

Formalizing the p -adic Numbers in Lean

Robert Y. Lewis

Vrije Universiteit Amsterdam

Logical Verification lecture 14



Motivation

A project at the VU: formalize modern results in number theory, in Lean.

- Develop comprehensive libraries that will help with many results.
- Target “research areas”/collections of moderate difficulty results, instead of single challenge theorems.
- Work on the system and automation alongside the formalizing.



Formalizing number theory

Number theory starts as “the study of \mathbb{Z} ” but quickly goes beyond this.

We need libraries for:

- computations on \mathbb{N} , \mathbb{Z} , \mathbb{Q} , \mathbb{R} : divisibility, modularity, factoring, arithmetic, inequalities, ...
- less familiar “number” structures, such as number fields, the *p -adic numbers*, ...
- univariate and multivariate polynomials, and related algebra and geometry
- special functions: Dirichlet series, modular forms, ...

Completions

The rational numbers

The rational numbers \mathbb{Q} are **incomplete**.

The sets

$$\{x \in \mathbb{Q} \mid x^2 < 2\}$$

$$\{x \in \mathbb{Q} \mid x^2 > 2\}$$

partition \mathbb{Q} , but both are open.

Alternatively: the sequence of rationals

1, 1.4, 1.41, 1.414, 1.4142, 1.41421, 1.414213, 1.4142135, 1.41421356, ...

does not converge to a rational.

Completing \mathbb{Q}

Definition.

A sequence $s : \mathbb{N} \rightarrow \mathbb{Q}$ is **Cauchy** if for every positive $\epsilon \in \mathbb{Q}$, there exists a number N such that for all $k \geq N$, $|s_N - s_k| < \epsilon$.

Intuition: a sequence is Cauchy if its entries eventually become arbitrarily close.

Definition.

Two sequences s and t are **equivalent**, written $s \sim t$, if for every positive $\epsilon \in \mathbb{Q}$, there exists an N such that for all $k \geq N$, $|s_k - t_k| < \epsilon$.

Intuition: two sequences are equivalent if they eventually become arbitrarily close to each other.

Completing \mathbb{Q}

Definition.

A sequence $s : \mathbb{N} \rightarrow \mathbb{Q}$ is **Cauchy** if for every positive $\epsilon \in \mathbb{Q}$, there exists a number N such that for all $k \geq N$, $|s_N - s_k| < \epsilon$.

Intuition: a sequence is Cauchy if its entries eventually become arbitrarily close.

Claim.

The sequence

$1, 1.4, 1.41, 1.414, 1.4142, 1.41421, 1.414213, 1.4142135, 1.41421356, \dots$

is Cauchy. Why?

The real numbers

We think of the real numbers \mathbb{R} as \mathbb{Q} plus points in the “gaps.”

Cauchy sequences identify these points.

Definition?

The set of **real numbers** \mathbb{R} is the set $\{s : \mathbb{N} \rightarrow \mathbb{Q} \mid s \text{ is Cauchy}\}$.

The real numbers

We think of the real numbers \mathbb{R} as \mathbb{Q} plus points in the “gaps.”

Cauchy sequences identify these points.

Problem!

Some Cauchy sequences identify the same “points.”

1, 1.4, 1.41, 1.414, 1.4142, 1.41421, 1.414213, 1.4142135, 1.41421356, ...

2, 1.5, 1.42, 1.415, 1.4143, 1.41422, 1.414214, 1.4142136, 1.41421357, ...

Quotients

Definition.

A binary relation is called an **equivalence relation** if it is reflexive, symmetric, and transitive.

Definition.

Let S be a set, \sim an equivalence relation on S , and $a \in S$. The **equivalence class** of a with respect to \sim , denoted $\llbracket a \rrbracket$, is the set $\{x \in S \mid a \sim x\}$. The **quotient** of S with respect to \sim , denoted S / \sim , is the set $\{\llbracket a \rrbracket \mid a \in S\}$.

