A Formal Proof of Hensel's Lemma over the *p*-adic Integers

Robert Y. Lewis

Vrije Universiteit Amsterdam

CPP 2019
January 14

Motivation

Lean Forward

A new 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.
- PI: Jasmin Blanchette

Lean Forward

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 multivatiate polynomials, and related algebra and geometry
- special functions: Dirichlet series, modular forms, ...

The p-adic numbers

The p-adic numbers $\mathbb{Q}_p$ and p-adic integers $\mathbb{Z}_p$

- are fundamental objects of study in number theory
- have applications in theory, numerics, CS
  - Diophantine equations
  - Efficient representations of rationals
  - FP approximations
- are obtained analogously to $\mathbb{R}$, but have very different properties
  - Complete $\mathbb{Q}$ with respect to the p-adic norm
  - Unordered, nonarchimedean norm, Hensel's lemma

Contributions

We have

- defined the p-adic valuation and norm on $\mathbb{Q}$
- generalized the `mathlib` construction of $\mathbb{R}$, using it to define $\mathbb{Q}_p$
- developed the basic theory of $\mathbb{Q}_p$ and $\mathbb{Z}_p$
- proved Hensel's lemma over $\mathbb{Z}_p$

in Lean.

Table of contents

The Lean theorem prover

Background: Lean

Lean is a new interactive theorem prover, developed principally by Leonardo de Moura at Microsoft Research, Redmond.

Calculus of Inductive Constructions with:

- Non-cumulative hierarchy of universes
- Impredicative `Prop`
- Quotient types and propositional extensionality
- Axiom of choice available

See `http://leanprover.github.io`

Background: Lean

Lean is a ~~new~~ interactive theorem prover, developed principally by Leonardo de Moura at Microsoft Research, Redmond.

Calculus of Inductive Constructions with:

- Non-cumulative hierarchy of universes
- Impredicative `Prop`
- Quotient types and propositional extensionality
- Axiom of choice available

See `http://leanprover.github.io`

Background: mathlib

Lean's mathematics library, `mathlib`, is maintained by Mario Carneiro and Johannes Hölzl, with many contributors.

- Classical mathematics
- $\sim$120k loc
- Developments in algebra, topology, analysis, set theory, category theory, . . .

This talk made possible by earlier contributions!

See `https://github.com/leanprover/mathlib`

Completions

The rational numbers

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

The sequence of rationals

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

does not converge to a rational.

Definition.

A sequence $s : \mathbb{N} \to \mathbb{Q}$ 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.

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 $\mathbb{Q}$.

Claim.

If $r_1 \sim r_2$ and $s_1 \sim s_2$ then $r_1 + s_1 \sim r_2 + s_2$. Thus addition lifts from $\mathbb{Q}$ to $\mathbb{R}$. The other ring (field) operations follow similarly.

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

General completions

We can generalize the measure of distance and the base type.

Definition.

A sequence $s : \mathbb{N} \to \mathbb{Q}$ 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 and the base type.

Definition.

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

Definition.

Let F be an ordered field. A function $\text{abs} : Q \to F$ 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

```
class is_absolute_value {α} [ordered_field α] {β} [ring β] (f : β → α) : Prop :=
(abv_nonneg : ∀ x, 0 ≤ f x)
(abv_eq_zero : ∀ {x}, f x = 0 ↔ x = 0)
(abv_add : ∀ x y, f (x + y) ≤ f x + f y)
(abv_mul : ∀ x y, f (x * y) = f x * f y)

parameters {α : Type} [comm_ring α] {β : Type} [ordered_field β]
           (abv : α → β) [is_absolute_value abv]

def is_cauchy (f : ℕ → β) : Prop := ∀ ε > 0, ∃ i, ∀ j ≥ i, abv (f j - f i) < ε

def cau_seq : Type := {f : ℕ → α // is_cauchy abv f}

def equiv (f g : cau_seq) : Prop := ∀ ε > 0, ∃ i, ∀ j ≥ i, abv (f j - g j) < ε

def completion : Type := quotient cau_seq equiv

instance : comm_ring completion := ...
```

Why this completion?

This can be done in various settings. Why this one?

- Doesn't depend on $\mathbb{R}$ (vs. metric completion, normed completion)
- Lightweight, computable (vs. uniform completion, ring completion)
- Easy to lift field operations (vs. uniform completion)

$\mathbb{R}$ and more

We easily prove `is_absolute_value (abs : ℚ → ℚ)` and define $\mathbb{R}$.

