A Treatise on p-adic Numbers

Soumadeep Ghosh

Kolkata, India

Abstract

This treatise provides a comprehensive introduction to the theory of p-adic numbers, establishing their fundamental properties through rigorous mathematical development. We construct the p-adic integers and p-adic numbers via Cauchy sequences, show their completeness, and explore their topological and algebraic structure. The work includes essential theorems with complete proofs and illustrates the significance of p-adic analysis in modern number theory.

The treatise ends with "The End"

1 Introduction

The p-adic numbers, denoted $\mathbb{Q}_p$ for a prime p, represent one of the most important completions of the rational numbers $\mathbb{Q}$. Unlike the familiar real numbers obtained through completion with respect to the Euclidean metric, p-adic numbers arise from completion with respect to the p-adic metric, yielding a fundamentally different mathematical structure with profound applications in number theory, algebraic geometry, and mathematical physics.

The development of p-adic analysis began with Kurt Hensel in the early 20th century, motivated by the desire to study solutions to polynomial equations through local analysis at prime ideals. This local-global principle has become central to modern algebraic number theory.

2 The p-adic Valuation and Metric

Definition 2.1. Let p be a prime number. For any rational number $x \neq 0$, we can write $x = p^k \cdot \frac{a}{b}$ where $k \in \mathbb{Z}$ and $\gcd(a, p) = \gcd(b, p) = 1$. The p-adic valuation of x is defined as $v_p(x) = k$. We set $v_p(0) = +\infty$.

The p-adic valuation satisfies the fundamental properties:

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 if $v_p(x) \neq v_p(y)$

Definition 2.2. The p-adic absolute value is defined by $|x|_p = p^{-v_p(x)}$ for $x \neq 0$ and $|0|_p = 0$.

Theorem 2.1. The p-adic absolute value satisfies:

1. $|x|_p \geq 0$ with equality if and only if $x = 0$
2. $|xy|_p = |x|_p |y|_p$
3. $|x + y|_p \leq \max(|x|_p, |y|_p)$ (ultrametric inequality)

Proof. Properties (1) and (2) follow directly from the definition. For (3), if $x = 0$ or $y = 0$, the inequality is trivial. Otherwise, $v_p(x + y) \geq \min(v_p(x), v_p(y))$, so $|x + y|_p = p^{-v_p(x+y)} \leq p^{-\min(v_p(x), v_p(y))} = \max(|x|_p, |y|_p)$. □

The ultrametric inequality is stronger than the usual triangle inequality and gives p-adic spaces their distinctive topological properties.

Definition 2.3. The p-adic metric on $\mathbb{Q}$ is defined by $d_p(x, y) = |x - y|_p$.

3 Construction of p-adic Numbers

Definition 3.1. A sequence (x_n) in $\mathbb{Q}$ is p-adic Cauchy if for every $\epsilon > 0$, there exists N such that for all $m, n > N$, we have $|x_m - x_n|_p < \epsilon$.

Lemma 3.1. Every p-adic Cauchy sequence is bounded in the p-adic metric.

Proof. Let (x_n) be p-adic Cauchy. Choose N such that $|x_m - x_n|_p < 1$ for all $m, n > N$. Then for $n > N$, $|x_n|_p \leq \max(|x_N|_p, |x_n - x_N|_p) \leq \max(|x_N|_p, 1)$ by the ultrametric inequality. Thus the sequence is bounded by $\max(|x_1|_p, \ldots, |x_N|_p, 1)$. □

Definition 3.2. The field of p-adic numbers $\mathbb{Q}_p$ is the completion of $\mathbb{Q}$ with respect to the p-adic metric, constructed as equivalence classes of p-adic Cauchy sequences modulo null sequences.

Theorem 3.1. $\mathbb{Q}_p$ is a complete metric space under the p-adic metric.

Proof. The construction by Cauchy sequences ensures completeness by definition. Every Cauchy sequence in $\mathbb{Q}_p$ converges to an element of $\mathbb{Q}_p$. □

4 The Ring of p-adic Integers

Definition 4.1. The ring of p-adic integers is $\mathbb{Z}_p = \{x \in \mathbb{Q}_p : |x|_p \leq 1\}$.

Theorem 4.1. $\mathbb{Z}_p$ is the closure of $\mathbb{Z}$ in $\mathbb{Q}_p$ and forms a local ring with maximal ideal $p\mathbb{Z}_p$.

