Unreal Numbers

The story of *p*-adic numbers

Jacqui Ramagge

1 July 2008
UOW Maths Teachers' Day

The Rational Basics

We can go from $\mathbb{N}$ to $\mathbb{Q}$ in one of two ways

$$\begin{tikzcd} & (\mathbb{N},+,\cdot) \arrow[dl, "-"'] \arrow[dr, "\div"] & \\ (\mathbb{Z},+,\cdot) \arrow[dr, "\div"'] & & (\mathbb{Q}^{\geq 0},+,\cdot) \arrow[dl, "-"] \\ & (\mathbb{Q},+,\cdot) & \end{tikzcd}$$

but either way we end up at the same place.

The Real Basics

The field $(\mathbb{Q},+,\cdot)$ is determined by $\mathbb{N}$ and its arithmetic.

The transition from $\mathbb{N}$ to $\mathbb{Q}$ is algebraic in nature.

The construction of $(\mathbb{R},+,\cdot)$ requires more than arithmetic.

We use a concept of distance to talk about limits.

The transition from $\mathbb{Q}$ to $\mathbb{R}$ is analytic in nature.

Ingredients for $\mathbb{R}$

To construct $\mathbb{R}$ from $\mathbb{N}$ we use addition, multiplication and the Euclidean metric where $d(x,y) = |x-y|$.

Different metrics produce different structures.

The Euclidean metric on $\mathbb{R}$ links the notion of distance to the notion of a magnitude, namely the absolute value.

p-adic absolute value

Fix a prime p. Each $x \in \mathbb{Q}$ has a unique expression of the form

$$x = \frac{a}{b}p^k \text{ with } a, b, k \in \mathbb{Z}, \text{ and } a, b, p \text{ all pairwise coprime.}$$

Define $|x|_p = p^{-k}$ in this case.

Example

If $p = 5$ then

1. $|5|_5 = 5^{-1}$, $|25|_5 = 5^{-2}$, $|\frac{1}{125}|_5 = 5^3 = 125$,
2. $|3|_5 = 5^0 = 1$, $|4|_5 = 1$, $|7|_5 = 1$, $|\frac{12}{7}|_5 = 1$,
3. $|\frac{60}{7}|_5 = |\frac{12}{7} \cdot 5|_5 = 5^{-1}$,and $|15|_5 = |3 \cdot 5|_5 = 5^{-1}$.

We call the map $|\cdot|_p : \mathbb{Q} \to \mathbb{R}$ the p-adic absolute value.

p-adic numbers

Use the p-adic absolute value to construct the p-adic ultrametric by defining

$$d_p(x, y) = |x - y|_p \quad \text{for} \quad x, y \in \mathbb{Q}.$$

Definition

The completion of $\mathbb{Q}$ with respect to the metric d_p is the set $\mathbb{Q}_p$ of *p-adic numbers*.

In other words, $\mathbb{Q}_p$ is the set of all "numbers" we can get arbitrarily close to using rationals under the p-adic definition of distance.

Note: $\sum_{n=1}^{\infty} 5^n = 5 + 5^2 + 5^3 + 5^4 + \cdots$ is a 5-adic number!

what is it?

What do p-adic numbers look like?

Every p-adic number has an expression of the form

$$\sum_{n=N}^{\infty} a_n p^n \quad \text{with} \quad a_i \in \{0, 1, \ldots, p-1\}, N \in \mathbb{Z}$$

called its *p-adic expansion*.

An example if $p > 5$ could be

$$2p^{-3} + p^{-2} + 4p^{-1} + 1 + 2p + 4p^2 + p^4 + \cdots$$

Contrast this to a decimal expansion of a number in terms of decreasing powers of 10, eg

$$2 \cdot 10^3 + 10^2 + 4 \cdot 10^1 + 1 + 2 \cdot 10^{-1} + 4 \cdot 10^{-2} + 10^{-4} + \cdots$$

(Note these expressions represent different numbers.)

What do p-adic numbers look like?

The p-adic expansion of a natural number is related to its expression in base p.

The 5-adic expansion of 198 is $\quad 3 + 4 \cdot 5 + 2 \cdot 5^2 + 1 \cdot 5^3$

What about -1? Or $\frac{1}{4}$?

The p-adics are a completion of $\mathbb{Q}$; every rational number is in $\mathbb{Q}_p$ and has a p-adic expansion. Challenge

What do p-adic numbers look like?

Whatever it looks like, -1 should satisfy $1 + (-1) = 0$.
For example, the 5-adic expansion of -1 is

$$\sum_{n=0}^{\infty} 4 \cdot 5^n = 4 + 4 \cdot 5 + 4 \cdot 5^2 + \cdots$$ Why?

Note that $-1 + \frac{4}{5} = -\frac{1}{5}$ is therefore

$$\sum_{n=-1}^{\infty} 4 \cdot 5^n = 4 \cdot 5^{-1} + 4 + 4 \cdot 5 + 4 \cdot 5^2 + \cdots$$

even though $\frac{1}{5} = 1 \cdot 5^{-1}$.

