Grade 11/12 Math Circles

November 8, 2023

P-adic numbers, Part 2

What are p-adics good for?

We've learned about the p-adic numbers and what they are in Part 1 of our lesson, let us recall the main properties of these numbers.

P-adic numbers

- Can be added
- Can be multiplied
- Can be negative (Theorem 1)
- Can be rational and irrational numbers
- Form a *field* if and only if p is a prime number

Now let's discuss why are they important for modern mathematics. The best way to show their impact is to demonstrate by example. We will consider two striking cases where the use of p-adics as a tool simplifies the original problem.

Definition 1

We say $x = y \ mod \ z$ or $x =_z y$ if the remainder r of $x \div z$ is equal to y.

Definition 2

We call x divisible by z if the remainder $x \div z$ is 0.

For instance $17 =_3 2$, because $17 = 5 \times 3 + \mathbf{2}$.

This allows us to solve equations in modular arithmetic like $x = y$ such that

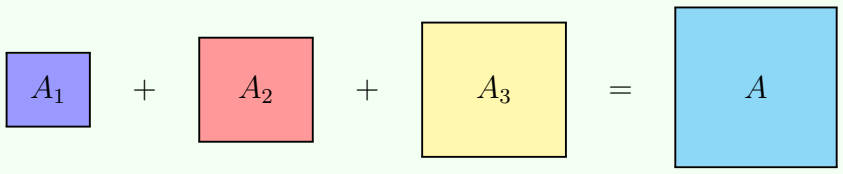
$$x = x_0 \times z^0 + x_1 \times z^1 + x_2 \times z^2 + \ldots, \quad y = y_0 \times z^0 + y_1 \times z^1 + y_2 \times z^2 + \ldots$$

by comparing each and every remainder of both x and y as

$$\begin{aligned} &x_0 = y_0, \\ &x =_z y, \quad \text{or } x_0 + x_1 \times z^1 =_z y_0 + y_1 \times z^1 \\ &x =_{z^2} y, \quad \text{or } x_0 + x_1 \times z^1 + x_2 \times z^2 =_{z^2} y_0 + y_1 \times z^1 + y_2 \times z^2 \end{aligned}$$

Example 1

Find 3 squares whose area create a bigger square of area $A = A_1 + A_2 + A_3$ and the side is a rational number. The area of the first square A_1 is the side length of the second square and the area of the second square A_2 is the side length of the third square (see image below).



Solution:

Set the side of the first square equal to x, then its' area $A_1 = x^2$.

Since the side length of the second square is equal to A_1, its' side is x^2 and its' area $A_2 = x^4$.

Finally, the side length of the third square is equal to A_2, its' side is x^4 and its' area $A_3 = x^8$.

We're looking for the side of the square y with area $A = A_1 + A_2 + A_3$, then

$$x^2 + x^4 + x^8 = y^2$$

It's hard to solve this equation in real number. For instance, $x = 1$. Then $y^2 = 1^2 + 1^4 + 1^8 = 3$, therefore $y = \sqrt{3}$, which is irrational.

Exercise 1

Find solution for y if $x = \frac{1}{2}$. Is it a rational number?

But how do we find this and other rational solutions? In order to do it we will need to use our helpful tool, the p-adics!

Let us restate the problem in 3-adics, i.e. we're looking for a 3-adic number x:

$$x = x_0 3^0 + x_1 3^1 + x_2 3^2 + \dots$$

such that

$$y^2 = x^2 + x^4 + x^8$$

and y is rational.

In this case,

$$x^2 = (x_0 3^0 + x_1 3^1 + x_2 3^2 + \dots)^2,$$

$$x^4 = (x_0 3^0 + x_1 3^1 + x_2 3^2 + \dots)^4,$$

$$x^8 = (x_0 3^0 + x_1 3^1 + x_2 3^2 + \dots)^8$$

We will now consider the first terms of each of the series and compare them *mod* 3, meaning we're looking only for the remainder of the result after division by 3:

$$x_0^2 + x_0^4 + x_0^8 =_3 y_0^2$$

Since in 3-adics we can only operate with digits $0, 1, 2$, the x_0, y_0 can only be one of these digits.

x_0	x_0^2	x_0^4	x_0^8	$x_0^2 + x_0^4 + x_0^8$
0	0	0	0	0
1	1	1	1	$3 \ mod \ 3 = 0$
2	1	1	1	$3 \ mod \ 3 = 0$

y_0	y_0^2
0	0
1	1
2	$4 \ mod \ 3 = 1$

Since for all values of x_0 the only value we get for $x_0^2 + x_0^4 + x_0^8$ is zero, the only possible y_0 is zero as well, however we can choose $x_0 - 0, 1, 2$ in 3-adics.

