p-adics and Their Problematic Antics

Get it?

Who? Fahad Hossaini

When? April 16, 2024

p-adics...

Who here knows anything about p-adics?

p-adic integers vs p-adic numbers

Just a formal note at the beginning.

We'll be talking about p-adic integers, not p-adic numbers for simplicity's sake. While the difference is minor, you can safely ignore this slide if what I said doesn't make sense.

As always, you can always ask questions, but for more complicated topics, keep it until the end of the talk!

A Simple Premise

There's many ways to introduce p-adics. Here's one way:

What if the rightmost digits were more significant than the leftmost digits...

The Main Idea

Consider the number 495. Clearly, the most 'significant' digit is the leftmost digit, 4.

But what if we decide to make the most 'significant' digit the rightmost digit, 5?

How does this change anything, and how do we formalize this?

Notation

The p in p-adic refers to a number. At our current level, this means what base we are working with.

For example, a 5-adic number is a base 5 number.

The number $69 = 2 \cdot 5^2 + 3 \cdot 5 + 4$
Thus, $69 = 234$ in base 5. We'll denote this as 234_5.

$123 = 443_5 = 11120_3 = 30_{41} = 234_7$

Base p

We formally state a base p number here:

Let p be given. Then, the base p representation of a number is:

$$a_0 + a_1 \cdot p + a_2 \cdot p^2 + \cdots + a_n p^n \text{ where } 0 \leq a_i < p$$

Or:

$$\sum_{i=0}^{n} a_i p^n \text{ where } 0 \leq a_i < p$$

Note that this is the reverse direction in which we read numbers. So $1 + 2 \cdot 4 + 3 \cdot 4^2 = 321_4$.

Another (not-so easy but still relatively easy) Example

Consider 2 in the 5-adics. We can write this out as:

$$2_5 = \ldots 00002_5$$

The reason is because like decimals, the number extends infinitely offwards to the left, but we cut it short.

We let addition, subtraction and multiplication be as we expect them.

What is 2^{-1}? i.e. What x has the property that $2x = 1$? i.e. What x has the property that $x + 2 = 0$?

Before that, what is -2?

Another (not-so easy but still relatively easy) Example Continued Part 1

$-2_5 = \ldots 44443_5$.

Do you believe me? Let's add them and check!

Another (not-so easy but still relatively easy) Example Continued Part 1.5

$-2_5 = \ldots 44443_5$.

Do you believe me? Let's add them and check!

$$
\begin{aligned}
&\ldots 44443_5 \\
+&\ldots 00002_5 \\
=&\ldots 44445_5 \\
=&\ldots 44450_5 \\
=&\ldots 44500_5 \\
=&\ldots 45000_5 \\
=&\ldots 00000_5
\end{aligned}
$$

Another (not-so easy but still relatively easy) Example Continued Part 2

$2^{-1}{}_5 = \ldots 22223_5$.

Do you believe me? Let's multiply them and check!

Another (not-so easy but still relatively easy) Example Continued Part 2.5

$2^{-1}{}_5 = \ldots 22223_5$.

So you believe me. Let's multiply them and check!

$$
\begin{aligned}
&\ldots 22223_5 \\
\times &\ldots 00002_5 \\
= &\ldots 22220_5 \\
\times &\ldots 00002_5 + \ldots 00011_5 \\
= &\ldots 22200_5 \\
\times &\ldots 00002_5 + \ldots 00101_5 \\
= &\ldots 22000_5 \\
\times &\ldots 00002_5 + \ldots 01001_5 \\
= &\ldots 00001_5
\end{aligned}
$$

...Maybe The Example Wasn't So Easy

This is the short term goal: Understand negatives and fractions in the p-adics.

