The Exotic Realm of p-adic Numbers

Daniel Mathews

September 5, 2003

Numbers come in many forms, shapes and sizes. We all use whole numbers, fractions, and real numbers every day, but many people never stop to ask why these types of numbers are so special, or natural: why should these numbers be as they are? Some mathematicians, on the other hand, do ask what the hell is going on, and how did these numbers get here, and by the way where did I put my coffee, and oh can you remind me what my name is again?

It turns out that these hare-brained mathematicians have a point. While the "usual" numbers mentioned above do form part of the world of numbers, this world of numbers and number systems is immeasurably broader, full of amazing and strange lands. And one of the most exotic corners of this world is the realm known as *p-adic numbers* — a realm rarely visited by the average mathematician, much less the average person!

So, let us don our Thinking Caps and Number Theoretical Boots and head off to this undiscovered country! We shall attempt to observe this exotic species in its natural state. But beware, p-adic numbers are a highly twisted bunch!

Our journey starts at the familiar land of integers (whole numbers). We should all know what a whole number is! But as the great mathematician Dedekind once said, "God made the integers; all the rest is the work of man." We quickly move on to the nearby field of fractions, or rational numbers, which hopefully we should all know as well.

We can be content with our knowledge of fractions from primary school, but a pure mathematician might ask how we got there from the land of integers. The answer is, of course, you get rational numbers by *dividing* one integer by another! Starting from 3 and 5, you get $\frac{3}{5}$ by dividing 3 by 5. A pure mathematician might go further and actually *define* rational numbers *in terms* of integers — in fact as an *ordered pair* or integers — but let's not trouble ourselves with details. We need to get to our destination, after all! But you might note that, in order to gain a better understanding of a number system like the fractions, you should try to relate it to a simpler number system like the integers.

So, after a brisk traversal of the field of rational numbers, we move on and arrive at the kingdom of real numbers. Now we still might have a pretty good idea of what a real number is, from our intuition. A real number is a point on the real number line. Or, maybe slightly more accurately, a real number is one that can be written as a decimal, for instance

$$-1.2,\ 0.66666\cdots,\ 1.414213562373\cdots,\ 26.$$

Note that the decimal digits can terminate, or continue infinitely far, with or without repetition.

However, our pure mathematician friend (if he hasn't got lost yet and strayed over into the sphere of complex numbers) might want a bit more detail here. Yes, but how did we get the real numbers from the rational numbers? Well, there are a few ways to answer this, but one way might be as follows (our friend Dedekind had a different answer). We can think of real numbers as *numbers approximated by rational numbers*. So for instance

$$1,\ 1.4,\ 1.41,\ 1.414,\ 1.4142,\ 1.41421,\ 1.414213,\ldots$$

is a sequence of rational numbers which approximates the real number $1.414213562\cdots = \sqrt{2}$, while the boring sequence

$$221, 221, 221, 221, \ldots$$

is a sequence of rational numbers approximating, you guessed it, 221! In this way we will be able to approximate all the rational numbers, but also we will add in extra numbers to the rationals, to get the entire real number line. Techncially, the "approximating" sequences we're looking at are called *Cauchy* sequences, but again let's not bother ourselves with details too much. This process is known as *completing* the rational numbers.

Having brought you this far on the journey, we must say *turn back!* We've actually gone too far, and need to go back to the field of rational numbers. So forget about the real numbers, go back to the fractions. And let's take a different route.

The clever mathematician (or maybe it's just too much exposure to the elements) might ask, "well, is there any *other* way to complete the rational numbers?" Because, while the main track through the field of rational numbers leads directly to the reals, there is another, less travelled road which, if you find it, leads to the exotic and surreal land of p-adic numbers.

How might we set out to complete this task of completion? Remember that the real numbers are made by approximating them with rational numbers. But there is more than one way to approximate numbers! The sequences we saw before approximate real numbers, in one sense. But here's another.