A different choice of absolute value leads us to $\mathbb{Q}_p$.

The p-adic norm

The p-adic valuation

Fix a natural number $p > 1$.

Definition.

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

$$\nu_p(z) = \max\left\{n \in \mathbb{N} \,\middle|\, p^n \mid z\right\}$$

with $\nu_p(0) = 0$.

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

$$\nu_p(q/r) = \nu_p(q) - \nu_p(r)$$

when q and r are coprime.

The p-adic valuation

Definition.

```
def padic_val (p : ℕ) (n : ℤ) : ℕ :=
if hn : n = 0 then 0
else if hp : p > 1 then nat.find_greatest (λ k, (p ^ k) ∣ n) n.nat_abs
else 0

def padic_val_rat (p : ℕ) (q : ℚ) : ℤ :=
(padic_val p q.num : ℤ) - (padic_val p q.denom : ℤ)
```

The p-adic norm

$$\nu_p(z) = \max\left\{n \in \mathbb{N} \;\middle|\; p^n \mid z\right\}$$

$$\nu_p(q/r) = \nu_p(q) - \nu_p(r)$$

Definition.

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

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

Definition.

```
def padic_norm (p : ℕ) (q : ℚ) : ℚ :=
if q = 0 then 0 else (p : ℚ) ^ (-(padic_val_rat p q))
```

The p-adic norm

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

```
instance {p} [prime p] : is_absolute_value (padic_norm p)
```

It is also nonarchimedean:

```
protected theorem nonarchimedean {p} [prime p] (q r : ℚ) :
padic_norm p (q + r) ≤ max (padic_norm p q) (padic_norm p r)
```

The p-adic numbers

The p-adic norm

We can complete $\mathbb{Q}$ with respect to $|\cdot|_p$. The result: the *p-adic numbers* $\mathbb{Q}_p$.

```
def padic (p : ℕ) [nat.prime p] := cau_seq.completion (padic_norm p)

notation ‘ℚ_[‘ p ‘]‘ := padic p
```

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 $a_i \in \{0, 1, \ldots, 9\}$.

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 $a_i \in \{0, 1, \ldots, p-1\}$.

Properties of the p-adics

- The p-adic norm on $\mathbb{Q}$ lifts to $\mathbb{Q}_p$.
  - Reason: for any Cauchy sequence $s : \mathbb{N} \to \mathbb{Q}$, $|s_i|_p$ is eventually constant.
- In Lean, we instantiate `ℚ_[p]` as a normed field.
  - It inherits a topology from the norm.
- The norm is nonarchimedean.
- As a consequence, if $|x|_p \leq 1$ and $|y_p| \leq 1$, then $|x + y|_p \leq 1$.
  - Thus the p-adic integers $\mathbb{Z}_p := \left\{z \in \mathbb{Q}_p \;\middle|\; |z|_p \leq 1\right\}$ form a ring.
  - Defined in Lean as a subtype:

```
def padic_int (p : ℕ) [p.prime] := {x : ℚ_[p] // ‖x‖ ≤ 1}
```

- $\mathbb{Z}_p$ is a normed commutative local ring.
- $\mathbb{Q}_p$ and $\mathbb{Z}_p$ are complete with respect to $|\cdot|_p$.

Formalization notes

- $\sim$1500 loc for all this, after the completion process
- Loosely follows Gouvêa, *p-adic Numbers* (1993).
- Uses `linarith`, `ring`, `wlog`, a custom tactic for simplifying sequence indices
- Heavy use of type classes

Hensel’s lemma

Hensel's lemma

Gouvêa: "most important algebraic property of the p-adic numbers."

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 $|z - a|_p < |f'(a)|_p$.

Theorem.

```
theorem hensels_lemma {p : ℕ} [hp : prime p] {a : ℤ_[p]} {F : polynomial ℤ_[p]} :
  ‖F.eval a‖ < ‖F.derivative.eval a‖^2 →
  ∃ z : ℤ_[p], F.eval z = 0 ∧ ‖z - a‖ < ‖F.derivative.eval a‖ ∧
   ∀ z' : ℤ_[p], F.eval z' = 0 → ‖z' - a‖ < ‖F.derivative.eval a‖ → z' = z
```

Hensel's lemma

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 $|z - a|_p < |f'(a)|_p$.