What is the 5-adic expansion of $\frac{1}{4}$? It should satisfy $4 \times \frac{1}{4} = 1$.

$$4 + \sum_{n=1}^{\infty} 3 \cdot 5^n = 4 + 3 \cdot 5 + 3 \cdot 5^2 + 3 \cdot 5^3 + \cdots$$ Why?

● $\mathbb{Q}_p \neq \mathbb{R}$

How do you know where to start?

The p-adic absolute value can be extended to $\mathbb{Q}_p$ and

$$\left| \sum_{n=N}^{\infty} a_n p^n \right|_p = p^{-N}.$$

If $x \in \mathbb{Q}$ has p-adic absolute value $|x|_p = p^k$ then

$$x = \sum_{n=-k}^{\infty} a_n p^n \quad \text{with} \quad a_i \in \{0, 1, \ldots, p-1\}.$$

To calculate the 5-adic expansion of $\frac{27}{250}$ we first calculate

$$\left| \frac{27}{250} \right|_5 = \left| \frac{3^3}{2} \cdot \frac{1}{5^3} \right|_5 = 5^3$$

so its 5-adic expansion begins at 5^{-3}.

Is $\mathbb{Q}_p$ just a complicated way of writing real numbers?

Since $\sqrt{p} \notin \mathbb{Q}_p$ we know $\mathbb{Q}_p$ does not contain all real numbers.

However, $\mathbb{Q}_p$ contains square roots of -1 whenever -1 is a square modulo p. For example

$$-1 \equiv 9 \mod 5$$

and in $\mathbb{Q}_5$ the number

$$\begin{aligned} i &= 2 + 1 \cdot 5 + 2 \cdot 5^2 + 0 \cdot 5^3 + 0 \cdot 5^4 + 1 \cdot 5^5 + 3 \cdot 5^6 + \\ &\quad + 1 \cdot 5^7 + 0 \cdot 5^8 + 0 \cdot 5^9 + 2 \cdot 5^{10} + 1 \cdot 5^{11} + \cdots \end{aligned}$$

has square -1.

Other examples exist when -1 is not a square modulo p.

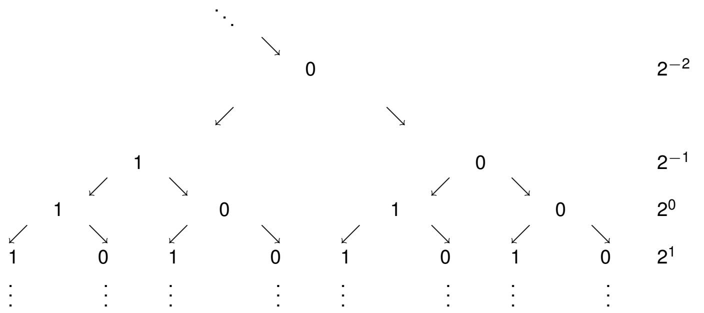
see examples

So $\mathbb{Q}_p$ is not a subset of $\mathbb{R}$.

Who needs $\mathbb{Q}_p$?

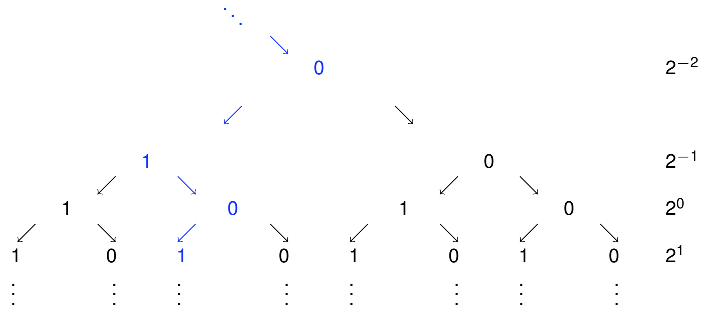
The p-adic numbers find applications in network analysis because they are associated to symmetries of certain graphs.

Eg $\mathbb{Q}_2$ acts on a homogeneous tree of valency 3;



$\mathbb{Q}_2$ and a tree

Each element of $\mathbb{Q}_2$ corresponds to an infinite path in this tree.
Eg, a 2-adic number beginning $1 \cdot 2^{-1} + 0 \cdot 2^0 + 1 \cdot 2^1 + \cdots$ looks a bit like



Action of $\mathbb{Q}_p$ on a tree

In this way we identify each of the "ends" of the tree at the bottom of such a picture with a p-adic number.

When you multiply two p-adic numbers together you get another p-adic number.

Given a fixed $x \in \mathbb{Q}_p$, multiplication by x represents a symmetry of the infinite paths in this tree and hence of the tree itself.

This is how they arise in my research.

Any Questions?

Thank you for your attention.