Negatives

As stated, we can define subtraction the exact same way. So let's look at -2_5 in a different light. What is $0 - 2$?

$$\begin{aligned} &\ldots 00000_5 \\ -&\ldots 00002_5 \\ =&\ldots 44445_5 \\ -&\ldots 00002_5 \\ =&\ldots 44443_5 \end{aligned}$$

-1

What is -1_p?

When $p = 5$, we have that $-1_5 = \ldots 44444_5$.

When $p = 7$, we have that $-1_7 = \ldots 66666_7$.

So it seems that
$-1_p = \ldots (p-1)(p-1)(p-1)(p-1)(p-1)_p$.
Note, these are digits, not multiplication!

A Cool Trick

Take for example $x = \ldots 00013501_7 = 3676$.

Let x_i be the ith digit. Then, set $-x_i$ so that $x_i + (-x_i) = p - 1$.

String these together to get:
$x - 1 = \ldots(-x_5)(-x_4)(-x_3)(-x_2)(-x_1)_p$

Then, $-x = x - 1 + 1 = \ldots 66653165_7 + \ldots 0001_7 = \ldots 66653166_7 = -3676$.

So $-x$ with $p = 8$ would be: $\ldots 77764277_8 = -5953$

What Next?

Computing inverses is tedious and time-consuming. But it helps us get a better understanding of fractions, so we must trek onwards.

Concept

We find the inverse of an integer directly by repeated division, but we'll use modulo. Then, we call this inverse the corresponding fraction. For example,
$\frac{1}{3} = 3^{-1} = 3^{-1}{}_{p}$.
Let's find this inverse in the 10-adics! (Yes, we can use non-prime bases, but you'll see why we don't in a bit...)

Find The First Digit!

Our target is the following number: $\ldots 00001_{10}$

We want the first digit to be 1. So, what x has the following property: $3x \equiv 1 \mod 10$?

Keep Crunching!

Set $x = 7$. Then $3x = 21$. So, our inverse must end with 7.

Now, we want the second digit to be 0. But we already have a 2 there! So, what x has the following property: $3x + 2 \equiv 0 \mod 10 \Rightarrow 3x \equiv 8 \mod 10$?

Crunching...

So $x = 6$ works, and we get that $6x + 2 = 20$. But wait, we have a 2 again! So the same x works!

I claim $\frac{1}{3}_{10} = \ldots 66667_{10}$.

If we truncate this infinite expansion, indeed, we have: $666\ldots667 \cdot 3 = 2000\ldots0001$. Thus, this works!

Let's Try A Similar Example

What is $\frac{2}{3}_{10}$? We want it to end in 2...

But we have the advantage of working in base 10. What number multiplied thrice is $x0000\ldots0002$ for some x?

How about: $x.00002$? Well, $x = 1$ works! Then, $0.33334 \cdot 3 = 1.00002$!

So, $\frac{2}{3}_{10} = \ldots 33334_{10}$.

Arbitrary p. Arbitrary fraction.

Let's say we want to find $\frac{11}{4}_5$. How would we do so?

First, find $\frac{3}{4}_5$ and add 2! Since arithmetic is well defined.

Our target number is $\ldots 000003_5$.

Solving for $4x = \ldots 000003_5$

First digit: $4x \equiv 3 \mod 5 \Rightarrow x = 2$. Then, $4x = 8 = 13_5$.

Second digit: $4x + 1 \equiv 0 \mod 5 \Rightarrow x = 1$. Then, $4x = 4_5$. But here, x is in the fives column, and we add with the previous term. We get: $40_5 + 13_5 = 103_5$.

Third digit: $4x + 1 \equiv 0 \mod 5 \Rightarrow x = 1$. Thus, the process repeats.

In the end: $\frac{3}{4}_5 = \ldots 111112_5$.

Thus, $\frac{11}{4}_5 = \ldots 111114_5$.

Particular Inverses

Consider 7 in base 7. This is 10_7. What's the inverse of 10_7? i.e. what number multiplied with 10_7 gives us $\ldots 0001_7$?

