THE P-ADIC NUMBER CIRCLE

I. EQUATIONS

You are probably already familiar with these number systems, each of which is included in the next:

- $\mathbb{N} =$ the NATURAL NUMBERS $0, 1, 2, 3, 4, \dots$
- $\mathbb{Z} =$ the INTEGERS $\dots, -3, -2, -1, 0, 1, 2, 3, \dots$
- $\mathbb{Q} =$ the RATIONAL NUMBERS $\frac{a}{b}$ (with a&b integers, and $b \neq 0$)
- $\mathbb{R} =$ the REAL NUMBERS, i.e. the entire continuum of numbers with decimal expansions like

  $$3.14159265358979323846264338327 9\dots$$

  which make up the number line:

One thing you can do with numbers is to solve equations. People have long been intrigued by equations with integer coefficients whose solutions are sought for in integers (or rational numbers). These are called DIOPHANTINE EQUATIONS, and I'll bet you all know at least one:

$$x^2 + y^2 = z^2.$$

Even in natural numbers it has infinitely many solutions, the simplest few being

$$(x, y, z) \ = \ (0, 0, 0), \ (3, 4, 5), \ (5, 12, 13)$$

Problem 1. Can you find the next? (Rather than plugging and chugging, try to find a pattern in the differences of squares $1^2, 2^2, 3^2, 4^2, \dots$ and use that to avoid computation altogether!)

Another famous example is PELL'S EQUATION

$$x^2 - 5y^2 = \pm 4.$$

Problem 2. Find all the solutions to Pell's equation with x and y natural numbers! Start by remembering the Fibonacci sequence. Plug those numbers in for y, and try to find a pattern for the numbers that work for x.

Next for some infamous Diophantine equations: first, there is FERMAT'S EQUATION

$$x^n + y^n = z^n \quad (n \geq 3)$$

which was proved insoluble in rational numbers (except for $(x, y, z) = (0, 0, 0)$) in 1995 by ANDREW WILES. Then, there is the equation

$$x^2 = 2,$$

which the Pythagoreans (ca. 500 BC) already knew can't be solved by a rational number.[1]

Indeed, if we had integers a and b with

$$\boxed{\left(\frac{a}{b}\right)^2 = 2},$$

then we can assume there is no prime number dividing them both. (Otherwise, just divide it out – this doesn't affect the fraction $\frac{a}{b}$.) Multiplying both sides by b^2 gives

$$a^2 = 2 \cdot b^2,$$

so that a^2 is even. Since the square of an odd number is odd, a itself must be even. Therefore $a = 2 \cdot c$ for some integer c, and our equation becomes

$$4 \cdot c^2 = 2 \cdot b^2.$$

Dividing through by 2,

$$2 \cdot c^2 = b^2$$

tells us as before that b must be even. But then a and b are both divisible by the prime number 2, in contradiction to our assumption. So the boxed equation cannot hold.

The real numbers give one enlargement of the rational numbers in which one can solve $x^2 = 2$. Since this solution

$$x = \sqrt{2} = 1.414213562373095\ldots$$

is not in $\mathbb{Q}$, we say that it is IRRATIONAL. In fact $\mathbb{R}$ is not the only enlargement of $\mathbb{Q}$ containing a square root of 2. For each prime number p, there is a continuum of numbers with "p-adic expansions" and (roughly speaking) making up a number *circle*. For some (but not all) choices of p, these "p-adic numbers" contain a solution to $x^2 = 2$. They have been around for a while, since their invention by KURT HENSEL in the mid-1890's, but haven't been popularized. Though we won't get into this today, they are very useful to mathematicians – for instance, in deciding when certain equations can be solved over $\mathbb{Q}$.

[1] Apparently, this upset them so much that they decided it must be hidden from the public, along with the dodecahedron.

II. Modular arithmetic

For each natural number $n \geq 2$, there is a very small number system:

$$\mathbb{Z}/n\mathbb{Z} = \{0, 1, 2, \ldots, n-1\},$$

called the “integers mod n”. To add, multiply, or subtract two “integers mod n”, just do it as you would normally . . . then add or subtract n enough times until your answer is in $\mathbb{Z}/n\mathbb{Z}$.

