Berkeley math circle: p-adic numbers

Richard Borcherds

2020 September 2

These are rather sketchy notes for a talk given to the Berkeley math circle (https://mathcircle.berkeley.edu/). There will probably be a video of the talk available on youtube.

1 10-adic integers

Problem: find a number whose square ends in the same 10 digits. Smaller examples are things like $76^2 = 5776$, $625^2 = 390625$, and so on. Two solutions are 1787109376 and 8212890625. We can find the second by repeatedly squaring 5: $5 \to 25 \to 625 \to 390625 \to \dots$

What happens if we continue this forever to get an "infinitely long integer"? This seems at first sight to make no sense, but is in fact something called a 10-adic number.

An ordinary integer can be represented as something like -12345 with a sign and a finite number of decimal digits. A 10-adic number is similar except that we omit the sign and allow an infinite string of digits going off to the left; for example $\cdots 87654321$. This differs from real numbers such as $3.1415926\cdots$ which have an infinite string going off to the right.

What can we do with 10-adic integers?

We can add them using the usual rules of arithmetic. This is because the last n digits of $a + b$ depend only on the last n digits of a and b. For example $\cdots 987 + \cdots 444 = \cdots 431$. Similarly we can multiply them.

Exercise 1.1. What is $1 + 9 \times \cdots 1111111$?

What about subtraction? You might think we need to put a sign in front to allow negative 10-adic integers, but in fact we do not. For example $\cdots 99999 + 1 = 0$. (You used to be able to see this on mechanical odometers.) The negative of a number is got by taking the 9's complement of each digit then adding 1. For example, the negative of $\cdots 3210$ is got by taking $\cdots 6789$ and adding 1 to get $\cdots 6790$. The reason this works is that the 9's complement of n is $\cdots 99999 - n = -1 - n$, so if we add 1 we get $-n$.

Computers these days treat integers as a sort of 2-adic number (in base 2 rather than base 10). For example, on an 8 bit computer, the integer -1 is represented as 11111111.

So we have addition, subtraction, and multiplication, and these obey most of the usual rules of algebra (in other words the 10-adic integers form a RING). How do we check this? We know the integers mod 10^n form a ring (denoted $\mathbb{Z}/10^n\mathbb{Z}$). A 10-adic number such as $\cdots 712$ can be thought of as a series 2, 12, 712, ... of integers mod 10, 100, 1000, that are compatible. (This construction is sometimes called a "projective limit" or "inverse limit" as we are taking a sort of weird limit of the rings $\mathbb{Z}/10^n\mathbb{Z}$.) We can multiply and add 10-adic numbers by just doing this mod 10, 100, 1000, and so on, so since the usual rules work for integers mod 10^n they also work for 10-adic numbers.

Now try division. $1/2$ does not exist, as if n is a 10-adic number then the last digit of $2n$ is even, not 1. Similarly we cannot form the inverse of any even 10-adic integer, or any 10-adic integer divisible by 5. What about 3? If $\cdots 9999$ is -1 then $\cdots 3333$ is $-1/3$, so $1/3$ is $\cdots 6667$. What about $1/7$? For real numbers $1/7 = \cdot 142857142857\ldots$ repeating endlessly, and we can find $2/7, 3/7, \ldots$ by shifting this. Let's try $\cdots 142857 \times 7$. We get $\cdots 99999 = -1$. So $1/7 = \cdots 857142857142 + 1 = \cdots 857142857143$.

Exercise 1.2. Find the numbers $1/7, 2/7, 3/7, 4/7, 5/7, 6/7$ as real numbers and as 10-adic numbers. What do you notice?

In general we can divide by any 10-adic integer whose units digit is 1, 3, 7, or 9, using a sort of long division process (which is just as tedious for 10-adic numbers as it is for real numbers).

