p-adic numbers and non-archimedean world

M. Temkin

September 19, 2019

A puzzle

Problem. Find a four-digit number $\overline{xyzt}$ such that $\overline{xyzt} \cdot \overline{xyzt} = \overline{****xyzt}$.

Solution.

- The last digit satisfies $t \cdot t = 10 \cdot u + t$, hence $t \in \{0, 1, 5, 6\}$.
- It turns out that for each such t there exists a unique z such that $\overline{zt} \cdot \overline{zt} = \overline{*zt}$, then there exists a unique y, etc. Prove this!
- In the end we get four candidates 0000, 0001, 0625 and 9376, but only 9376 is a four-digit number.
- The answer: 9376*9376=87909376.

Hint: for each t, we want

$$\overline{*zt} = (10 \cdot z + t)^2 = 100 \cdot z^2 + 20 \cdot z \cdot t + t^2 = \ldots + 20 \cdot z \cdot t + 10 \cdot u + t.$$

So, $2 \cdot t \cdot z + u = \overline{*z}$ and $(2t - 1)z + u$ is divisible by 10. This determines z uniquely (why?). Similarly for y, etc.

Arithmetic

- Arithmetic studies numbers, especially 4 operations: $+, -, *, /$ Despite seeming simplicity it is one of the deepest areas of mathematics, called the Queen of Mathematics by Gauss.
- A famous example: Fermat claimed in 1637 that for any $n \geq 3$ the equation $x^n + y^n = z^n$ has only “trivial” rational (or integral) solutions, where $x = 0$, $y = 0$ or $z = 0$. This was finally proved only in 1994.
- A typical example of a problem: find all rational (or integral) solutions of a given polynomial equation (or a system).
- Such problems can be very difficult and even unsolvable. There are concrete systems which are provably(!) unsolvable.
- For comparison, there are algorithms to describe the set of all real solutions of such a system. Finding real solutions is much easier!

Fields

- In mathematics, a field is a set with elements $0, 1$, four arithmetic operations and all usual properties: $a(b+c) = ab + ac$, $0 \cdot a = 0$, etc. If only $+$, $-$, $*$ are defined, then the set is called a ring.
- For example: integral numbers only form a ring $\mathbb{Z}$. The minimal field containing $\mathbb{Z}$ is the set of all rational numbers $\mathbb{Q}$. Larger fields are the sets of all real and complex numbers $\mathbb{R}$ and $\mathbb{C}$.
- Naturally, arithmetic "likes" to work with fields, for example, $\mathbb{Q}$. As we saw, it is often easier to solve problems in large fields.
- Only $\mathbb{R}$ and $\mathbb{C}$ are really important for physics, because our physical world (space, time) is continuous (at least in the first approximation).
- In arithmetic and mathematics there are other very important large fields, so-called non-archimedean ones.

Fields of residues

Example

Let $\mathbb{F}_2$ be the set of two elements $0, 1$, with all usual rules like $1 + 0 = 1$, $1 * 0 = 0$, and the strange rule $1 + 1 = 0$. This is a field!

- The real meaning of $\mathbb{F}_2$ is parity: 0="even", 1="odd". Rules make perfect sense and $\mathbb{F}_2$ reveals the arithmetic of residues modulo 2.
- For any $n \geq 1$ the set $\mathbb{Z}/n\mathbb{Z}$ of residues modulo n is a ring, but not always a field. E.g., in $\mathbb{Z}/10\mathbb{Z}$ one has $2 \neq 0$ and $5 \neq 0$, but $2 * 5 = 10 = 0$.
- In general, one cannot divide by 2 and 5 in $\mathbb{Z}/10\mathbb{Z}$. For example, $2 * 0 = 0 = 2 * 5$ and $2 * 1 = 2 = 2 * 6$ in $\mathbb{Z}/10\mathbb{Z}$.
- A $p > 1$ is prime if it has no divisors between 1 and p, e.g. 2,3,5,7,11,13,17,19,23,29....

Theorem

The ring $\mathbb{Z}/p\mathbb{Z}$ is a field (denoted $\mathbb{F}_p$) if and only p is prime.

Congruences

- Solving equations modulo p often provides valuable information, e.g. $x^2 - 3y^2 = 5$ has no solutions in $\mathbb{Z}$ because it has no solutions even in $\mathbb{F}_3$ (modulo 3). Check that x^2 is never 2 in $\mathbb{F}_3$.
- It is also useful to look for solutions modulo p^k. For example, $x^2 \in \{0, 1, 4\}$ in $\mathbb{Z}/8\mathbb{Z}$, hence $x^2 + y^2 + z^2 = 8m + 7$ has no solutions for any m.
- Typically, one finds all solutions modulo p, then lifts them modulo p^2, p^3, etc.
- In our puzzle we worked with $p = 10$ (which is not prime) and solved $x^2 = x$ modulo 10, 100, 1000, etc.
- In fact, we found 4 (!) series of solutions $x = \overline{\dots x_3 x_2 x_1 x_0}$:
  two trivial ones: 0 and 1,
  two strange ones: $\dots 0625$ and $\dots 9376$.