For example,in $\mathbb{Z}/7\mathbb{Z}$,

$$4 \cdot 4 = 16 \overset{(7)}{\equiv} 2.$$

The “$\overset{(7)}{\equiv}$” means “equals mod 7”; it’s there so that you don’t have to write “$16 = 2$”, which would just feel too strange.

Problem 3. Try multiplying $3 \cdot 4$ in $\mathbb{Z}/5\mathbb{Z}$, in $\mathbb{Z}/6\mathbb{Z}$, in $\mathbb{Z}/7\mathbb{Z}$, and in $\mathbb{Z}/8\mathbb{Z}$. What do you notice?

In order to be able to divide in a number system, we can’t have products of nonzero numbers giving zero. If $a \cdot b = 0$, with $b \neq 0$, division by a cannot even be possible: you would face the contradiction

$$b = \frac{a \cdot b}{a} = \frac{0}{a} = 0.$$

As you can see, when n isn’t prime, this is a problem; so we usually let n be a prime p.

For instance, let $p = 7$. In $\mathbb{Z}/7\mathbb{Z}$, $3 \cdot 5 = 15 \overset{(7)}{\equiv} 1$ and so we say that 5 is “$\frac{1}{3}$”.

Problem 4. What is $\frac{1}{3}$ in $\mathbb{Z}/11\mathbb{Z}$? in $\mathbb{Z}/5\mathbb{Z}$?

We denote by $(\mathbb{Z}/p\mathbb{Z})^*$ the $p-1$ nonzero elements $\{1, 2, \ldots, p-1\}$.

Problem 5. What elements of $(\mathbb{Z}/3\mathbb{Z})^*$, $(\mathbb{Z}/5\mathbb{Z})^*$, $(\mathbb{Z}/7\mathbb{Z})^*$ are squares? On the basis of your results, what proportion of elements of $(\mathbb{Z}/p\mathbb{Z})^*$are squares in general?

III. OINK?

Well, you know that the real numbers are those with a decimal expansion

$$c_2 c_1 c_0 . c_{-1} c_{-2} c_{-3} c_{-4} \ldots$$

where the c_i are integers between 0 and 9 called DIGITS. The expansion can go on forever to the right, but *always terminates to the left*. If you prefer, you can write this number as

$$c_2 \cdot 10^2 + c_1 \cdot 10 + c_0 + \frac{c_{-1}}{10} + \frac{c_{-2}}{10^2} + \frac{c_{-3}}{10^3} + \frac{c_{-4}}{10^4} + \cdots .$$

We could also do numbers in a different "base" than 10 – for instance, base p for p a prime. (Maybe you've even done this before, in school or in another math circle.)

But that's not what we're going to do. What we are going to do is rather bizarre. We're going to consider "numbers" which *terminate to the right*, like

$$\ldots a_3 a_2 a_1 a_0 . a_{-1} a_{-2}$$

$$= \frac{a_{-2}}{p^2} + \frac{a_{-1}}{p} + a_0 + a_{-1} \cdot p + a_{-2} \cdot p^2 + a_{-3} \cdot p^3 + \cdots ,$$

where the a_i are integers between 0 and $p-1$ called (...ahem) PIGITS. These numbers are the p-ADIC RATIONALS and the collection of all of them is denoted $\mathbb{Q}_p$. Multiplication and addition take place in essentially the same way, by "carrying to the left" (which *can now go on forever*). That's the general idea. But now let's be a little more careful and work with a more manageable set of p-adic numbers.

IV. The p-adic integers

Let p be a prime number, like $2, 3, 5, 7$, etc. We define $\mathbb{Z}_p$ to consist of the formal infinite sums

$$a_0 + a_1 \cdot p + a_2 \cdot p^2 + a_3 \cdot p^3 + \cdots$$

with each pigit a_i between 0 and $p-1$ (inclusive). “Formal” here means “don't add it up”. The sums can be infinite or finite.

