 1,\ b = 3$: then $|a+b| = 1/4$ and $|a| = 1,\ |b| = 1.$ ✓
- $a = 2,\ b = 7$

Towards the p-adics, V

With our absolute value $|n| = 1/2^k$ for $n = 2^k q$ where q is odd, let's try out the triangle inequality $|a+b|_2 \leq |a|_2 + |b|_2$:

- $a = 1,\ b = 3$: then $|a+b| = 1/4$ and $|a| = 1,\ |b| = 1.$ ✓
- $a = 2,\ b = 7$: then $|a+b| = 1$ and $|a| = 1/2,\ |b| = 1.$ ✓
- $a = 2,\ b = 4$

Towards the p-adics, V

With our absolute value $|n| = 1/2^k$ for $n = 2^k q$ where q is odd, let's try out the triangle inequality $|a+b|_2 \leq |a|_2 + |b|_2$:

- $a = 1$, $b = 3$: then $|a+b| = 1/4$ and $|a| = 1$, $|b| = 1$. ✓
- $a = 2$, $b = 7$: then $|a+b| = 1$ and $|a| = 1/2$, $|b| = 1$. ✓
- $a = 2$, $b = 4$: then $|a+b| = 1/2$ and $|a| = 1/2$, $|b| = 1/4$. ✓
- $a = 4$, $b = 4$

Towards the p-adics, V

With our absolute value $|n| = 1/2^k$ for $n = 2^k q$ where q is odd, let's try out the triangle inequality $|a+b|_2 \leq |a|_2 + |b|_2$:

- $a = 1$, $b = 3$: then $|a+b| = 1/4$ and $|a| = 1$, $|b| = 1$. ✓
- $a = 2$, $b = 7$: then $|a+b| = 1$ and $|a| = 1/2$, $|b| = 1$. ✓
- $a = 2$, $b = 4$: then $|a+b| = 1/2$ and $|a| = 1/2$, $|b| = 1/4$. ✓
- $a = 4$, $b = 4$: then $|a+b| = 1/8$ and $|a| = 1/4$, $|b| = 1/4$. ✓
- $a = 4$, $b = 12$

Towards the p-adics, V

With our absolute value $|n| = 1/2^k$ for $n = 2^k q$ where q is odd, let's try out the triangle inequality $|a+b|_2 \le |a|_2 + |b|_2$:

- $a = 1$, $b = 3$: then $|a+b| = 1/4$ and $|a| = 1$, $|b| = 1$. ✓
- $a = 2$, $b = 7$: then $|a+b| = 1$ and $|a| = 1/2$, $|b| = 1$. ✓
- $a = 2$, $b = 4$: then $|a+b| = 1/2$ and $|a| = 1/2$, $|b| = 1/4$. ✓
- $a = 4$, $b = 4$: then $|a+b| = 1/8$ and $|a| = 1/4$, $|b| = 1/4$. ✓
- $a = 4$, $b = 12$: then $|a+b| = 1/16$, $|a| = 1/4$, $|b| = 1/4$. ✓
- $a = 8$, $b = 8$

Towards the p-adics, V

With our absolute value $|n| = 1/2^k$ for $n = 2^k q$ where q is odd, let's try out the triangle inequality $|a + b|_2 \leq |a|_2 + |b|_2$:

- $a = 1,\ b = 3$: then $|a + b| = 1/4$ and $|a| = 1,\ |b| = 1$. ✓
- $a = 2,\ b = 7$: then $|a + b| = 1$ and $|a| = 1/2,\ |b| = 1$. ✓
- $a = 2,\ b = 4$: then $|a + b| = 1/2$ and $|a| = 1/2,\ |b| = 1/4$. ✓
- $a = 4,\ b = 4$: then $|a + b| = 1/8$ and $|a| = 1/4,\ |b| = 1/4$. ✓
- $a = 4,\ b = 12$: then $|a + b| = 1/16,\ |a| = 1/4,\ |b| = 1/4$. ✓
- $a = 8,\ b = 8$: then $|a + b| = 1/16,\ |a| = 1/8,\ |b| = 1/8$. ✓
- $a = 40,\ b = 80$

Towards the p-adics, V

With our absolute value $|n| = 1/2^k$ for $n = 2^k q$ where q is odd, let's try out the triangle inequality $|a+b|_2 \leq |a|_2 + |b|_2$:

- $a = 1$, $b = 3$: then $|a+b| = 1/4$ and $|a| = 1$, $|b| = 1$. ✓
- $a = 2$, $b = 7$: then $|a+b| = 1$ and $|a| = 1/2$, $|b| = 1$. ✓
- $a = 2$, $b = 4$: then $|a+b| = 1/2$ and $|a| = 1/2$, $|b| = 1/4$. ✓
- $a = 4$, $b = 4$: then $|a+b| = 1/8$ and $|a| = 1/4$, $|b| = 1/4$. ✓
- $a = 4$, $b = 12$: then $|a+b| = 1/16$, $|a| = 1/4$, $|b| = 1/4$. ✓
- $a = 8$, $b = 8$: then $|a+b| = 1/16$, $|a| = 1/8$, $|b| = 1/8$. ✓
- $a = 40$, $b = 80$: $|a+b| = 1/8$, $|a| = 1/8$, $|b| = 1/16$. ✓

It looks like it always works. In fact, an even stronger statement seems to hold: $|a+b|_2$ is always less than or equal to the maximum of $|a|_2$ and $|b|_2$.

Towards the p-adics, VI

Let's prove that:

Proposition

Suppose that $|n|_2 = 1/2^k$ *for* $n = 2^k q$ *where* q *is odd. Then for any integers* a *and* b *we have* $|a+b|_2 \leq \max(|a|_2, |b|_2)$.

Towards the p-adics, VI

Let's prove that:

Proposition

Suppose that $|n|_2 = 1/2^k$ for $n = 2^k q$ where q is odd. Then for any integers a and b we have $|a+b|_2 \leq \max(|a|_2, |b|_2)$.

Proof:

- If $a = 0$ or $b = 0$ the result is trivial.
- Now suppose $a = 2^{k_a} q_a$ and $b = 2^{k_b} q_b$ where q_a, q_b are odd. By swapping a, b if necessary, suppose $k_a \leq k_b$.
- Then $|a| = 2^{-k_a}$ and $|b| = 2^{-k_b}$ so $\max(|a|_2, |b|_2) = 2^{-k_a}$.
- Also $a + b = 2^{k_a}(q_a + 2^{k_b - k_a} q_b)$, so we see that the power of 2 dividing $a + b$ is at least 2^{k_a}. This means $|a + b|_2 \leq 2^{-k_a} = \max(|a|_2, |b|_2)$ as desired.

Towards the p-adics, VII

So what was the point of all this?

- The point was to show that we can define an alternate absolute value function on integers with the property that increasing powers of 2 have absolute values tending to 0 (in fact, tending to 0 exponentially).
- The plan now is to use this absolute value to make sense of this infinite series $1 + 2 + 4 + 8 + 16 + \cdots$.

Towards the p-adics, VIII

But before we do that, I want to observe that nothing here was specific to the prime 2.

- If we replace 2 with some other prime p (e.g., 3, or 5, or 2027) we can define a similar absolute value function: for $n = p^k q$ where q is not divisible by p, define $|n|_p = 1/p^k$.
- Then by the same argument, this absolute value function satisfies all three of our desired properties:
  (1) $|a|_p \geq 0$ with equality only for $a = 0$.
  (2) $|ab|_p = |a|_p |b|_p$ for any integers a and b.
  (3) $|a + b|_p \leq |a|_p + |b|_p$ for any integers a and b.
- This function $|n|_p$ is called the p-adic absolute value. In fact we have a stronger property:
  (3') $|a + b|_p \leq \max(|a|_p, |b|_p)$ for any integers a and b.

Towards the p-adics, IX

In fact, here's a much more interesting fact:

Theorem (Ostrowski's Theorem)

Suppose $|\cdot|$ is a nontrivial[3] *absolute value on the integers, meaning that*

(1) $|a| \geq 0$ *with equality only for* $a = 0$.

(2) $|ab| = |a||b|$ *for any integers* a *and* b.

(3) $|a+b| \leq |a| + |b|$ *for any integers* a *and* b.

Then $|\cdot|$ is a either a power of the usual absolute value or a power of the p-adic absolute value for some prime p.

So what this means is: up to normalizing, these are the only possible nontrivial[3] absolute value functions on $\mathbb{Z}$.