10-adic numbers

- Define the ring of 10-adic numbers $\mathbb{Q}_{10}$ to be the set of "numbers" finite to the left and infinite to the right (!):

$$x = \overline{\dots x_2 x_1 x_{0\bullet} x_{-1} \dots x_{-k}} = \frac{x_{-k}}{10^k} + \dots + \frac{x_{-1}}{10} + x_0 + 10x_1 + 100x_2 + \dots$$

  Where x_i are arbitrary digits from 0 to 9.
- $+, -, *$ are defined by usual arithmetic. Similarly to $\mathbb{Z}/10\mathbb{Z}$, the set $\mathbb{Q}_{10}$ is a ring, but not a field.
- For example, we have found 4 solutions of $x^2 = x$ in $\mathbb{Q}_{10}$: 0,1,$y = \dots 0625$ and $z = \dots 9376$. One has $y \neq 0$, $y - 1 \neq 0$, but $y(y-1) = y^2 - y = 0$. So, $\mathbb{Q}_{10}$ is not a field.

p-adic numbers

- Why not to replace 10 by any $n > 1$? For example, in programming one represents numbers in base-2 or base-16 system.
- For any $n > 1$ define the ring of n-adic numbers $\mathbb{Q}_n$ to be the set of base-n numbers finite to the left and infinite to the right (!):

$$x = \overline{\ldots x_2 x_1 x_{0\bullet} x_{-1} \ldots x_{-k}} = \frac{x_{-k}}{n^k} + \ldots + \frac{x_{-1}}{n} + x_0 + x_1 n + x_2 n^2 + \ldots$$

  Where x_i are arbitrary digits from 0 to $n-1$.
- $+$, $-$, $*$ are defined by the usual base-n arithmetic, so $\mathbb{Q}_n$ is a ring. Similarly to $\mathbb{Z}/n\mathbb{Z}$, it is a field if and only if n is prime.
- From now on we only consider p-adic numbers with a prime p.

The p-adic absolute value

- Does the formal sum $x = \overline{\dots x_2 x_1 x_0} = x_0 + x_1 p + x_2 p^2 + \dots$ make sense?
- If $|p| < 1$, then yes! It converges as a geometric sequence!
- The <u>p-adic absolute value</u> $|\ |_p$ is chosen so that $|p|_p < 1 < |p^{-1}|_p$.
- The formula is very strange: any $x \in \mathbb{Q}$ can be presented as $x = \pm p^k \frac{a}{b}$ with a, b prime to p and then $|x|_p = p^{-k}$.
- The absolute value is <u>non-archimedean</u>: $|n|_p \leq 1$ for any integral n.
- Nevertheless, $|xy|_p = |x|_p |y|_p$ and it satisfies the strong triangle inequality $|x+y|_p \leq \max(|x|_p, |y|_p) \leq |x|_p + |y|_p$.
- Exercise: deduce that any point in the p-adic disc of radius r around x is a center of the disc.

Advertisement

- Similarly to the reals $\mathbb{R}$, the field of p-adic numbers $\mathbb{Q}_p$ is a completion of $\mathbb{Q}$ – any reasonable (Cauchy) sequence from $\mathbb{Q}$ converges to an element in $\mathbb{Q}_p$. In particular, one can study analysis in $\mathbb{Q}_p$ as over the reals!
- It is easier to do arithmetic in $\mathbb{Q}_p$ – no signs needed, and no double presentations like $1.0 = 0.99999\dots$ show up.
- For example, $-1 = \dots 11111$ in $\mathbb{Q}_2$ because $1 + 2 + 4 + \dots = \frac{1}{1-2} = -1$. What is -1 in $\mathbb{Q}_5$?

Example

Real roots can be computed by $\sqrt{1+t} = 1 + \frac{1}{2}t - \frac{1}{8}t^2 + \frac{1}{16}t^3 - \dots$ when $|t| < 1$. The same formula allows to compute roots in $\mathbb{Q}_p$. The most subtle (but not too difficult) case is $\mathbb{Q}_2$. For example, $|16|_2 = \frac{1}{16}$ and $\sqrt{17} = 1 + 8 - 32 + 256 - \dots$ converges in $\mathbb{Q}_2$, but $\sqrt{5}$ does not exist in $\mathbb{Q}_2$ ($|4|_2$ is not small enough and $1 + 2 - \frac{1}{2} + 4 - \dots$ diverges).

Two famous theorems

- Are these *p*-adic numbers so natural? Yes!
- Can one find zillions other strange completions and absolute values? No!

Theorem (Ostrowski)

The usual and p-adic absolute values are the only absolute values on $\mathbb{Q}$ *(up to equivalence), and* $\mathbb{R}$ *and* $\mathbb{Q}_p$ *are the only completions of* $\mathbb{Q}$.

Solving polynomial equations in $\mathbb{R}$ and all $\mathbb{Q}_p$ can be done effectively (there are algorithms). In ideal situations, this tells us a lot about rational solutions. Here is the most famous example:

Theorem (Hasse-Minkowski)

A quadratic equation (like $x^2 + 3xy - 2x - 5yz + 7z^2 = 2019$*) has a solution in* $\mathbb{Q}$ *if and only if it has solutions in each* $\mathbb{Q}_p$ *and in* $\mathbb{R}$.

Conclusions

- *p*-adic numbers are as central for number theory as real numbers. There even are computations of certain numbers (rational or algebraic) via *p*-adic approximations, which work better/faster than computations via real approximations.
- Many areas of mathematics, such as analysis, dynamics, etc., were developed both for real and *p*-adic numbers.
- For a mathematician, there is no doubt that *p*-adic numbers are very natural and useful "god given" objects of the "mathematical world".
- Physics is based on real numbers. Probably, number theory and *p*-adic numbers will never be essentially used to study our "physical world".
- Nevertheless, there are applications to "real life" – computer science and cryptography.