Inside $\mathbb{Z}_p$ are all the natural numbers $\mathbb{N}$. In fact, they are exactly the p-adic integers given by finite sums. For instance, 37 is a natural number; we would like to express it in $\mathbb{Z}_5$. Writing “p” for 5 to resist the urge to “add it all up”, we just need to find a_0, a_1, a_2, etc. so that

$$\text{(I)} \quad \boxed{37 = a_0 + a_1 \cdot p + a_2 \cdot p^2 + \cdots .}$$

Considering both sides “mod $p\,(= 5)$”,[2] we find

$$2 = a_0.$$

Subtracting this from equation (I) gives

$$\text{(II)} \quad \boxed{35 = a_1 \cdot p + a_2 \cdot p^2 + \cdots .}$$

Taking this “mod $p^2 (= 25)$” yields

$$10 = a_1 \cdot p.$$

So $a_1 = 2$, and subtracting this from equation (II) we've got

$$25 = a_2 \cdot p^2.$$

Hence $a_2 = 1$, and we have shown that

$$2 + 2 \cdot p + p^2$$

expresses 37 as an element of $\mathbb{Z}_5$.

[2] In $\mathbb{Z}/p\mathbb{Z}$, $p \overset{(p)}{\equiv} 0$; so this has the effect of chopping everything after a_0 off on the right-hand side of boxed equation (I).

Problem 6. Express 37 in $\mathbb{Z}_3$. Then plot it on the "3-adic number circle" below. (You're welcome to do this with other natural numbers – be my guest!)[3]

[3] But what ever you do, *don't try to add p-adic numbers on the circle!* It's a cute way of arranging them, but adding distances (from zero) doesn't work. Maybe you can demonstrate this!

V. ADDING AND MULTIPLYING

You have two p-adic integers

$$\alpha = a_0 + a_1 \cdot p + a_2 \cdot p^2 + \cdots$$

$$\beta = b_0 + b_1 \cdot p + b_2 \cdot p^2 + \cdots$$

and would like to add them. (Well, you personally may not like to add them, but I want you to.) The problem if you just write

$$(a_0 + b_0) + (a_1 + b_1) \cdot p + (a_2 + b_2) \cdot p^2 + \cdots$$

is that the pigits $(a_i + b_i)$ won't always be less than p. So you have to "carry", a process with which you are well acquainted from adding natural numbers.

For instance, sticking for the moment with finite expansions, if $p = 5$ and

$$\alpha = 2 + 2 \cdot p + p^2$$

$$\beta = 4 + 3 \cdot p$$

then

$$\alpha + \beta = (2 + 4) + 2 \cdot p + 3 \cdot p + p^2$$

$$= 1 + (1 + 2 + 3) \cdot p + p^2$$

$$= 1 + p + (1 + 1) \cdot p^2$$

$$= 1 + p + 2 \cdot p^2.$$

As you can check, we have just added $37 + 19 = 56$, but in 5-adic notation.

Problem 7. Try $\alpha \cdot \beta$ in $\mathbb{Z}_5$, with the same numbers α and β.

Now for an example with infinite expansions. You may be surprised by the answer.

Problem 8. Let $p = 3$. Try adding (in $\mathbb{Z}_3$) $\alpha = 1$ to

$$\beta = 2 + 2 \cdot p + 2 \cdot p^2 + 2 \cdot p^3 + 2 \cdot p^4 + \cdots$$

.

VI. Subtracting and dividing

The last problem raises the question: how do you find "$-\alpha$"? Since we already know how to write all natural numbers as p-adic integers, this will tell us how to express all integers p-adically, demonstrating that "$\mathbb{Z}$ is included in $\mathbb{Z}_p$".