[3] The trivial absolute value is the one with $|0| = 0$ and $|n| = 1$ for all $n \neq 0$.

The p-adic Metric, I

So, now that we have the p-adic absolute value $|\cdot|_p$, we can use it to make sense of sequences.

- The idea is that we can use it to define a distance metric on integers by setting $d_p(a, b) = |a - b|_p$.

The p-adic Metric, I

So, now that we have the p-adic absolute value $|\cdot|_p$, we can use it to make sense of sequences.

- The idea is that we can use it to define a distance metric on integers by setting $d_p(a, b) = |a - b|_p$.
- This p-adic distance function makes $\mathbb{Z}$ into a metric space:
  1. First, $d_p(a, a) = |a - a|_p = 0$.
  2. Second, $d_p(a, b) = |a - b|_p = |b - a|_p = d_p(b, a)$ since $|-1|_p = 1$.
  3. Finally, $d_p(a, b) + d_p(b, c) = |a - b|_p + |b - c|_p \leq |(a - b) + (b - c)|_p = |a - c|_p = d_p(a, c)$ by applying the triangle inequality for the p-adic absolute value.

The main purpose of having this distance metric is to talk about convergent sequences.

The p-adic Metric, II

If $\{a_n\}_{n \geq 1}$ is a sequence in a metric space with distance function d, we say that the sequence converges to a limit L when $d(a_n, L) \to 0$ as $n \to \infty$.

- Inside $\mathbb{R}$ with the usual absolute value distance $d(a, b) = |a - b|$, this is just the usual notion of a convergent sequence of real numbers.

The p-adic Metric, II

If $\{a_n\}_{n\geq 1}$ is a sequence in a metric space with distance function d, we say that the sequence converges to a limit L when $d(a_n, L) \to 0$ as $n \to \infty$.

- Inside $\mathbb{R}$ with the usual absolute value distance $d(a, b) = |a - b|$, this is just the usual notion of a convergent sequence of real numbers.
- The exciting part is to work instead inside $\mathbb{Z}$ with the p-adic metric d_p.
- Here's a nontrivial example: under the 2-adic metric, the sequence with $a_n = 2^n$ converges to $L = 0$ as $n \to \infty$, since $d_2(a_n, 0) = |2^n - 0|_2 = 1/2^n$ tends to 0 as n grows.
- This is encouraging, since the whole point was to find a place where higher powers of 2 become smaller and smaller.

The p-adic Metric, III

Our original interest was in trying to understand the sum $1 + 2 + 4 + 8 + 16 + \cdots$, which our illegal use of the geometric series formula told us was equal to -1.

- Let's see what happens with the 2-adic metric.
- If we take the nth partial sum $a_n = 1 + 2 + 4 + 8 + \cdots + 2^{n-1}$ of this sequence, then we can just check the formula $a_n = 2^n - 1$ (e.g., by induction).
- Therefore, under the 2-adic metric d_2, we have $d_2(a_n, -1) = |a_n + 1|_2 = |(2^n - 1) + 1|_n = |2^n|_n = 1/2^n$.
- Hence under the 2-adic metric, the sequence of partial sums converges to -1!

The p-adic Metric, IV

So, if we (very reasonably) define the expression $1 + 2 + 4 + 8 + 16 + \cdots$ to be the limit of its partial sums, then under the 2-adic metric, the statement $1 + 2 + 4 + 8 + 16 + \cdots = -1$ is now completely, 100% correct!

[Pause to allow the audience to feel the amazement of this fact.]

The p-adic Metric, IV

So, if we (very reasonably) define the expression $1 + 2 + 4 + 8 + 16 + \cdots$ to be the limit of its partial sums, then under the 2-adic metric, the statement $1 + 2 + 4 + 8 + 16 + \cdots = -1$ is now completely, 100% correct!

[Pause to allow the audience to feel the amazement of this fact.]

- We can do a similar calculation to see that $9 + 90 + 900 + 9000 + \cdots$ also converges 2-adically to -1.
- Explicitly, for $a_n = 9 + 90 + \cdots + 9 \cdot 10^{n-1} = 10^n - 1$ we see $d_2(a_n, -1) = |a_n + 1|_2 = |10^n|_2 = 1/2^n \to 0$ as $n \to \infty$.
- Hence under the 2-adic metric, we have $9 + 90 + 900 + 9000 + \cdots = -1$.
- In fact, this statement is also true under the 5-adic metric, since $|10^n|_5 = 1/5^n$ also tends to zero.