What about square roots? Here we run into a complication: a 10-adic integer can have more than 2 square roots, which is rather tiresome. The problem is that it is possible to have $ab = 0$ even if a and b are both nonzero. In fact we saw an example at the beginning of this talk: we found a number with $x^x = x$ but $x \neq 0, 1$, so $x(x-1) = 0$ and both factors are nonzero. This means that 1 has at least 4 square roots, because as well as 1 and -1 we also get $\cdots 357418751^2 = (2x-1)^2 = 1$.

This problem can be traced back to the fact that the integers mod 10 have zero divisors ($ab = 0$ but $a \neq 0, b \neq 0$), which in turn is due to the fact that 10 has more than 1 prime factor. This suggests that instead of using 10-adic numbers, we will get a better theory by looking at p-adic numbers for a prime p.

2 p-adic numbers

We construct the p-adic numbers for p a prime 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. In other words, if a and b are nonzero p-adic integers then so is ab. To see this look at the rightmost nonzero digits of a and b. The product of these mod p is nonzero as p is prime, and is the rightmost nonzero digit of ab.

What about unique factorization into primes for p-adic integers? Recall that every nonzero integer has a factorization into primes and units that is unique up to units and order. For p adics the same is true but much simpler because there is only one prime (p of course). In fact any nonzero p-adic integer is a power of p times something with nonzero units digit, and the p-adic integers with nonzero units digit all have inverses.

Example: the 2-adic integer $101000_2 = 10_2^3 \times 101_2$ (where 10_2 means 2.

The p-adic numbers. We can also invert p is we allow digits after the decimal (p-adic?) point, because $\cdot 1 = 1/p$, just as in base p. We call something with an infinite number of digits before the point and a finite number after a p-adic number (rather than integer). So any nonzero p-adic number n has an inverse $1/n$. We say the p-adic numbers form a field, because they have the 4 operations $+$, -, $\times$, $/$.

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 $7 = 21_3$ as $\cdots 0111$ by finding the digits one by one. (There are much faster ways of course, such as Newton's method.)

Exercise 2.1. Find the first three digits of the square root of ten 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 2.2. (Easy) Find the first few digits of $\sqrt{17}$ in the 2-adic integers. (Hard) Show that a 2-adic integer that is a unit has a square root if and only if its last 3 digits are 001.

3 Sequences 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 $|x|_\infty$. For a p-adic number we define the size $|x|_p$ to be p^n where $p^n x$ is a unit. (And $|0|_p = 0$.) So the number p^n for n large is a large real number but a small p-adic number.

Exercise 3.1. Show that $|xy|_p = |x|_o |y|_p$.

Exercise 3.2. Show that if x is a rational number then the product of all the numbers $|x|_p$ for p a prime or infinity is 1. (Hint: first prove it for primes.)

For real numbers we can define the distance $d(x, y)$ between them to be $|x - y|_\infty$ and this satisfies the inequality $d(x, z) \leq d(x, y) + d(y, z)$. For p-adics, we can define distance as $d(x, y) = |x - y|_p$.

Exercise 3.3. Show that $d(x,z) \leq d(x,y) + d(y,z)$ for p-adic numbers. Better still, show that $d(x,z) \leq \max(d(x,y), d(y,z))$.

For real numbers, convergence of a series can be very tricky. For example, the series $1 + 1/2 + 1/3 + \cdots$ does not converge even though the terms tend to 0, while the sum of the series $\log(2) = 1 - 1/2 + 1/3 - \cdots$ 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 $1 + x + x^2 + \cdots$ converges p-adically if $|x|_p < 1$.

We can now try to define exponential functions and logarithms of p-adic numbers. Logarithms are a bit easier so we do these first. We recall that for the reals,

$$\log(1+x) = x - x^2/2 + x^3/3 - \cdots$$

at least if $|x|_\infty < 1$ which is needed to make the series converge. For example, we can work out the 2-adic log of 3 to 3 significant figures as $2 - 2^2/2 + 2^3/3 - 2^4/4$.

For the real numbers we have the exponential function

$$\exp(x) = e^x = 1 + x + x^2/2! + x^3/3! + \cdots$$

The p-adic exponential function is a bit more complicated. The number e is not defined, so we try to use the exponential series. At first sight convergence seems easy because the numbers $1/n!$ look very small. However they are in fact rather large p-adically!