Unfortunately, No number multiplied with 0 gives us 1 under our rules. Unless... maybe we change the rules a bit...

Solution: Add digits to the right. We won't concern ourselves with this. We'll just look at $\mathbb{Z}_p$, the p-adic integers.

Why is p Usually Prime?

What issues arise when we use non-prime bases? Insolvability.

We can never have $2x \equiv 1 \mod 10$. Thus, $\frac{1}{2}_{10}$ cannot exist in $\mathbb{Z}_p$, the p-adic integers.
Recall: if p is prime, then $gcd(x, p) = 1$ if $1 < x < p$.

While we can solve this problem by adding digits to the right, another issue arises later down the line. We get a form of non-zero dividers which destroys the formalization of the p-adics. Thus, p needs to be prime.

TL;DR: While 10-adics exist, they aren't useful to study. Same with every composite number.

Time for a 15-second break!

Number Theory Time!

Let's introduce another way you might think about these p-adics.

Solving Polynomials Congruence Modulo p

We love congruence modulo in Number Thoery. A very common problem is this: What are the solutions to polynomials modulo p?

We look at a specific example. $X^2 \equiv 2 \mod p^n$ where we take $n \to \infty$. We'll use X to denote the polynomial and reserve x for variables.

Fun Fact: This section of MAT315 is where I first heard of p-adics in an academic context!

$X^2 \equiv 2 \mod p$

Let $p = 7$ and start with $n = 1$. Then, what x solves $X^2 \equiv 2 \mod 7$?

$X^2 \equiv 2 \mod p^2$

The answer is 3.
Continue with $n = 2$. Then, what x solves $X^2 \equiv 2 \mod 7^2$?

$X^2 \equiv 2 \mod p^3$

The answer is 10. We'll do this one more time before we list out all of the numbers.
Continue with $n = 3$. Then, what x solves $X^2 \equiv 2 \mod 7^3$?

I need a funny title name here

The answer is 108.
We can keep continuing this process.
Enter, Mathematica

For[i = 1, i < 20,i++,
Print[Solve[$x^2 == 2$, Modulus $->$ 7^i]]]

$$x- > 3, x- > 4$$
$$x- > 10, x- > 39$$
$$x- > 108, x- > 235$$
$$x- > 2166, x- > 235$$
$$x- > 4567, x- > 12240$$
$$x- > 38181, x- > 79468$$
$$x- > 155830, x- > 667713$$
$$x- > 24862120, x- > 15491487$$
$$x- > 266983762, x- > 15491487$$
$$x- > 1961835256, x- > 15491487$$
$$\vdots$$

Getting Our Sequence

More Mathematica Code:

L = {3,10,108,2166,4567,38181,155830,
1802916,24862120,266983762,1961835256,
5916488742,19757775943,116646786350,
116646786350,96117698062 36,42844700375837,
275475214363044,6789129606004840}

More code:

```
For[i=1, i<20, i++, Print[BaseForm[Part[L,i],7]]]
```

$$\ldots 00000000000003_7$$
$$\ldots 00000000000013_7$$
$$\ldots 00000000000213_7$$
$$\ldots 00000000006213_7$$
$$\ldots 00000000016213_7$$
$$\ldots 00000000216213_7$$
$$\ldots 00000001216213_7$$
$$\ldots 00000021216213_7$$
$$\ldots 00004212162137$$
$$\ldots 00064212162137$$
$$\ldots 00664212162137$$
$$\ldots 02664212162137$$
$$\ldots 12664212162137$$

p-adics Unlock New Worlds

So, $\sqrt{2}$ exists in the 7-adics.

We denote the 7-adics as $\mathbb{Q}_7$ (p-adic numbers) or $\mathbb{Z}_7$ (p-adic integers).

So, $\sqrt{2} = \ldots 12664212162136_7$.