References

Introductory texts:

F. Quadros, *p-adic Numbers: An Introduction*, Springer 2003.

F. Gouvea, *p-adic Numbers: An Introduction*, Springer 1993.

Extension texts:

A.M. Robert, *A course in p-adic Analysis*, Springer 2000.

J.W.S. Cassells, *Local Fields*, Springer 2003.

P. de la Harpe, *Topics in Geometric Group Theory*, UCP 2000.

A very comprehensive text (not for the faint-hearted!):

J-P. Serre, *A course in arithmetic*, Springer 1970.

Notions of distance

Definition

A *metric* on $\mathbb{Q}$ is a map $d : \mathbb{Q} \times \mathbb{Q} \to \mathbb{R}$ satisfying

1. $d(x,y) \geq 0$ and $d(x,y) = 0 \Leftrightarrow x = y$ (positivity)
2. $d(x,y) = d(y,x)$ (symmetry)
3. $d(x,z) \leq d(x,y) + d(y,z)$ (triangle inequality)

for all $x, y, z \in \mathbb{Q}$.

A metric on $\mathbb{Q}$ is an *ultrametric* if it satisfies the *ultrametric inequality*

$$d(x,z) \leq \max\{d(x,y), d(y,z)\} \quad \text{for all} \quad x, y, z \in \mathbb{Q}$$

which is stronger than the triangle inequality.

◂ $\mathbb{R}$ ◂ p-adic numbers

What is the 5-adic number $5 + 5^2 + 5^3 + \cdots$?

Suppose $x = \sum_{i=1}^{\infty} 5^n = 5 + 5^2 + 5^3 + \cdots$.

Then $x - 5 = 5x$.

So $4x = -5$.

From this we see $x = -\frac{5}{4}$.

◂ $\mathbb{Q}_p$

Recurring expansions

Prove the following result.

Theorem

The rational numbers are precisely the p-adic numbers with recurring p-adic expansions.

Note that terminating expansions are included in the statement by virtue of being recurring expansions which have recurring zeroes at the end.

◂ $\mathbb{Q}$ in $\mathbb{Q}_p$

Expansion of -1 in $\mathbb{Q}_5$

To see that the 5-adic expansion of -1 is

$$4 + 4 \cdot 5 + 4 \cdot 5^2 + 4 \cdot 5^3 + \cdots$$

consider what happens when you add 1 to it.

Firstly, $1 + 4 = 5 = 0 + 1 \cdot 5$ so the first term of the sum is 0 and we have to "carry" a 5.

Then $1 \cdot 5 + 4 \cdot 5 = 5 \cdot 5 = 0 \cdot 5 + 1 \cdot 5^2$ so the second term in the sum is 0 and we "carry" a 5^2.

A brief inductive argument shows that at the n^{th} step we are adding $1 \cdot 5^n$ to $4 \cdot 5^n$ to get 0 as the n^{th} term in the expansion and carry $1 \cdot 5^{n+1}$ to the next term; the limit of this process is 0. Note that the carry digits are actually getting smaller in magnitude each time because we are working in the 5-adics.

◂ -1 in $\mathbb{Q}_p$

Expansion of $\frac{1}{4}$ in $\mathbb{Q}_5$

What happens if you multiply $4+3\cdot 5+3\cdot 5^2+3\cdot 5^3+\cdots$ by 4?

Firstly, $4\times 4=16=1+15=1+3\cdot 5$ so the first term of the product is 1 and we have to "carry" $3\cdot 5$.

Then $4\times 3\cdot 5=12\cdot 5$ and $3\cdot 5+12\cdot 5=15\cdot 5=3\cdot 5^2$ so the second term in the sum is 0 and we "carry" $3\cdot 5^2$.

If the mixture of addition and multiplication in this process confuses you, consider what happens when you use a multiplication algorithm to calculate a product of two natural numbers with several digits each.

A brief inductive argument shows that, with the exception of the first step, at the n^{th} step we are multiplying $3\cdot 5^n$ by 4 to get $12\cdot 5^n$ and then adding $3\cdot 5^n$ to get 0 as the n^{th} term in the expansion with a "carry" of $3\cdot 5^{n+1}$ to the next term.

◂ $\frac{1}{4}$ in $\mathbb{Q}_p$

Why $\mathbb{Q}_p$ is not in $\mathbb{R}$

Even when $i\notin\mathbb{Q}_p$ we can find numbers in $\mathbb{Q}_p$ which can not be real.

Theorem

For every prime p the equation

$$x_1^2+x_2^2+x_3^2+x_4^2=-1$$

has a nontrivial solution in $\mathbb{Q}_p$*.*

So for each p there exist $x_1, x_2, x_3, x_4\in\mathbb{Q}_p$, not all of which are zero, satisfying the above equation; these can't be real.
A sum of squares in $\mathbb{R}$ is always positive.
This generalises the case of $i\in\mathbb{Q}_p$ because i is a solution to the equation $x^2=-1$.

◂ $\mathbb{Q}_p\neq\mathbb{R}$