The real numbers

Definition.

Two sequences s and t are **equivalent**, written $s \sim t$, if for every positive $\epsilon \in \mathbb{Q}$, there exists an N such that for all $k \geq N$, $|s_k - t_k| < \epsilon$.

Claim.

The relation \sim is an equivalence relation.

Definition.

The set of **real numbers** \mathbb{R} is the quotient of the set of rational Cauchy sequences, with respect to \sim . We call this the **completion** of \mathbb{Q} .

The real numbers

We define addition of sequences in the obvious way.

Claim.

If $r_1 \sim r_2$ and $s_1 \sim s_2$ then $r_1 + s_1 \sim r_2 + s_2$.

This lets us define addition on \mathbb{R} : $[[r]] + [[s]] = [[r + s]]$.

Similarly for multiplication, etc.

Question:

In the construction of \mathbb{R} , what was hardcoded? What can we abstract?

General completions

We can generalize the measure of distance.

Definition.

A sequence $s : \mathbb{N} \rightarrow \mathbb{Q}$ is **Cauchy** if for every positive $\epsilon \in \mathbb{Q}$, there exists a number N such that for all $k \geq N$, $|s_N - s_k| < \epsilon$.

General completions

We can generalize the measure of distance.

Definition.

A sequence $s : \mathbb{N} \rightarrow \mathbb{Q}$ is **Cauchy** with respect to an absolute value abs if for every positive $\epsilon \in \mathbb{Q}$, there exists a number N such that for all $k \geq N$, $\text{abs}(s_N - s_k) < \epsilon$.

Definition.

A function abs on \mathbb{Q} is a (generic) **absolute value** if it is

- positive-definite: $\text{abs}(0) = 0$ and $\text{abs}(k) > 0$ otherwise
- subadditive: $\text{abs}(x + y) \leq \text{abs}(x) + \text{abs}(y)$
- multiplicative: $\text{abs}(x \cdot y) = \text{abs}(x) \cdot \text{abs}(y)$

General completions

We can also generalize the base type from \mathbb{Q} to any metric space.

But we'll focus on \mathbb{Q} for today.

Absolute values on \mathbb{Q}

Definition.

A function abs on \mathbb{Q} is a (generic) **absolute value** if it is

- positive-definite: $\text{abs}(0) = 0$ and $\text{abs}(k) > 0$ otherwise
- subadditive: $\text{abs}(x + y) \leq \text{abs}(x) + \text{abs}(y)$
- multiplicative: $\text{abs}(x \cdot y) = \text{abs}(x) \cdot \text{abs}(y)$

Example.

The trivial absolute value on \mathbb{Q} is given by

$$|x|_0 = \begin{cases} 0 & x = 0 \\ 1 & x \neq 0 \end{cases}$$

The p-adic norm

The p -adic valuation

Fix a natural number $p > 1$.

Definition.

The p -adic valuation $v_p : \mathbb{Z} \rightarrow \mathbb{N}$ is defined by

$$v_p(z) = \max \{n \in \mathbb{N} \mid p^n \mid z\}$$

with $v_p(0) = \infty$ (or 0, we don't care for now).

This extends to $v_p : \mathbb{Q} \rightarrow \mathbb{Z}$ by setting

$$v_p(q/r) = v_p(q) - v_p(r)$$

when q and r are coprime.

The p -adic norm

$$v_p(z) = \max \{n \in \mathbb{N} \mid p^n \mid z\}$$

$$v_p(q/r) = v_p(q) - v_p(r)$$

Definition.

The p -adic norm $|\cdot|_p : \mathbb{Q} \rightarrow \mathbb{Q}$ is defined by

$$|x|_p = \begin{cases} 0 & x = 0 \\ \frac{1}{p^{v_p(x)}} & x \neq 0 \end{cases}$$

The p -adic norm

Examples.

x	$v_3(x)$	$ x _3$
1	0	1
3	1	$\frac{1}{3}$
6	1	$\frac{1}{3}$
18	2	$\frac{1}{9}$
$\frac{1}{3}$	-1	3
118098	10	$\frac{1}{59049}$
118099	0	1

The p -adic norm

When p is prime, the p -adic norm is an absolute value on \mathbb{Q} .