And indeed,
$12664212162136^2{}_7 = 20156216344100000000000026_7$

And indeed, $-\sqrt{2} = 540024545045^2{}_7 =$
$43024164250120000000000026_7$

Let's find out what $\mathbb{Q}_7$ is!

Another 15-second break

Absolute Values

We continue in what seems a very distant land...

Properties of an Absolute Values

Given a field $\mathbb{F}$, define a function $|\cdot| : \mathbb{F} \to \mathbb{R}$.
$|\cdot|$ is an absolute value if it has the following properties:

- Positive Definiteness
- Homogeneity
- Triangle Inequality

We'll let our field be $\mathbb{Q}$ for any applications.

Positive Definiteness

For all $x \in \mathbb{F}$, $|\cdot|$ is positive definite if:

$$|x| \geq 0 \text{ and } |x| = 0 \Leftrightarrow x = 0$$

Homogeneity

For all $x, y \in \mathbb{F}$, $|\cdot|$ is homogeneous if:

$$|xy| = |x||y|$$

Triangle Inequality

For all $x, y \in \mathbb{F}$, $|\cdot|$ has the Triangle Inequality if:

$$|x + y| \leq |x| + |y|$$

Why Is This Useful?

Traditionally, a norm denotes 'distance' of some kind. And absolute value is a norm. But is there any way we can define 'distance' in a meaningful way so that leftmost digits are insignificant?

The Traditional Absolute Value

The traditional absoulte value, which we'll denote $|\cdot|_\infty$ is defined as follows:

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

This absolute value tells us how far away we are from 0. Namely, our leftmost digits have the greatest impact.

Convergence

We need to talk about convergence to understand how we can create an alternate absolute value.

We say a sequence (x_n) converges to some point x if: for all $\epsilon > 0$, we can find a natural number N so that: $|x_n - x| < \epsilon$ for all $n > N$.

i.e. Our sequence of numbers after some point N has a small 'distance' to x, the point we are converging to.

We want some notion of convergence so that our rightmost digits are most significant...

What Do We Want?

We'll drop the purple text color for numbers in base p. No more hand holding.

We want
$|\ldots 11110_p| > |\ldots 11100_p| > |\ldots 11000_p| > \cdots$.
However, this depends on our choice of p ($10000 = 41104_7$). So our absolute value will depend on p.

A Suggestive Sequence

There's one particular sequence that very well describes what we want.

Let p be given. Consider p^n for $n \geq 0$. We get:

$$
\begin{aligned}
p^0 &= 1_p \\
p^1 &= 10_p \\
p^2 &= 100_p \\
p^3 &= 1000_p \\
p^4 &= 10000_p \\
&\vdots \\
p^n &= \ldots 000_p
\end{aligned}
$$

How Do We Frame This?

So we want $p^n \to 0$. i.e. $|p^n| \to 0$. And maybe you notice that we can attribute the number of zeroes some value. Now we'll define the p-adic absolute value.

The p-adic Absolute Value

Let p be prime. Let $x \in \mathbb{Q}$. Then write $x = p^r \cdot x'$ so that $p \nmid x'$. i.e. r is the exponent of p in the prime factorization of x. Then $v_p(x) = r$. This is called the valuation.

Then we claim that $|x|_p = x^{-v_p(x)}$ is an absolute value. We call this the p-adic absolute value.

We'll postpone the proof until later.

Why Does The p-adic Absolute Value Work?

There's a little bit of magic that goes into constructing this absolute value from scratch. As in, why it's a negative exponent or why is there's an exponent. I'll keep that mystery hidden (we can chat later if you want). I'd rather investigate *how* this works.