We skip the $x_0 = 0$, as a trivial solution, we want a nonzero solution, take for example $x_0 = 1$, then the next step is to figure out the value for x_1 by considering the equation *mod* 9, i.e.

$$x =_9 1 + 3x_1, \quad y =_9 3y_1$$

$$x^2 + x^4 + x^8 =_9 (1 + 3x_1)^2 + (1 + 3x_1)^4 + (1 + 3x_1)^8 =_9 (3y_1)^2 =_9 y^2$$

Since we're considering equation *mod* 9, the first term

$$(1+3x_1)^2 =_9 1+6x_1+9x_1^2 =_9 1+6x_1$$

The next term is previous one square

$$(1+3x_1)^4 =_9 (1+6x_1)^2 =_9 1+12x_1+36x_1^2 =_9 1+3x_1$$

The final term is then $(1+3x_1)^2$, which is *mod* 9 just $1+6x_1$ again. Finally $y^2 =_9 (3y_1)^2 =_9 9y_1^2 =_9 0$!

We get the equation

$$(1+6x_1)+(1+3x_1)+(1+6x_1) =_9 0,$$

$$3+15x_1 =_9 0$$

which has a lot of solutions in *mod* 9 , for example take $x_1 = 1$.

Exercise 2

Check that $x_1 = 1$ is a solution to $3+15x_1 =_9 0$.

Continue in the same fashion, consider equation *mod* 27:

$$x =_{27} 1+3x_1+3^2x_2, \quad y =_{27} 3y_1+3_2^y$$

$$x^2+x^4+x^8 =_{27} (1+3x_1+3^2x_2)^2+(1+3x_1+3^2x_2)^4+(1+3x_1+3^2x_2)^8 =_{27}$$

$$(1+3+9x_2)^2+(1+3+3^2x_2)^4+(1+3+3^2x_2)^8 =_{27} (4+9x_2)^2+(4+3^2x_2)^4+(4+3^2x_2)^8 =_{27} (0+9y_2)^2$$

Since we're considering equation *mod* 27, the first term

$$(4+9x_2)^2 =_{27} 16+18x_2+81x_2^2 =_{27} 16+18x_2$$

The next term is previous one square

$$(16+18x_2)^4 =_{27} 256+576x_2+324x_2^2 =_{27} 13+9x_2$$

The final term is then $(13+9x_2)^2$, which is *mod* 27

$$169 + 243x_2 + 81x_2^2 =_{27} 7 + 18x_2$$

So

$$(16 + 18x_2) + (13 + 9x_2) + (7 + 18x_2) =_{27} 81y_2^2 =_{27} 0,$$

$$36 + 45x_2 =_{27} 9 + 18x_2 =_{27} 0,$$

which leads to $x_2 = 1$.

This is not a coincidence, in fact all $x_n = 1$! So the answer is $x = \ldots 1111111_3$.

Let's try to find what that number is in real numbers:

$$x = 1 + 3^1 \times 1 + 3^2 \times 1 + \ldots$$

is a divergent series, however let's still apply the formula for the sum of the geometric series, we'll explain why we can do that later in the lesson.

