Grade 11/12 Math Circles
October 25, 2023
P-adic numbers, Part 1

Introduction

You're familiar with the powers of 2, but you may not know about a pattern hidden in their digits. To see it, let's give each of the digits 0 through 9 its own color.

$2^0 = \boxed{1}$ $\quad 2^1 = \boxed{2}$ $\quad 2^2 = \boxed{4}$ $\quad 2^3 = \boxed{8}$

$2^4 = \boxed{1}\boxed{6}$ $\quad 2^5 = \boxed{3}\boxed{2}$ $\quad 2^6 = \boxed{6}\boxed{4}$ $\quad 2^7 = \boxed{1}\boxed{2}\boxed{8}$

$2^8 = \boxed{2}\boxed{5}\boxed{6}$ $\quad 2^9 = \boxed{5}\boxed{1}\boxed{2}$ $\quad 2^{10} = \boxed{1}\boxed{0}\boxed{2}\boxed{4}$

If we arrange these digits in rows with all the digits in the ones place are in the same column, all the digits in the tens place are in the same column, and so onwe will get a triangle. Overall the structure inside the triangle would look pretty random.

But what if we just look at certain rows? Here is the 1st row, 10th row, and 100th row, 1000th row, etc.

$2^1 =$												2
$2^{10} =$									1	0	2	4
$2^{100} = \dots$	4	9	6	7	0	3	2	0	5	3	7	6
$2^{1000} = \dots$	2	0	5	6	6	8	0	6	9	3	7	6
$2^{10000} = \dots$	7	9	2	5	9	6	7	0	9	3	7	6
$2^{100000} = \dots$	3	8	9	8	8	3	1	0	9	3	7	6
$2^{1000000} = \dots$	1	6	2	7	4	7	1	0	9	3	7	6
$2^{10000000} = \dots$	8	9	1	3	8	7	1	0	9	3	7	6
$2^{100000000} = \dots$	1	7	7	7	8	7	1	0	9	3	7	6

The numbers are too big, so I've chopped if off after 12 digits, but even with this amount of data we can see a pattern emerging: $\dots\boxed{8}\boxed{7}\boxed{1}\boxed{0}\boxed{9}\boxed{3}\boxed{7}\boxed{6}$.

What this is suggesting is that the last few digits of $2^{10^{n+1}}$ are exactly the same as the last few digits of 2^{10^n}. And as we increase n, the agreement gets better and better. In other words, in some sense, these numbers are converging to something.

Of course, they're not converging in the usual way. 2^{10^n} doesn't converge to anything as n gets larger. Its value grows and the number diverges to infinity. Is it finite? What does $\dots 87109376$ as a sequence of digits represent?

What we just discovered is a number that belongs to a completely different number system, other than the one we're used to.

We'll see below how this new number system works, and why this infinite-looking numbers actually make sense. This new number system is called p-adic numbers, where p can be any positive number and provides an alternative to the real numbers.

Strange things can happen with p-adics, for example:

$$\lim_{n\to\infty} 10^n = \dots 0$$

Stop and Think
What other infinite sequences of digits that is neither terminating nor recurring you know? What do they represent?

Notations

There are several different conventions for writing p-adic expansions. So far we used a notation for p-adic expansions in which powers of p increase from right to left.

Important! When performing arithmetic in this notation, digits are carried to the left. It is also possible to write p-adic expansions so that the powers of p increase from left to right, and digits are carried to the right. With this left-to-right notation we will use p-adic expansion of

$$2^{11} = 2048$$

can be written as $\ldots 2048$ or 2048_2, and $2^{11}+2$ is simply $\ldots 2050$ or 2050_2.

10-adic numbers

Let's start with 10-adic numbers, i.e. $p = 10$ and check what properties of known number systems would hold for the 10-adic numbers.

Example 1

How do we add two 10-adic numbers $\ldots 945873683 + \ldots 982887761 =?$

Solution:

Addition of p-adic numbers can be done in a usual fashion, i.e. digit by digit:

$$\begin{array}{r} \ldots 945873683 \\ {}^{+}\underline{\ldots 982887761} \\ \ldots 928761444 \end{array}$$

Example 2

How do we multiply two 10-adic numbers $\ldots 59333 \times \ldots 61444 =?$

Solution:

Multiplication is basically summation performed many times, again it is fairly straightforward, yet might be time consuming:

$$\begin{array}{r} \ldots 59333 \\ {}^{\times}\underline{\ldots 61444} \\ \ldots 237332 \\ \ldots 2373320 \\ \ldots 23733200 \\ \ldots 593330000 \\ {}^{+}\underline{\ldots 3559980000} \\ \ldots 3645656852 \end{array}$$

Now we will consider a special case. Take a 10-adic number $\ldots 857142857143$ and multiply it by a single digit number 7:

$$\begin{array}{r} \ldots 857142857143 \\ \times\ \underline{\ldots 000000000007} \\ \ldots 000000000001 \end{array}$$

So, this number times 7 equals 1 as we disregard all zeros before the 1 in a 10-adic system.