Here's Why It Works

Consider the sequence p^n again. Recall, $|x|_p = p^{v_p(x)}$. Then:

$$|p^0|_p = |1|_p = p^0 = 1$$

$$|p^1|_p = |10_p|_p = p^{-1} = \frac{1}{p}$$

$$|p^2|_p = |100_p|_p = p^{-2} = \frac{1}{p^2}$$

$$|p^3|_p = |1000_p|_p = p^{-3} = \frac{1}{p^3}$$

$$|p^4|_p = |10000_p|_p = p^{-4} = \frac{1}{p^4}$$

$$|p^5|_p = |100000_p|_p = p^{-5} = \frac{1}{p^5}$$

Correlation

The p-adic absolute value tells us how many zeroes there are in the base p expansion of our number!

This is partially the truth. It gets quite complicated for certain rationals, and this 'intuition' doesn't explain how divergence to p-adic infinity works.

This absolute value tells us that $\frac{1}{p^n}$ should diverge p-adically, but once again, the inverse doesn't exist.

Proving The p-adic Absolute Value

Positive Definiteness: Clearly, $|x|_p = p^{v_p(x)} \geq 0$.

If $x = 0$, then $v_p(x) = \infty \Rightarrow |x|_p = p^{-\infty} = 0$. Yes, this is allowed.
If $x \neq 0$, then $v_p(x) = c < \infty \Rightarrow |x|_p = p^c \neq 0$.

Thus, $|\cdot|_p$ is Positive Definite

Proving The p-adic Absolute Value

Homogeneity. Let $x, y \in \mathbb{Q}$. Then,

$$|x|_p|y|_p = p^{v_p(x)} \cdot p^{v_p(y)} = p^{v_p(xy)} = |xy|_p$$

Proving The p-adic Absolute Value

Triangle Inequality: We'll prove a stronger version, the Strong Triangle Inequality: $|x + y|_p \leq \max\{|x|_p, |y|_p\}$.

We'll first prove the Strong Triangle Inequality for integers. Let $x_1, x_2 \in \mathbb{Z}$. Then we'll show that the Strong Triangle Inequality will hold.

Proving The p-adic Absolute Value

Note that since integers will only have non-negative exponents, we must have that: $|x_1 + x_2|_p \leq 1$. Let $|x_1 + x_2|_p$ be given so that $v_p(x_1 + x_2) = i$. Then, $x_1 + x_2 \equiv 0 \mod p^i$ and $x_1 + x_2 \not\equiv 0 \mod p^{i+1}$.

Thus, either (a) $p^{i+1} \nmid x_1$ and $p^{i+1} | x_2$,
(b) $p^{i+1} \nmid x_2$ and $p^{i+1} | x_1$
or (c) $p^{i+1} \nmid x_1, x_2$.

In case (a), $|x_1|_p \leq \frac{1}{p^i}$.

In the case of (b), $|x_2|_p \leq \frac{1}{p^i}$.

In the case of (c), $|x_1|_p \leq \frac{1}{p^i}$.

Proving The p-adic Absolute Value

Now, prove the Strong Triangle Inequality for all rationals. Let $x_1, x_2 \in \mathbb{Q}$. Then, we can write $x_1 = \frac{a}{b}$ and $x_2 = \frac{c}{d}$ with $a, b \in \mathbb{Z}$ and $c, b \in \mathbb{N}$.
Then, we have:

Proving The p-adic Absolute Value

$$
\begin{aligned}
|x_1 + x_2|_p &= \left|\frac{a}{b} + \frac{c}{d}\right|_p \\
&= \left|\frac{ad + bc}{bd}\right|_p \\
&= \left|\frac{1}{bd}\right|_p \cdot |ad + bc|_p \\
&\leq \left|\frac{1}{bd}\right|_p \cdot \min\{|ad|_p, |bc|_p\} \\
&= \min\{\left|\frac{ad}{bd}\right|_p, \left|\frac{bc}{bd}\right|_p\} \\
&= \min\{\left|\frac{a}{b}\right|_p, \left|\frac{c}{d}\right|_p\} \\
&= \min\{x_1, x_2\}
\end{aligned}
$$

A Curious Case Of Choosing Canonical Constants

The astute among you might have noticed something interesting. The base of the absolute value doesn't matter!