Stop and Think

For which λ does the general formula for sum of a geometric series with growth factor λ work

$$1 + \lambda + \lambda^2 + \cdots = \frac{1}{1-\lambda}$$

$$1 + 3^1 \times 1 + 3^2 \times 1 + \cdots = \frac{1}{1-3} = -\frac{1}{2},$$

substitude it back into the eqaution to get

$$\left(-\frac{1}{2}\right)^2 + \left(-\frac{1}{2}\right)^4 + \left(-\frac{1}{2}\right)^8 = y^2$$

simplify to get

$$\frac{1}{4}+\frac{1}{16}+\frac{1}{256}=\frac{81}{256}=\left(\frac{9}{16}\right)^2,$$

Hence $y=\frac{9}{16}$. We just found a solution we already saw in Example 1.

Other solution can be found if we chose $x_0=2$ instead of $x_0=1$, and generally there might be infinitely many solutions.

Let's go back to the question, why could we actually apply the geometric series formula even though $\lambda=3>1$ in this case?

Distance and series

We first define the size of a p-adic or real number. For a real number its size is just the absolute value. For a p-adic number we define the size to be to be smallest p^n where $p^n\times x$ is any nonzero unit. ($|0|_p=0$.) In other words, the absolute value of a p-adic number is the number of subsequent zeros in it counting from right to left. So the number p^n for n large is a large real number but a small p-adic number.

Example 2

What's $|x|_p$ for $x=231400000_p$?

Solution:

$$231400000=p^5\times(unit)$$

therefore $|x|_p=p^{-5}$.

This means a distance between two large 3-adic numbers, let's say $s_1=\ldots 2101102_3$ and $s_2=\ldots 2102102_3$, with all subsequent digits equal each other i.e.

$$s_1=2+3^1\times 0+3^2\times 1+3^3\times 1+3^4\times 0+\ldots,\quad s_2=2+3^1\times 0+3^2\times 1+3^3\times 2+3^4\times 0+\ldots$$

$$s_1-s_2=3^3,\quad |s_1-s_2|_3=3^{-3}=\frac{1}{27}$$

So the further the digit in the number, the smaller the distance between s_1 and s_2 which is the opposite to how distance for the real numbers works.

For real numbers, convergence of a series can be very tricky. For example, the series $1+\frac{1}{2}+\frac{1}{3}+\ldots$ does not converge even though the terms tend to 0, while the sum of the series $\log(2) = 1-\frac{1}{2}+\frac{1}{3}-\ldots$ changes if we change the order of the terms. For p-adic numbers, things are much simpler: a series converges if and only if its terms terns to zero (meaning that their p-adic sizes tend to 0).

For example, the series $1+x+x^2+$ converges p-adically if $|x|_p < 1$.

It's easy to see now why we used sum of geometric series of $\ldots 11111_3$ and got a finite number. This is due to the size of

$$|x|_3 = |\ldots 11111|_3 = 3^{-\infty} = 0 < 1.$$

Exercise 3

What's bigger the distance between $s_1 = \ldots 010101$ and $s_2 = \ldots 101010$ or the absolute value of their sum in 3-adics?

We will consider one more important problem that can be effectively solved with p-adics.

Example 3

When is n^2+7 divisible by a large power of 2?

Solution:

When we write a few first values of n we get:

$$\begin{aligned}
0^2+7 &= 7 = 2^0 \times 7,\\
1^2+7 &= 8 = 2^3 \times 1,\\
2^2+7 &= 11 = 2^0 \times 11,\\
3^2+7 &= 16 = 2^4 \times 1,\\
4^2+7 &= 23 = 2^0 \times 23,\\
5^2+7 &= 32 = 2^5 \times 1
\end{aligned}$$

the higher the power of 2 you want n^2+7 to be divisible, the larger the n you need, for example the first solution we find for 2^8 is $n = 53$.

The quick way to find such numbers is by considering them in 2-adics and we want $n^2+7 \approx 0$ in

2-adic sense, which can be stated as an equation $x^2 + 7 = 0$ in 2-adic sense.

Using a special procedure mathematicians call Newton's method we can find a solution for any power of 2 by taking enough steps of the following form:

$$x^{(i+1)} = x^i - \frac{(x^i)^2 + 7}{2x^i}$$

starting with $x^0 = 1_2$. Using this technique you can find for example, the 2-adic number which in real numbers can be written as $x = 206036503412917$ such that

$$x^2 + 7 = 2^{51} \times 18852049138927$$

Further reading

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).