Therefore, $\ldots 857142857143 \times 7 = 1$, or simply $\ldots 857142857143 = \frac{1}{7}$.

Which means a 10-adic system can has rational numbers!

Exercise 1

Find a 10-adic number that equals $\frac{1}{3}$.

Now let's consider another special 10-adic number $\ldots 9999999999$. What does it represent?

To figure this one out we will start by setting it equal to some value x:

$$\ldots 9999999999 = x$$

and we will multiply the number by 10 (since we already know how to multiply p-adics) to get

$$\ldots 9999999990 = 10x$$

Now subtract one number from another to get

$$\begin{array}{r} \ldots 9999999999 \\ -\ \underline{\ldots 9999999990} \\ \ldots 0000000009 \end{array}$$

In other words, $x - 10x = 9$, then $x = -1$, so $\ldots 9999999999 = -1$. Negative p-adics! Notice that you don't need a negative sign to describe all negative p-adic numbers.

It is easy to see why $\ldots 9999999999 = -1$, just add two 10-adic numbers $\ldots 9999999999$ and 1 and see what happens.

Exercise 2

Find a 10-adic number that equals -3.

There is a more general rule on negative 10-adic numbers, which can be stated as follows.

Theorem 1

To find a negative 10*-adic number take the complement of every digit of a positive* 10*-adic number and then add* 1*.*

Exercise 3

How would you prove Theorem 1?

Example 3

What's a negative of $\ldots 857142857143$?

Solution:

We use Theorem 1 and we first take complement of every digit to digits of $\ldots 857142857143$ as

$$\ldots 857142857143$$
$$\ldots 142857142856$$

where a complement of 3 is $9-3=6$, complement of 4 is $9-4=5$, etc. Then adding 1 to the result we get $\ldots 142857142856 + 1 = \ldots 142857142857$.

Quick check to verify this is indeed $-\frac{1}{7}$:

$$\begin{array}{r} \ldots 857142857143 \\ + \underline{\ldots 142857142857} \\ \ldots 000000000000 \end{array}$$

We have established that 10-adic numbers have fractions and negative numbers, yet we have a strange property, which is not common for a conventional number systems, such as real numbers, which is that some 10-adic number multiplied by itself result in itself, and they are not necessarily equal to 0 or 1. For instance $\ldots 92256259918212890625$.

You can verify that this number indeed has the property $n \times (n-1) = 0$ by simply multiplying it by itself minus one

$$\begin{array}{r} \ldots 92256259918212890625 \\ \times \; \underline{\ldots 92256259918212890624} \\ \ldots 00000000000000000000 \end{array}$$

Stop and Think

How do integer numbers look like in 10-adic expansion?

This number is itself squared! In other words, $n^2 = n$ and $\ldots \neq 0, 1$. This breaks a very fundamental property we usually use a special property of zero, which is if

$$a \times b = 0,$$

then at leas one of a, b is equal to zero. This does not hold for 10-adics. However, we will see further that this is not a problem of all p-adics.

3-adic numbers

We construct the p-adic numbers for prime p in the same way we construct the 10-adic integers, except of course we work in base p not base 10. There is a bonus property coming from the fact that p is prime: there are no zero divisors.

Let us use $p = 3$, which is a prime number to demonstrate. Note that any prime number $2, 3, 5, 7, \ldots$ can generally be used to do the same.

While 3 is a prime number, 10 is not, it's 2×5. When you multiply 10-adics and the result is zero, which pair of digits can do that? One option is when one of the digit s is zero:

$$\begin{array}{r} \ldots ????????????0 \\ \times \; \underline{\ldots ????????????2} \\ \ldots ????????????0 \end{array}$$

But there's another case:

$$\begin{array}{r} \ldots ????????????2 \\ \times \; \underline{\ldots ????????????5} \\ \ldots ????????????0 \end{array}$$

If we switch to a prime p, say 3, this is not the case anymore as only digits we have now are $0, 1, 2$ and out of all possible products of digits in a 3-adic numbers only pairs with 0 will result in a zero digit, like here

$$\begin{array}{r} \ldots 1201021012 \\ \times \; \underline{\ldots 0000000000} \\ \ldots 0000000000 \end{array}$$

Stop and Think

How does 4 look like in a 3-adic system?