The proof: Newton's method. Follows a writeup by Keith Conrad.

- Define a recursive sequence $\mathbb{N} \to \mathbb{Z}_p$ satisfying certain properties.
- Show this sequence is Cauchy.
- Show the limit is a root of f.
- Show this root is unique within a neighborhood of a.

The Newton sequence

Informally, we write:

$$a_0 = a$$
$$a_{n+1} = a_n - \frac{f(a_n)}{f'(a_n)}$$

It is nontrivial to show that these values lie in $\mathbb{Z}_p$.

But casts in Lean are annoying.

The Newton sequence

```
def T : ℝ := ‖(F.eval a).val / ((F.derivative.eval a).val)^2‖

def ih (n : ℕ) (z : ℤ_[p]) : Prop :=
‖F.derivative.eval z‖ = ‖F.derivative.eval a‖ ∧
  ‖F.eval z‖ ≤ ‖F.derivative.eval a‖^2 * T ^ (2^n)

def newton_seq : Π n : ℕ, {z : ℤ_[p] // ih n z}
| 0 := ⟨a, ih_0⟩
| (k+1) := ih_n (newton_seq k).2
```

The Newton sequence

A large part of the proof is spent verifying the successor step.

- algebraic manipulations
- chains of (simple) nonlinear inequalities

```
def ih (n : ℕ) (z : ℤ_[p]) : Prop :=
‖F.derivative.eval z‖ = ‖F.derivative.eval a‖ ∧
  ‖F.eval z‖ ≤ ‖F.derivative.eval a‖^2 * T ^ (2^n)

def ih_n {n : ℕ} {z : ℤ_[p]} (hz : ih n z) :
  {z' : ℤ_[p] // ih (n+1) z'} := ...
```

The Newton sequence is Cauchy

We then establish that this sequence is Cauchy.

- Limit arguments: some work to reconcile sequential limits and filter limits.
- More chains of inequalities and algebraic identities.
  - nonarchimedean property of the norm
  - $\forall x \forall y \exists k. f(x+y) = f(x) + f'(x) \cdot y + k \cdot y^2$
  - $\forall x \forall y \forall n \exists k. (x+y)^n = x^n + n \cdot x^{n-1} \cdot y + k \cdot y^2$

Interesting note: the argument given by Conrad fails when the initial point a is already a solution.

The limit is a unique root

It follows from the induction hypothesis that the limit of the Newton sequence is a root of f.

Only slightly more work to show it is unique.

Special case when $f(a) = 0$ is immediate (the sequence is constant).

Conclusions

Formalization notes:

- $\sim$400 loc, corresponding to $\sim$65 informal lines.
- This could be greatly shortened with better automation for inequalities and casts.

Future work:

- Generalize! (Characterize “henselian rings.”)
- Extend!
- More number theory!

Related work:

- Constructions of $\mathbb{Q}_p$ in HOL Light (Harrison) and UniMath (Pelayo, Voevodsky, Warren).
- A variant of Hensel’s lemma over $\mathbb{Z}$ in Coq (Martin-Dorel, Hanrot, Mayero, Théry).

References

Keith Conrad.
Hensel's lemma.
http://www.math.uconn.edu/ kconrad/blurbs/gradnumthy/hensel.pdf.

Fernando Q. Gouvêa.
***p-adic Numbers*.**
Universitext. Springer, Berlin, second edition, 1997.

Appendix

The p-adic norm

Examples.

x	$\nu_3(x)$	$\lvert x \rvert_3$
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 numbers

Arithmetic in $\mathbb{Q}_5$

$$
\begin{array}{rr}
 & {\scriptstyle 1\,1\,1\,1\,1\,1\,1\,} \\
 & \ldots 44444444 \\
+ & 1 \\
\hline
 & 0
\end{array}
\qquad
\begin{array}{rr}
 & {\scriptstyle 1\,2\,1\,2\,1\,2\,1\,} \\
 & \ldots 31313132 \\
\times & 3 \\
\hline
 & 1
\end{array}
\qquad
\begin{array}{rr}
 & {\scriptstyle 1\,1\,1\,1\,1\,1\,1\,} \\
 & \ldots 31313132 \\
+ & \ldots 44444444 \\
\hline
 & \ldots 31313131
\end{array}
$$

The p-adic numbers