So we can complete \mathbb{Q} with respect to $|\cdot|_p$.

The result: the p -adic numbers \mathbb{Q}_p .

The p -adic numbers

The p -adic numbers

A real number in base 10 is

$$\pm \sum_{i=-\infty}^k a_i \cdot 10^i$$

where k is a (possibly negative) integer and each $a_i \in \{0, 1, \dots, 9\}$.

A p -adic number in base p is

$$\sum_{i=k}^{\infty} a_i \cdot p^i$$

where k is a (possibly negative) integer and each $a_i \in \{0, 1, \dots, p-1\}$.

The p -adic numbers

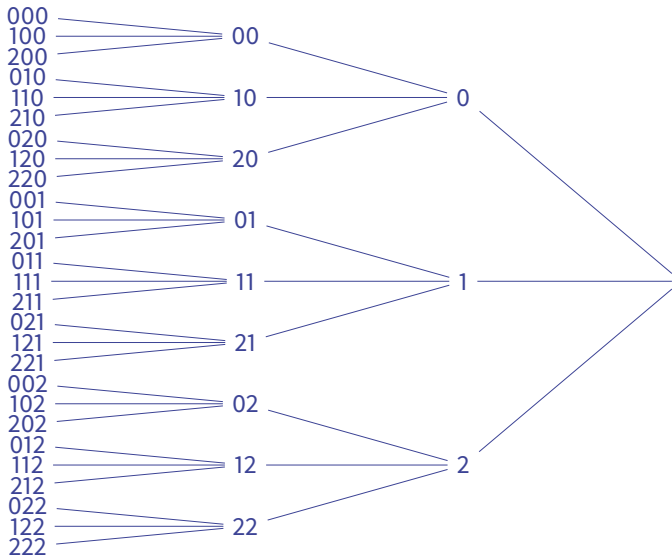
Arithmetic in \mathbb{Q}_5

$$\begin{array}{r} 1111111 \\ \dots 4444444 \\ + 1 \\ \hline 0 \end{array}$$

$$\begin{array}{r} 1212121 \\ \dots 3131313 \\ \times 3 \\ \hline 1 \end{array}$$

$$\begin{array}{r} 1111111 \\ \dots 3131313 \\ + 4444444 \\ \hline \dots 31313131 \end{array}$$

The p -adic numbers



Properties of the p -adic norm

The p -adic norm on \mathbb{Q} lifts to \mathbb{Q}_p .

(Reason: for any Cauchy sequence $s : \mathbb{N} \rightarrow \mathbb{Q}$, $|s_i|_p$ is eventually constant.)

Theorem.

The p -adic norms on \mathbb{Q} and \mathbb{Q}_p are **nonarchimedean**. That is, for all x and y ,

$$|x + y|_p \leq \max(|x|_p, |y|_p).$$

This simplifies many things in the study of \mathbb{Q}_p .

The p -adic integers

A consequence of the nonarchimedean property: if $|x|_p \leq 1$ and $|y|_p \leq 1$, then $|x + y|_p \leq 1$.

Definition.

The p -adic integers \mathbb{Z}_p are the set

$$\{z \in \mathbb{Q}_p \mid |z|_p \leq 1\}.$$

This set forms a ring.

Hensel's lemma

Let $\mathbb{Z}_p[X]$ denote the set of polynomials with coefficients in \mathbb{Z}_p .

Theorem.

Suppose that $f(X) \in \mathbb{Z}_p[X]$ and $a \in \mathbb{Z}_p$ satisfy $|f(a)|_p < |f'(a)|_p^2$. There exists a unique $z \in \mathbb{Z}_p$ such that $f(z) = 0$ and $|z - a|_p < |f'(a)|_p$.