Introduction to p-adic Analysis

Mathematical Analysis

Algebraic Foundations

The p-adic Valuation

Definition 1.1 (p-adic valuation)

Let p be a prime number. For any rational number $x \neq 0$, we can write x uniquely as

$$x = p^k \cdot \frac{a}{b}$$

where $k \in \mathbb{Z}$, and a, b are integers with $\gcd(a,p) = \gcd(b,p) = 1$. The **p-adic valuation** of x is defined as $v_p(x) = k$. We set $v_p(0) = +\infty$.

Properties of the p-adic valuation:

1. $v_p(xy) = v_p(x) + v_p(y)$
2. $v_p(x+y) \geq \min\{v_p(x), v_p(y)\}$ with equality when $v_p(x) \neq v_p(y)$
3. $v_p(x) = +\infty$ if and only if $x = 0$

The p-adic Absolute Value

Definition 1.2 (p-adic absolute value)

The **p-adic absolute value** $|\cdot|_p$ is defined by

$$|x|_p = \begin{cases} 0 & \text{if } x = 0 \\ p^{-v_p(x)} & \text{if } x \neq 0 \end{cases}$$

Theorem 1.1 (Properties of p-adic absolute value)

The p-adic absolute value satisfies:

1. $|x|_p = 0$ if and only if $x = 0$
2. $|xy|_p = |x|_p |y|_p$
3. **Strong triangle inequality (Ultrametric inequality)**: $|x+y|_p \leq \max\{|x|_p, |y|_p\}$

Proof of Theorem 1.1

Properties 1 and 2 follow directly from the definition and properties of the valuation. For property 3:
If $x = 0$ or $y = 0$, the inequality is trivial. Otherwise, let $v_p(x) = k$ and $v_p(y) = \ell$. Then:

- $|x + y|_p = p^{-v_p(x+y)}$
- By property 2 of valuations, $v_p(x + y) \geq \min\{k, \ell\}$
- Therefore, $|x + y|_p = p^{-v_p(x+y)} \leq p^{-\min\{k,\ell\}} = \max\{p^{-k}, p^{-\ell}\} = \max\{|x|_p, |y|_p\}$

Corollary 1.1

In the p-adic metric, every triangle is isosceles. If $|x|_p \neq |y|_p$, then $|x + y|_p = \max\{|x|_p, |y|_p\}$.

Ostrowski's Theorem

Theorem 1.2 (Ostrowski's Theorem)

Every non-trivial absolute value on $\mathbb{Q}$ is equivalent to either the usual absolute value $|\cdot|_\infty$ or to some p-adic absolute value $|\cdot|_p$ for a prime p.

This theorem classifies all possible ways to measure "size" on the rational numbers, showing that the familiar absolute value and the p-adic absolute values are essentially the only possibilities.

Algebraic Consequences

Definition 1.3 (p-adic integers)

The ring of **p-adic integers** is defined as

$$\mathbb{Z}_p = \{x \in \mathbb{Q} : |x|_p \leq 1\} = \{x \in \mathbb{Q} : v_p(x) \geq 0\}$$

Theorem 1.3

$\mathbb{Z}_p$ is a local ring with unique maximal ideal $\mathfrak{m} = p\mathbb{Z}_p = \{x \in \mathbb{Z}_p : |x|_p < 1\}$.

Proof of Theorem 1.3

First, we show $\mathbb{Z}_p$ is a ring. If $x, y \in \mathbb{Z}_p$, then $|x|_p \leq 1$ and $|y|_p \leq 1$.

- $|xy|_p = |x|_p|y|_p \leq 1$, so $xy \in \mathbb{Z}_p$
- $|x + y|_p \leq \max\{|x|_p, |y|_p\} \leq 1$, so $x + y \in \mathbb{Z}_p$

The units of $\mathbb{Z}_p$ are precisely $\{x \in \mathbb{Z}_p : |x|_p = 1\}$, since if $|x|_p = 1$, then x has inverse x^{-1}

with $|x^{-1}|_p = 1$. The non-units form the ideal $\mathfrak{m} = \{x \in \mathbb{Z}_p : |x|_p < 1\}$, which is maximal since $\mathbb{Z}_p/\mathfrak{m} \cong \mathbb{Z}/p\mathbb{Z}$ is a field.

