The p-adic number and Finding roots in $\mathbb{Z}_p$

Matseoi Zau

March 4, 2025

Overview

Three Parts:

1. Non Archimedean Absolute Value

Overview

Three Parts:

1. Non Archimedean Absolute Value
2. Defining p-adic numbers

Overview

Three Parts:

1. Non Archimedean Absolute Value
2. Defining p-adic numbers
3. Application: Hensel's Lemma

Part 1: Non Archimedean Absolute Value

Definition

A *non-Archimedean absolute value* $|\cdot|_p$ mapping from a field K to $\mathbb{R}^+$ is an absolute value that satisfies the *non-archimedean property*:

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

for all $x, y \in K$. Additionally:

- $|x| \geq 0$, and $|x| = 0$ if and only if $x = 0$,
- $|xy| = |x||y|$ for all $x, y \in K$,
- $|x+y| \leq |x| + |y|$ for all $x, y \in K$.

Part 1: Non Archimedean Absolute Value

p-adic absolute value is an example of non Archimedean absolute value

Definition

The *p-adic valuation* $v_p(x)$ of a nonzero rational number x is given by:

$$v_p(x) = \max\{k \in \mathbb{Z} : p^k \text{ divides } x\}$$

For $x = 0$, $v_p(0) = +\infty$.

Definition

The *p-adic absolute value* $|\cdot|_p$ on the field of rational numbers $\mathbb{Q}$ is defined as for any nonzero rational number x, then:

$$|x|_p = p^{-v_p(x)}$$

and $|0|_p = 0$.

Ostrowski's Theorem

Theorem

Ostrowski's Theorem states that any absolute value on the field of rational numbers $\mathbb{Q}$ is equivalent to either:

- *the usual absolute value $|\cdot|$, or*
- *the p-adic absolute value $|\cdot|_p$ for some prime number p.*

In other words, every nontrivial absolute value on $\mathbb{Q}$ is either Archimedean (the usual absolute value) or non-Archimedean (a p-adic absolute value).

Part 2: The p-adic numbers

Definition

A p-adic number can be expressed as an infinite series of the form:

$$x = \sum_{n=N}^{\infty} a_n p^n,$$

where:

- $N \in \mathbb{Z}$ (allowing for negative powers of p),
- $a_n \in \{0, 1, \ldots, p-1\}$ are the coefficients,
- p is a fixed prime number.

Part 2: The p-adic numbers

Example: 3-adic Expansion of 72

Consider the 3-adic expansion of the number 72:

$$72 = 0 \cdot 3^0 + 0 \cdot 3^1 + 2 \cdot 3^2 + 2 \cdot 3^3$$

where $a_n \in \{0, 1, 2\}$ are the coefficients. Here, 72 is represented in the base-3 system.

Part 2: The p-adic numbers

3-adic Expannsion of -$\frac{1}{2}$
Consider the sequence:

$$x_n = 1 + 3 + 3^2 + \cdots + 3^n$$

In the real numbers $\mathbb{R}$, this sequence diverges. However, in the 3-adic numbers $\mathbb{Q}_3$, this sequence converges to:

$$\ldots 33331_3 = \frac{1}{1-3} = -\frac{1}{2}$$

This example highlights the difference in convergence behavior between $\mathbb{R}$ and $\mathbb{Q}_3$.

Part 3: Hensel's Lemma

Motivation

- **Roots in $\mathbb{Z}$:** Use modular arithmetic (e.g., Gauss Lemma).
- **Roots in $\mathbb{Q}$:** Rational Root Theorem provides systematic candidates.
- **Roots in $\mathbb{Z}_p$:** How do we lift solutions from $\mathbb{Z}/p\mathbb{Z}$ to higher moduli $\mathbb{Z}/p^k\mathbb{Z}$?

Part 3: Hensel's Lemma

Theorem

Hensel's Lemma states that if $F(X) = a_0 + a_1X + a_2X^2 + \cdots + a_nX^n$ *is a polynomial with coefficients in* $\mathbb{Z}_p$*, and there exists a p-adic integer* $\alpha_1 \in \mathbb{Z}_p$ *such that:*

$$F(\alpha_1) \equiv 0 \pmod{p\mathbb{Z}_p}$$

and

$$F'(\alpha_1) \not\equiv 0 \pmod{p\mathbb{Z}_p},$$

where $F'(X)$ *is the formal derivative of* $F(X)$*, then there exists a unique p-adic integer* $\alpha \in \mathbb{Z}_p$ *such that:*

$$\alpha \equiv \alpha_1 \pmod{p\mathbb{Z}_p}, \quad F(\alpha) = 0.$$

Part 3: Hensel's Lemma

Example: Applying Hensel's Lemma
Let $f(X) = X^2 - 4$ over the 5-adic integers. We have:

$$f(3) \equiv 0 \pmod 3, \quad f'(3) = 2 \times 3 \equiv 1 \pmod 3$$

To find the square root of 4:

$$4 \equiv 3^2 \pmod 5$$

$$4 \equiv (3 + 4 \cdot 5)^2 \pmod{25}$$

$$4 \equiv (3 + 4 \cdot 5 + 1 \cdot 5^2) \pmod{125}$$

Therefore, the root is:

$$\ldots 141$$

Acknowledgments

I would like to thank:

- Matthew for the mentoring,
- The Directed Reading Program Committee for organizing this opportunity,
- The audience for their attention and participation.