Exercise 4

Find a 3-adic expansion of -1.

This means there are no 3-adic number that is itself squared, except for $0, 1$. In other words, 3-adics have all the good properties of 10-adics and do not break rules. We say the p-adic numbers form a field, because they have the 4 operations $+, -, \times, \div$. This can be stated as the following result.

Definition 1

(Informal) A field is a set, along with two operations defined on that set: an addition operation $+$, and a multiplication operation written as $\times$, both of which must behave in the same way as they behave for real numbers, which means these operations are required to satisfy field axioms.

name	addition	multiplication
associativity	$(a+b)+c=a+(b+c)$	$(a\,b)\,c=a\,(b\,c)$
commutativity	$a+b=b+a$	$a\,b=b\,a$
distributivity	$a\,(b+c)=a\,b+a\,c$	$(a+b)\,c=a\,c+b\,c$
identity	$a+0=a=0+a$	$a\cdot 1=a=1\cdot a$
inverses	$a+(-a)=0=(-a)+a$	$a\,a^{-1}=1=a^{-1}\,a$ if $a\neq 0$

Theorem 2

The p-adic numbers with prime p with "$+$" and "$\times$" defined above form a field.

Square roots

When does a nonzero 3-adic number have a square root?

First of all we can take out factors of 3, and there most be an even number of these. So we reduce to the case when the units digit is 1 or 2. If the last digit is 2 there is no square root, even mod 3. So what if the last digit is 1? Then we can always find a square root. For example, we can find the square root of $\sqrt{16}$ as $\ldots 11$ by finding the digits one by one. (There are much faster ways of course, such as Newton's method.)

$$\begin{array}{r} \ldots 000011 \\ \times\ \underline{\ldots 000011} \\ \ldots 000011 \\ +\ \underline{\ldots 000110} \\ \ldots 000121 \end{array}$$

Where $\ldots 000121_3 = 1 \times 3^0 + 2 \times 3^2 + 1 \times 3^2 = 16$.

What is the relation between irrational numbers and p-adics? The following exercise will help you understand the connection.

Exercise 5

Find the first three digits of $\sqrt{7}$ in the 3-adic integers.

Finding each digit requires us to divide by 2, so this does not work for 2-adic integers, and for these square roots are more complicated. For example, $5 = 101_2$ has no square root even though its units digit is 1.

Exercise 6

Find the first few digits of $\sqrt{17}$ in the 2-adic integers.

Exercise 7

Find p for which the equation $x^2 = -1$ has at least a single solution.

Hint:

Check $p = 2, 3$, then consider $\lim_{n\to\infty} 2^{5^n}$ in a 5-adic system.

The p-adics with prime base have been successfully used by researches to crack world's toughest mathematical puzzles of all time such as

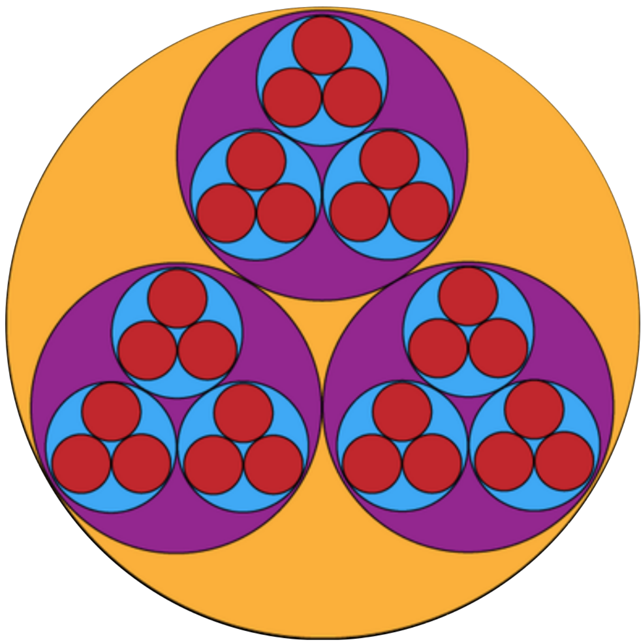
Fermat's last theorem

The equation $x^n + y^n = z^n$ has no solutions in integers for $n > 2$.