The *p*-adic Metric, V

So, we see that under the 2-adic metric, we have $9 + 90 + 900 + 9000 + \cdots = -1$.

- But the original sum we were after was $1 + 10 + 100 + 1000 + \cdots$, which was supposed to equal $-1/9$.
- Obviously, we cannot make a valid statement like that inside the integers, since $-1/9$ is not an integer.
- The question still remains, however: does the sum $1 + 10 + 100 + 1000 + \cdots$ converge under the 2-adic metric?
- The direct answer is: it cannot converge to an integer (since if it did, multiplying that integer by 9 would yield -1, but there is no such integer).
- But what if we take a different notion of convergence?

The p-adic Metric, VI

Another way to decide if a sequence of real numbers converges is to test whether it is a Cauchy sequence.

- A sequence $\{a_n\}_{n\geq 1}$ is Cauchy if for any $\epsilon > 0$ there exists N such that $d(a_m, a_n) < \epsilon$ whenever $m, n \geq N$.
- Intuitively, the terms in a Cauchy sequence all get (and stay) arbitrarily close as we go far out in the sequence.
- Cauchy sequences are used in constructing the real numbers starting from the rational numbers, since every real number is the limit of a Cauchy sequence of rational numbers.
- More precisely, if we define two Cauchy sequences $\{a_n\}$ and $\{b_n\}$ to be equivalent if $d(a_n, b_n) \to 0$ as $n \to \infty$, then the real numbers are obtained as the equivalence classes of Cauchy sequences of rational numbers under the usual distance.

The p-adic Integers, I

We can perform an analogous completion procedure on the integers under the p-adic metric to obtain a place where all of our Cauchy sequences actually converge.

Definition

The p-adic integers, denoted $\mathbb{Z}_p$, consist of all equivalence classes of Cauchy sequences of integers under the p-adic metric.

- This is a fairly opaque definition since it relies on Cauchy sequences.
- Fortunately, there is a much more concrete description of the elements of $\mathbb{Z}_p$, and in fact, the elements look just like the kinds of sums we have been considering.

The p-adic Integers, II

Explicitly, the elements of $\mathbb{Z}_p$ are all uniquely given as "infinite base-p expansions", of the form $a_0 + a_1 p + a_2 p^2 + a_3 p^3 + a_4 p^4 + \cdots$, where each a_i has $0 \leq a_i \leq p-1$.

- In base p, we would write such a number as $\ldots a_4 a_3 a_2 a_1 a_0$.
- It is not hard to see that the partial sums of any such expansion are a Cauchy sequence under the p-adic metric (since for $m > n$, the difference between the mth and nth has all terms with at least p^n in them).
- It is a bit more work to show that every Cauchy sequence is equivalent to one of these, and that all of these sequences are inequivalent. (But it's true.)

The p-adic Integers, III

What is even nicer is that we can add, subtract, and multiply p-adic integers as well.

- Intuitively, they behave like power series in p, but with carrying: we just add, subtract, or multiply as appropriate, keeping track of carries as we go.
- If we want to write down the terms up to p^n, we can just do the calculations with the terms up to p^n.
- For example, with $p = 5$, if we want to add $1 + p + p^2 + p^3 + p^4 + \cdots$ to $1 + 4p + 2p^2 + 0p^3 + 0p^4 + \cdots$, we just add term-by-term to get $1 + 5p + 3p^2 + p^3 + p^4 + \cdots$ and then resolve the carry in the p-coefficient to get $1 + 0p + 4p^2 + p^3 + p^4 + \cdots$.
- Multiplication is similar: just use the distributive law and then resolve all of the carries at the end.

The p-adic Integers, IV

Multiplication is similar: just use the distributive law and then resolve all of the carries at the end.