Analytic Foundations

Metric and Topological Properties

The p-adic absolute value induces a metric $d_p(x, y) = |x - y|_p$ on $\mathbb{Q}$. This metric has unusual properties compared to the usual Euclidean metric.

Theorem 2.1 (Ultrametric space properties)

The metric space $(\mathbb{Q}, d_p)$ satisfies:

1. Every ball is both open and closed (clopen)
2. If two balls intersect, one is contained in the other
3. Every point in a ball is a center of that ball
4. The space is totally disconnected

Proof sketch of Theorem 2.1

These follow from the strong triangle inequality. For example, for property 3: if $z \in B_r(x) = \{y : |y - x|_p < r\}$, then for any $w \in B_r(x)$, we have $|w - z|_p \le \max\{|w - x|_p, |x - z|_p\} < r$, so $B_r(x) \subseteq B_r(z)$. Similarly, $B_r(z) \subseteq B_r(x)$.

Sequences and Convergence

Definition 2.1 (p-adic convergence)

A sequence (x_n) in $\mathbb{Q}$ converges p-adically to x if $|x_n - x|_p \to 0$ as $n \to \infty$.

Theorem 2.2

A sequence (x_n) converges p-adically if and only if $|x_{n+1} - x_n|_p \to 0$.

Proof of Theorem 2.2

The "only if" direction is standard. For "if": suppose $|x_{n+1} - x_n|_p \to 0$. We show (x_n) is Cauchy.
For any $m > n$, we have:

$$|x_m - x_n|_p = |x_m - x_{m-1} + x_{m-1} - x_{m-2} + \cdots + x_{n+1} - x_n|_p$$

By the ultrametric inequality applied repeatedly:

$$|x_m - x_n|_p \leq \max\{|x_m - x_{m-1}|_p, |x_{m-1} - x_{m-2}|_p, \dots, |x_{n+1} - x_n|_p\}$$

Since $|x_{k+1} - x_k|_p \to 0$, given $\epsilon > 0$, there exists N such that for all $k \geq N$, $|x_{k+1} - x_k|_p < \epsilon$. Therefore, for $m > n \geq N$, $|x_m - x_n|_p < \epsilon$, proving (x_n) is Cauchy.

Series and Power Series

Definition 2.2 (p-adic series)

A series $\sum_{n=0}^{\infty} a_n$ converges p-adically if the sequence of partial sums converges p-adically.

Theorem 2.3 (p-adic convergence criterion)

A series $\sum_{n=0}^{\infty} a_n$ converges p-adically if and only if $|a_n|_p \to 0$ as $n \to \infty$.

This is much stronger than the real case, where we only get convergence if terms go to zero, but the converse is not true.

Example: The geometric series $\sum_{n=0}^{\infty} p^n$ diverges p-adically since $|p^n|_p = p^{-n} \not\to 0$.

However, $\sum_{n=0}^{\infty} p^n x^n$ converges for $|x|_p < 1$ to $\frac{1}{1-px}$.

p-adic Functions

Definition 2.3 (p-adic analytic function)

A function $f : U \to \mathbb{Q}_p$ where $U \subseteq \mathbb{Q}_p$ is open is called **p-adic analytic** if for every $a \in U$, there exists a neighborhood V of a and a power series $\sum_{n=0}^{\infty} c_n (x-a)^n$ that converges to $f(x)$ for all $x \in V$.

Key differences from real analysis:

1. **Radius of convergence**: For $\sum_{n=0}^{\infty} a_n x^n$, the radius is $R = \frac{1}{\limsup_{n\to\infty} |a_n|_p^{1/n}}$
2. **Behavior on boundary**: p-adic power series often converge on their entire boundary
3. **Maximum principle**: If f is analytic on a disk, then $\max_{|x|_p \leq r} |f(x)|_p = \max_{|x|_p = r} |f(x)|_p$

Completions

The Field of p-adic Numbers

The rational numbers $\mathbb{Q}$ are not complete with respect to the p-adic metric. Just as we complete $\mathbb{Q}$ with respect to the usual absolute value to get $\mathbb{R}$, we can complete it with respect to $|\cdot|_p$.