Example: We calculate exp(3) is the 3-adic integers as $1+3+3^2/2+3^3/6+....$ In "base 3" this is $1 + 10 + \cdots 1111200 + \cdots 1111200 + \cdots = \cdots 111$.

Exercise 3.4. Find the next two digits of exp(3) in the 3-adic integers.

To study when exp converges we need to know how many times p divides $n!$. This is given by $[n/p] + [n/p^2] + [n/p^3] + \cdots$, where x is the integer part of x. This sum is at most $n/(p-1)$.

Exercise 3.5. Show that if p is an odd prime then $\exp(x)$ converges if x is divisible by p. What happens if $p = 2$?

The log and exp functions obey most of the usual rules at least when they are defined; for example, $\exp(a+b) = \exp(a)\exp(b)$. One way to define powers is by $a^b = \exp(b \log a)$, at least for a close to 1 and b close to 0.

Exercise 3.6. The Bessel function $J_0(x)$ can be defined as

$$J_0(x) = 1 - (x/2)^2/1!^2 + (x/2)^4/2!^2 - (x/2)^6/3!^2 + \cdots$$

When does this converge for x real? What about for x a p-adic integer for p odd?

4 The p-adic Gamma function

The gamma function is more or less the same as the factorial function except for a change of variable: $\Gamma(n+1) = n!$. Euler found a way to extend it to positive real numbers x.

$$\Gamma(x) = \int_0^\infty e^{-t} t^{x-1} dt$$

Exercise 4.1. Prove that $\Gamma(x+1) = x\Gamma(x)$ (hint: integrate by parts). Prove that $\Gamma(1) = 1$. Prove that $\Gamma(n+1) = n!$ when n is a positive integer (hint: induction).

Can we find a p-adic factorial or gamma function? Let's try to define a factorial function from $\mathbb{Z}/p\mathbb{Z}$ to $\mathbb{Z}/p\mathbb{Z}$. This is a complete flop because $n! \equiv 0 \bmod p$ for $n \geq p$.

Try again. The problem is the numbers divisible by p, so we just miss them out and try defining $n!_p$ to be the product of all numbers from 1 to n that are not divisible by p. For example, if $p = 5$ then the values for this mod 5 are

$$1, 1, 2, 1, 4, 4, 4, 3, 4, 1, 1, 1, 2, 1, 4, 4, 4, 3, 4, ...$$

This is much better but still not quite right: it is periodic, but the period is 10 not 5. Looking more closely we see that if we add 5 to n we change the sign of $n!_5$. This is easy to fix: we just put in a factor of $(-1)^n$. So $(-1)^n n!_5$ is well defined mod 5 if n is defined mod 5.

The key point that made this work it that the product of all numbers 1, 2, 3, 4 is -1 mod 5. The same works for any ODD prime power p^k: the product of all numbers from 1 to p^k not divisible by p is $-1 \bmod p^k$. This is called Wilson's theorem, and shows that $(-1)^n n!_p$ is well defined mod p^k and so gives a function from p-adic integers to p-adic integers.

We can prove Wilson's theorem by observing that all the numbers from 1 to $p^k - 1$ not divisible by p pair off into pairs a, b with $ab \equiv 1 \bmod p^k$, except for the numbers ± 1 with square 1.

Exercise 4.2. (Easy) What happens if you try to use Wilson's theorem for $p^k = 2^3$? In other words what is the product of all odd numbers from 1 to 7 mod 2^3? How many solutions of $x^2 \equiv 1 \bmod 2^3$ are there? (Hard) Can you think of a way to define a 2-adic factorial?

Further reading.

Borevich and Shafarevich, Number theory.

J.-P. Serre, A course in arithmetic

N. Koblitz, p-adic numbers, p-adic analysis and zeta functions. This discusses more advanced topics such as p-adic integration and p-adic analogs of the Riemann zeta function.