- For example, with $p = 5$, if we want to multiply $1 + 2p + 3p^2 + \cdots$ with $1 + 4p + 2p^2 + \cdots$, we distribute, collect terms, and then resolve carries to get

$$\begin{aligned}
&(1 + 2p + 3p^2 + \cdots)(1 + 4p + 2p^2 + \cdots) \\
&= 1(1 + 4p + 2p^2 + \cdots) + 2p(1 + 4p + 2p^2 + \cdots) + 3p^2(1 + 4p + 2p^2 + \cdot\cdot \\
&= (1 + 4p + 2p^2 + \cdots) + (2p + 8p^2 + 4p^3 + \cdots) + (3p^2 + 12p^3 + 6p^4 + \cdot\cdot \\
&= 1 + 6p + 13p^2 + \cdots \\
&= 1 + p + 4p^2 + \cdots
\end{aligned}$$

The p-adic Integers, V

In many situations, we can even find multiplicative inverses of elements of $\mathbb{Z}_p$, which in turn allows us to do division.

- For example, in $\mathbb{Z}_p$ we have the product
$(1-p)(1+p+p^2+p^3+p^4+\cdots)$
$= (1+p+p^2+p^3+\cdots) + (-p)(1+p+p^2+p^3+\cdots)$
$= (1+p+p^2+p^3+\cdots) + (-p-p^2-p^3\cdots) = 1.$
- That means $1-p$ has a multiplicative inverse in $\mathbb{Z}_p$, namely, $1+p+p^2+p^3+p^4+\cdots$.
- Or, written differently: $1/(1-p) = 1+p+p^2+p^3+p^4+\cdots$. Precisely our geometric series formula!

More generally, an element $a_0 + a_1p + a_2p^2 + a_3p^3 + a_4p^4 + \cdots$ will have a multiplicative inverse precisely when $a_0 \neq 0$.

Solving Equations Mod p^n, I

Historically, the motivation for constructing and studying the p-adic integers came from studying solutions to polynomial equations modulo primes and prime powers.

- A natural way to try to solve a polynomial equation modulo a prime power p^n is first to solve it mod p, then solve it mod p^2, then solve it mod p^3, and so forth.
- The reason this is a good idea is that any solution mod p^2 must reduce to one of the solutions found mod p, so one can just test the solutions mod p plus multiples of p to get the solutions mod p^2.
- The same idea works to solve the equation mod p^3 given the solutions mod p^2: a solution mod p^3 must reduce to one mod p^2, so just test the solutions mod p^2 plus multiples of p^2.

Solving Equations Mod p^n, II

To illustrate, let's solve the very simple equation $x + 1 = 0$ modulo powers of 2.

- First, solve it mod 2^1: obviously we have one solution $x \equiv 1 \pmod{2}$.

Solving Equations Mod p^n, II

To illustrate, let's solve the very simple equation $x + 1 = 0$ modulo powers of 2.

- First, solve it mod 2^1: obviously we have one solution $x \equiv 1 \pmod{2}$.
- Next, solve it mod 2^2. It reduces to the solution above mod 2, so it is of the form $x \equiv 1 + 2a \pmod{4}$ for some $a = 0, 1$. Testing possible a gives only $a = 1$, so that $x = 1 + 2 \pmod{4}$.

Solving Equations Mod p^n, II

To illustrate, let's solve the very simple equation $x + 1 = 0$ modulo powers of 2.

- First, solve it mod 2^1: obviously we have one solution $x \equiv 1 \pmod{2}$.
- Next, solve it mod 2^2. It reduces to the solution above mod 2, so it is of the form $x \equiv 1 + 2a \pmod{4}$ for some $a = 0, 1$. Testing possible a gives only $a = 1$, so that $x = 1+2 \pmod{4}$.
- Next, solve it mod 2^3. It reduces to the solution above mod 4, so it is of the form $x \equiv 1 + 2 + 4a \pmod{4}$ for some $a = 0, 1$. Testing possible a gives only $a = 1$, so that $x = 1 + 2 + 4 \pmod{8}$.

Solving Equations Mod p^n, II

To illustrate, let's solve the very simple equation $x + 1 = 0$ modulo powers of 2.

- First, solve it mod 2^1: obviously we have one solution $x \equiv 1 \pmod{2}$.
- Next, solve it mod 2^2. It reduces to the solution above mod 2, so it is of the form $x \equiv 1 + 2a \pmod{4}$ for some $a = 0, 1$. Testing possible a gives only $a = 1$, so that $x = 1 + 2 \pmod{4}$.
- Next, solve it mod 2^3. It reduces to the solution above mod 4, so it is of the form $x \equiv 1 + 2 + 4a \pmod{4}$ for some $a = 0, 1$. Testing possible a gives only $a = 1$, so that $x = 1 + 2 + 4 \pmod{8}$.
- Repeating this process yields a unique solution each time, namely $x = 1 + 2 + 4 + 8 + \cdots + 2^{n-1} \pmod{2^n}$.
- Of course, this is just -1 mod 2^n, the actual integer solution of the equation.