With $p = 3$, consider

$$\alpha = 1 + p^2 + p^3;$$

we want

$$\beta = b_0 + b_1 \cdot p + b_2 \cdot p^2 + b_3 \cdot p^3 + \cdots$$

(with each pigit $b_i = 0,\ 1,$ or 2) such that

$$(*)\quad \boxed{\alpha + \beta = 0}$$

in $\mathbb{Z}_3$. The idea for solving this is to "solve it modulo all powers of p". To do this, we should actually substitute in 3 for p:

(*) mod 3: $1 + b_0 \overset{(3)}{\equiv} 0 \quad\Longrightarrow\quad b_0 = 2$

(*) mod 9: $3 + b_1 \cdot 3 \overset{(9)}{\equiv} 0 \quad\Longrightarrow\quad 1 + b_1 \overset{(3)}{\equiv} 0 \quad\Longrightarrow\quad b_1 = 2$

(*) mod 27: $9 + 9 + 9 \cdot b_2 \overset{(27)}{\equiv} 0 \quad\Longrightarrow\quad 2 + b_2 \overset{(3)}{\equiv} 0 \quad\Longrightarrow\quad b_2 = 1$

(*) mod 81: $27 + 27 + 27 \cdot b_3 \overset{(81)}{\equiv} 0 \quad\Longrightarrow\quad b_3 = 1$

and then $b_4 = b_5 = b_6 = \cdots = 2$. (There are some steps to fill in.) So

$$-\alpha = 2 + 2 \cdot p + p^2 + p^3 + 2 \cdot p^4 + 2 \cdot p^5 + 2 \cdot p^6 + \cdots .$$

So I've done subtraction; your job is to divide!

Problem 9. ($p = 5$) Recall $\alpha = 2 + 2 \cdot p + p^2$ expresses "37" in $\mathbb{Z}_5$. Express $\frac{1}{37}$ in $\mathbb{Z}_5$ by writing $\beta = b_0 + b_1 \cdot p + b_2 \cdot p^2 + \cdots$, demanding that

$$\alpha \cdot \beta = 1,$$

and using the same method as above. (Just try to find b_0 and b_1, maybe b_2.)

It turns out that this worked because 37 isn't divisible by 5. To express all rational numbers p-adically, you need to allow $\frac{1}{p}$. So you'd be back where we started, at the p-adic rationals mentioned above.

VII. Square roots

Now you're ready to demonstrate conclusively that $\mathbb{Z}_p$ and $\mathbb{Q}_p$ contain "more" numbers than $\mathbb{Z}$ or $\mathbb{Q}$.

Problem 10. Let $p = 7$, and $\alpha = a_0 + a_1 \cdot p + a_2 \cdot p^2 + \cdots$. Start to solve $\alpha^2 = 2$ in $\mathbb{Z}_7$, by again going mod 7, mod 7^2, mod 7^3 to find a_0, a_1, a_2.

The next problem is more abstract, but more satisfying if you can master it.

Problem 11. To really see that a solution exists, suppose we know $\alpha_{n-1} = a_0 + a_1 \cdot p + \cdots + a_{n-1} p^{n-1}$ solving $\alpha_{n-1} \overset{(p^n)}{\equiv} 2$. Can you find a_n so that $\alpha_n = \alpha_{n-1} + a_n \cdot p^n$ solves $(\alpha_n)^2 \overset{(p^{n+1})}{\equiv} 2$? [Hint: $(\alpha_{n-1})^2 \overset{(p^{n+1})}{\equiv} 2 + k \cdot p^n$ for some k between 0 and 6.]

If you've made it this far, you can now say "$\sqrt{2}$ [an irrational number!] belongs to $\mathbb{Z}_7$". But not to $\mathbb{Z}_5$:

Problem 12. (a) ($p = 5$) Show that $\alpha^2 = 2$ has no solution in $\mathbb{Z}_5$. [Hint: it's enough to go mod 5.]
(b) On the other hand, can you solve $\alpha^2 + 1 = 0$ in $\mathbb{Z}_5$?

A number theorist once told me he thought tomorrow's kids would be raised on p-adics and find them every bit as natural as real numbers. What do you think?