Definition 3.1 (p-adic numbers)

The **field of p-adic numbers** $\mathbb{Q}_p$ is the completion of $\mathbb{Q}$ with respect to the p-adic absolute value $|\cdot|_p$.

Theorem 3.1 (Properties of $\mathbb{Q}_p$)

1. $\mathbb{Q}_p$ is a complete metric space under the p-adic metric
2. $\mathbb{Q}_p$ is a field containing $\mathbb{Q}$ as a dense subfield
3. The p-adic absolute value extends uniquely to $\mathbb{Q}_p$
4. $\mathbb{Q}_p$ is locally compact

Construction via Cauchy Sequences

Elements of $\mathbb{Q}_p$ can be represented as equivalence classes of Cauchy sequences in $\mathbb{Q}$ under the p-adic metric.

Alternative representation: Every non-zero element $x \in \mathbb{Q}_p$ can be written uniquely as:

$$x = p^k \sum_{i=0}^{\infty} a_i p^i$$

where $k \in \mathbb{Z}$, $a_i \in \{0, 1, 2, \dots, p-1\}$, and $a_0 \neq 0$.

The Ring of p-adic Integers

Definition 3.2 (Completion of p-adic integers)

The **ring of p-adic integers** $\mathbb{Z}_p$ is the completion of $\{x \in \mathbb{Q} : |x|_p \leq 1\}$, equivalently:

$$\mathbb{Z}_p = \{x \in \mathbb{Q}_p : |x|_p \leq 1\}$$

Theorem 3.2 (Structure of $\mathbb{Z}_p$)

1. $\mathbb{Z}_p$ is a compact, complete metric space
2. $\mathbb{Z}_p$ is a local ring with maximal ideal $p\mathbb{Z}_p$
3. Every element of $\mathbb{Z}_p$ can be written uniquely as $\sum_{i=0}^{\infty} a_i p^i$ where $a_i \in \{0, 1, \dots, p-1\}$
4. $\mathbb{Z}_p / p^n \mathbb{Z}_p \cong \mathbb{Z}/p^n\mathbb{Z}$

Hensel's Lemma

> ❗ Theorem 3.3 (Hensel's Lemma)
>
> Let $f(x) \in \mathbb{Z}_p[x]$ be a polynomial, and suppose $a \in \mathbb{Z}_p$ satisfies:
>
> 1. $f(a) \equiv 0 \pmod p$
> 2. $f'(a) \not\equiv 0 \pmod p$
>
> Then there exists a unique $\alpha \in \mathbb{Z}_p$ such that $f(\alpha) = 0$ and $\alpha \equiv a \pmod p$.

This powerful lifting theorem allows us to solve polynomial equations in $\mathbb{Q}_p$ by first solving them modulo p and then "lifting" the solutions.

Example: The equation $x^2 = 2$ has solutions in $\mathbb{Q}_7$ but not in $\mathbb{Q}_3$, demonstrating that $\mathbb{Q}_p$ depends crucially on the prime p.

Applications and Further Directions

The theory of p-adic numbers connects to many areas of mathematics:

- **Number Theory**: Studying Diophantine equations, local-global principles
- **Algebraic Geometry**: p-adic varieties and rigid analytic spaces

- **Representation Theory**: p-adic representations of Galois groups
- **Mathematical Physics**: p-adic quantum mechanics and string theory

The completion process we've described here is fundamental to modern algebraic number theory and provides a powerful tool for understanding the arithmetic of rational numbers through "local" information at each prime.

References

For further reading on p-adic analysis, consult:

- Koblitz, N. *p-adic Numbers, p-adic Analysis, and Zeta-Functions*
- Robert, A. *A Course in p-adic Analysis*

- Gouvêa, F. *p-adic Numbers: An Introduction*