Solving Equations Mod p^n, III

The 2-adic equality $1 + 2 + 4 + 8 + \cdots = -1$ encapsulates all of these calculations at once, and reflects that the original equation $x + 1 = 0$ actually has an integer solution $x = -1$.

- This lifting procedure works for most polynomial equation too, as first shown explicitly by Hensel:

Theorem (Hensel's Lemma)

Suppose $q(x)$ is a polynomial with integer coefficients. If $q(a) \equiv 0$ (mod p^d) and $q'(a) \not\equiv 0$ (mod p), then there is a unique k modulo p such that $q(a + kp^d) \equiv 0$ (mod p^{d+1}. Explicitly, this value is $k = -\dfrac{1}{q'(a)} \cdot \dfrac{q(a)}{p^d}$.

This result says if $x = a$ is a root of $q(x)$ mod p, and $q'(a) \neq 0$ (mod p), then it lifts to a unique root of the polynomial mod p^2, mod p^3, mod p^4, ...: and in fact, in $\mathbb{Z}_p$.

Solving Equations Mod p^n, IV

Although the expression in Hensel's lemma may look very unpleasant, the iteration procedure is actually quite nice.

- From the description, the new root $a' = a + kp^d$ is given by $a' = a - \dfrac{q(a)}{q'(a)}$, and this is precisely the same as the iteration procedure used in Newton's method for finding a zero of a differentiable function $q(x)$.
- What this means is: this procedure is really just applying Newton's method inside the p-adic integers to compute a root of the polynomial $q(x)$.

Some Other Facts About $\mathbb{Z}_p$

There is so very much more to say about the p-adic numbers, but since I don't want to take way too much time, let me just say a few of the really neat facts:

- $\mathbb{Z}_p$ has very interesting topological properties. For example, $\mathbb{Z}_p$ is compact, locally compact, and totally disconnected.
- The only closed subgroups of $\mathbb{Z}_p$ are the sets $p^n\mathbb{Z}_p$, which has finite index p^n. As a consequence, every closed subgroup of $\mathbb{Z}_p$ is open.
- An infinite series of p-adic integers converges if and only if the terms have norms tending to zero.
- A function defined by a power series $f(x) = \sum_{n=0}^{\infty} a_n x^n$ will converge for all $x \in \mathbb{Z}_p$ with $|x|_p < r$ for an appropriate radius of convergence r determined by the p-adic valuations of the coefficients. In particular, if the coefficients are integers, then the series converges for all $|x|_p < 1$.

A Mind-Bending Calculation

By manipulating the series appropriately, one can show that the usual binomial expansion for the square root function $\sqrt{1+x} = \sum_{n=0}^{\infty} \frac{(1/2)(1/2-1)(1/2-2)(1/2-n+1)}{n!} x^n$, when squared, actually produces the value $1 + x$ in $\mathbb{Z}_p$ as long as $|x|_p < 1$.

- Setting $x = 7/9$, which has $|x| < 1$ and $|x|_7 < 1$, gives $\sum_{n=0}^{\infty} \frac{(1/2)(1/2-1)\cdots(1/2-n+1)}{n!}(7/9)^n = 1 + \frac{1}{2} \cdot \frac{7}{9} - \frac{1}{4}(\frac{7}{9})^2 + \cdots$.
- Over the real numbers, this sum converges to the value $\sqrt{16/9} = 4/3$.
- However, 7-adically, this sum is congruent to 1 modulo 7 (since all of the terms after the "1" have a factor of 7 in them). But $x = 4/3$ is congruent to -1 modulo 7 (since $1/3 \equiv -2 \pmod 7$), and so in fact the 7-adic series converges to $-4/3$.
- So: the exact same series converges to different roots of the polynomial $x^2 - 16/9$ over the real numbers and in $\mathbb{Z}_7$!

Thanks!

Thanks to Sam Lowe and the other math club organizers for providing me the opportunity to speak here today!

I hope you enjoyed my talk, and I'd like to thank you for attending! Enjoy your weekend!