In fact to solve it, the p-adics had to be invented.

The geometry of the p-adics

P-adic do not exits on the number line on the contrary to the real numbers. In this section, we discuss the topology induced by the p-adic metric in an attempt to better visualize the p-adic numbers. Let us start with the following construction for representation of 3-adics to show how it all works. Before formalizing the details, we examine the image above. Each circle contains three main sub-circles. The integers within a subcircle of a given circle have a particular 3-adic distance from integers in another subcircle of that circle.



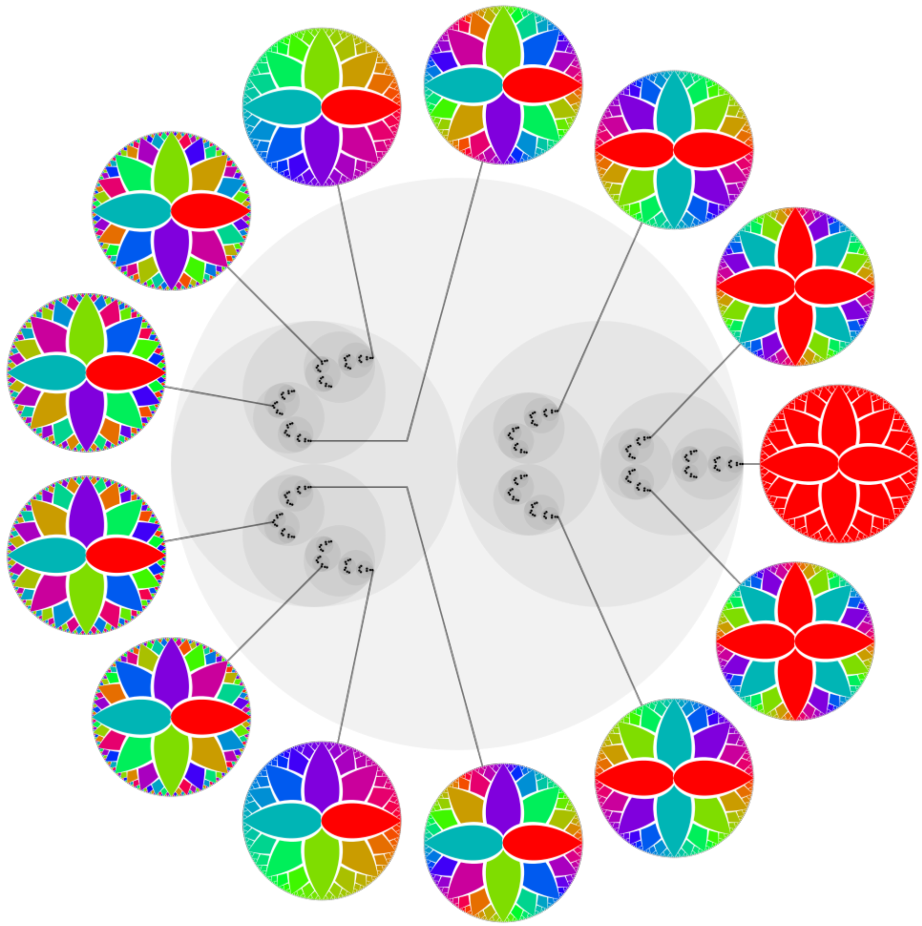
A visualization of the 3-adic integers.

For example, the orange circle has purple subcircles. The integers within a purple subcircle are a distance of one away from the integers in a different purple subcircle. The distance corresponding to the largest circle is one since one is the largest possible 3-adic distance between integers. While there are no circles larger than the orange one, the circles can get infinitely small! As we can choose numbers that differ by larger and larger powers of 3. In this way, the p-adic integers are not discrete even though they are disconnected. Hence, a good image of the p-adic integers would be fractal-like, as the figure above is.

There is so much more that can be acomplished with the fascinating new tool we learned about today and we will master its use in the second part of the lecture.

P-adics are simply beautiful

One last thing, take a moment to pause and enjoy this image created by Christopher Culter shows the compact Abelian group of 2-adic integers (black points), with selected elements labeled by the corresponding character on the Pontryagin dual group (colored discs).



References

Koblitz, N. (2012). $p-$adic Numbers, $p-$adic Analysis, and Zeta-Functions (Vol. 58). Springer Science & Business Media.

Borcherds, R. (2020). Berkeley math circle: $p-$adic numbers (lecture notes).