Specifically, we could have defined $|x|_p = c^{v_p(x)}$ for any $c > 1$. So why choose p? If you're curious, ask me later!

The Upshot

This absolute value is a norm. That means metrics. That means topology on a 'well behaved' space.

Here's what it's all been building up to.

p-adic Topology
Something Witty

Who? p-adic Topology

When? p-adic Topology

O7s in the chat plz

I'm so sorry my dear first-years. This is the conclusion of the talk. So bare with me for a few more slides.

Motivating $\mathbb{Q}_p$

There's two ways to construct $\mathbb{Q}_p$, the p-adic numbers.

1. Start with $\mathbb{Z}_p$ and add in the inverses.

2. Start with $\mathbb{Q}$ and complete it with respect to the metric. I prefer method 2 because it's all analysis, no algebra. i.e. only MAT257 is required.

Completion

Informally, we take $\mathbb{Q}$ and represent it as an equivalence class of limit points of sequences inside $\mathbb{Q}$. Then, we add all the Cauchy sequences that exist using the p-metric to $\mathbb{Q}$ to get $\mathbb{Q}_p$.

If $(x_i) \to x$, then $\|x\|_p = \lim_{i \to \infty} \|x_i\|_p$. Since $x_i \in \mathbb{Q}$, this is well defined.

So $\mathbb{Q}_p$ is the equivalence classes of limits of all Cauchy sequences.

Interesting Properties

Now that $\mathbb{Q}_p$ is a complete metric space, what interesting properties can we say about $\mathbb{Q}_p$ for all prime p?

1. Every ball is clopen.
2. Let $x, y \in \mathbb{Q}_p$ and $r \in \mathbb{R}$. If $y \in B(x, r)$, then $B(x, r) = B(y, r)$.
3. $\mathbb{Q}_p$ is totally disconnected. i.e. Only singletons are connected.
4. $\mathbb{Z}_p$ is the unit ball of $\mathbb{Q}_p$ centered at 0 for all p.

The first three properties come directly from the Strong Triangle Inequality. And metric spaces with the Strong Triangle Inequality are called ultrametric spaces and the metric is considered an ultrametric. The fourth property is just fun.

That was long...

That's it! Thanks for taking some time out of your day to enjoy some p-adics!

Citations

"P-adic number," Wikipedia, February 5, 2024, https://en.wikipedia.org/wiki/P-adic_number.

Richeson, David. "What are p-adic numbers." Division By Zero. Last modified November 24, 2008. https://divisbyzero.com/2008/11/24/what-are-p-adic-numbers/.

Andrew Rich (2008) Leftist Numbers, The College Mathematics Journal, 39:5, 330-336, DOI: 10.1080/07468342.2008.11922313

"Monsky's theorem," Wikipedia, January 5, 2024, https://en.wikipedia.org/wiki/Monsky%27s_theorem

Citations

Holloway, Paul James. “p-adic numbers.” Division By Zero. Last modified May, 2014. https://people.math.carleton.ca/ cingalls/ studentProjects/padicpaul.pdf

”Ostrowski’s theorem,” Wikipedia, December 11, 2023, https://en.wikipedia.org/wiki/ Ostrowski%27s_theorem

”Totally disconnected space,” Wikipedia, May 19, 2023, https://en.wikipedia.org/wiki/ Totally_disconnected_space

”Ultrametric space,” Wikipedia, July 16, 2023, https://en.wikipedia.org/wiki/Ultrametric_space

Citations

Albeverio, Sergio, Andrei Khrennikov, and Vladimir M. Šelkovič. Theory of p-adic distributions: Linear and nonlinear models. Cambridge: Cambridge University Press, 2010.

Gouvêa, Fernando Q. *P-adic numbers: An introduction*. Cham, Switzerland: Springer Cham, 2020.