On a whim let's try to find numbers congruent to 221 modulo 7. So for instance we have

$$221 \equiv 4 \bmod 7$$

for a start. Then, let's try for a larger modulus. Let's try modulo $7^2 = 49$, which (in a vague way) is a "refinement" of modulo 7.

$$221 \equiv 25 \bmod 7^2$$

And now let's keep going...

$$\begin{aligned} 221 &\equiv 221 \bmod 7^3 \\ 221 &\equiv 221 \bmod 7^4 \\ 221 &\equiv 221 \bmod 7^5 \\ &\cdots \end{aligned}$$

So, by refining our search by taking higher and higher modulos, we can obtain a sequence of rational numbers which "approximate" 221, in some fashion! The sequence is

$$4, 25, 221, 221, 221, 221, \ldots.$$

Seems pretty ridiculous? Of course, but we're about to see some even stranger stuff. Let's see if we can get a sequence of numbers, using the same method, to approximate $\sqrt{2}$, which you might recall is *not* a rational number! Well, finding $\sqrt{2}$ is the same thing as finding a solution x to the equation $x^2 = 2$. So, again we'll investigate the problem modulo 7, 7^2, 7^3, and so on.

$$\begin{aligned} x^2 \equiv 2 \bmod 7 &\Rightarrow x \equiv 3, 4 \bmod 7 \\ x^2 \equiv 2 \bmod 7^2 &\Rightarrow x \equiv 10, 39 \bmod 7^2 \\ x^2 \equiv 2 \bmod 7^3 &\Rightarrow x \equiv 108, 235 \bmod 7^3 \\ x^2 \equiv 2 \bmod 7^4 &\Rightarrow x \equiv 2166, 235 \bmod 7^4 \end{aligned}$$

Now, as a mathematician named Hensel found in the 19th century, it turns out that you get *exactly* two solutions for every modulus 7^n (can you prove it?), so we get two sequences of rational numbers (in fact just integers)

$$3, 10, 108, 2166, \ldots \text{ and } 4, 39, 235, 235, \ldots$$

which approximate the two numbers $\pm\sqrt{2}$ somehow! In fact, we say that these sequences *converge 7-adically* to $\pm\sqrt{2}$. So $\sqrt{2}$ is a 7-adic number, and quite close to 108, though even closer to 2166!

If you can escape from the previous discussion with your brain intact, then you're well on the way to p-adic land! Because the p-adic numbers are just what you get, when you complete the rational numbers, adding in all the necessary extra numbers, in this bizarre, insane, who-fried-my-brain kind of way. The are *numbers approximated by congruences modulo larger and larger powers of p.* Note that, as you might have guessed, the p here stands for a prime (we took $p = 7$ above).

Let's think a bit more about what we're saying by "approximating" here, because it has mind-bending implications. Normally, if we're given two numbers x, y and asked to see how "close" they are, we look at $|x-y|$. This is our standard notion of *distance.* But this is no longer the case in the p-adic realm! Here we don't think of distance as $|x - y|$, but rather *how many times $x - y$ is divisible by our prime p.* The more times divisible, the closer the numbers are. This is the p-adic notion of distance! So, 1 and 1001 are quite close 2-adically, since 1000 is divisible by 2, three times. The numbers 1 and 1000001 are even closer, since 1000000 is divisible by 2, six times. But 1 and 0 are far apart 2-adically (in fact, any-adically), since 1 is not divisible by 2 (or any other prime p). Truly an exotic realm!

As one final glimpse into this surreal world before we must set sail, let's look at the series

$$1 + 2 + 4 + 8 + 16 + 32 + \cdots.$$

Let's look at the partial sums 2-adically, and compare them to -1.

$$\begin{aligned} 1 &\equiv -1 \bmod 2 \\ 1+2=3 &\equiv -1 \bmod 2^2 \\ 1+2+4=7 &\equiv -1 \bmod 2^3 \\ 1+2+4+8=15 &\equiv -1 \bmod 2^4 \\ 1+2+4+8+16=31 &\equiv -1 \bmod 2^5 \end{aligned}$$

So we can see that these partial sums are getting closer and closer to -1. Therefore, in the limit we have the following astounding sum, which incidentally agrees with the formula you might have learnt for geometric series!

$$1+2+4+8+16+32+\cdots=-1$$

Or, you could write this equation in "2-adic binary notation", in which case the left-hand side has an infinite expansion, but *before the decimal point, not after*!!!

$$\cdots 1111111111111 = -1$$

What's so special about p-adic numbers, you ask? Surely we could have made up any dumb rules we wanted to complete the rational numbers and come up with a silly number system! Well, it turns out (a result known as Ostrowski's theorem) that the *only* way you can properly complete the rational numbers is to get either some p-adic numbers, or the reals! Since there are 2-adic, 3-adic, in fact infinitely many families of p-adic numbers, in one sense *most* of the number systems obtained from completing the rational numbers are p-adic! So they are quite important... and number theorists use them a lot as well.

But, unfortunately for us, our voyage is over, and we must return to the mundane land of integers... For some detail, see, for instance, *p-adic numbers: an introduction* by Gouvea.