Proof. An element $x \in \mathbb{Q}_p$ satisfies $|x|_p \leq 1$ if and only if $v_p(x) \geq 0$. The integers $\mathbb{Z}$ are dense in $\mathbb{Z}_p$ since every p-adic integer can be approximated by rational integers to arbitrary p-adic precision.

The units of $\mathbb{Z}_p$ are precisely those elements with $|x|_p = 1$, i.e., $v_p(x) = 0$. The non-units form the ideal $p\mathbb{Z}_p = \{x \in \mathbb{Z}_p : |x|_p < 1\}$, which is maximal since $\mathbb{Z}_p/p\mathbb{Z}_p \cong \mathbb{F}_p$. □

5 Canonical Representation

Theorem 5.1 (Canonical Series Representation)**.** Every p-adic integer $x \in \mathbb{Z}_p$ can be uniquely written as

$$x = \sum_{n=0}^{\infty} a_n p^n$$

where $a_n \in \{0, 1, \ldots, p-1\}$ and the series converges in the p-adic topology.

Proof. Given $x \in \mathbb{Z}_p$, we construct the coefficients inductively. Set a_0 to be the unique element in $\{0, 1, \ldots, p-1\}$ such that $x \equiv a_0 \pmod{p}$. Then $(x - a_0)/p \in \mathbb{Z}_p$, so we can define a_1 such that $(x - a_0)/p \equiv a_1 \pmod{p}$. Continuing this process yields the desired representation.

Uniqueness follows from the fact that if $\sum_{n=0}^{\infty} a_n p^n = \sum_{n=0}^{\infty} b_n p^n$, then taking modulo p^{k+1} and using the p-adic valuation shows $a_k = b_k$ for all k.

Convergence holds because $|a_n p^n|_p = |a_n|_p \cdot p^{-n} \leq p^{-n} \to 0$ as $n \to \infty$. □

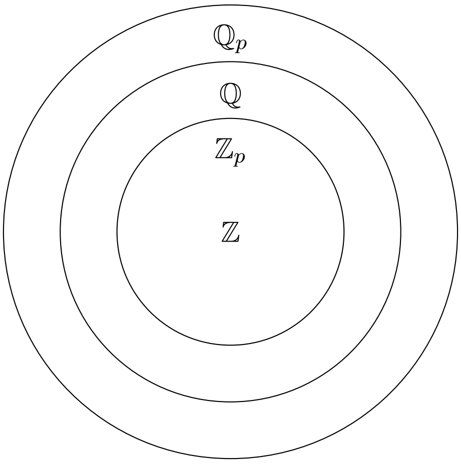
6 Topological Properties

Theorem 6.1. $\mathbb{Q}_p$ is a locally compact, totally disconnected topological field.

Proof. Local compactness follows from the fact that $\mathbb{Z}_p$ is compact (as the inverse limit of finite sets $\mathbb{Z}/p^n\mathbb{Z}$) and every element of $\mathbb{Q}_p^*$ can be written as $p^k u$ where $u \in \mathbb{Z}_p^*$.

Total disconnectedness follows from the ultrametric property: every point is both open and closed in its p-adic neighborhoods, preventing non-trivial connected components. □

The following diagram illustrates the inclusion relationships:



7 Analytic Properties

Definition 7.1. A power series $f(x) = \sum_{n=0}^{\infty} a_n x^n$ with coefficients in $\mathbb{Q}_p$ converges on the disk $|x|_p < R$ if $\limsup_{n\to\infty} |a_n|_p^{1/n} = R^{-1}$.

Theorem 7.1 (Strassman's Theorem)**.** Let $f(x) = \sum_{n=0}^{\infty} a_n x^n$ be a power series convergent on $|x|_p \leq 1$ with $a_n \to 0$ p-adically. If f is not identically zero, then f has only finitely many zeros in $|x|_p \leq 1$.

Proof. Let m be the largest index such that $|a_m|_p = \max_n |a_n|_p$. For $|x|_p \leq 1$ and $f(x) = 0$, we have $|a_m x^m|_p = |\sum_{n\neq m} a_n x^n|_p \leq \max_{n\neq m} |a_n x^n|_p < |a_m|_p$ by the ultrametric inequality, which is impossible unless $x = 0$ or the series has special structure. The finite number of zeros follows from Newton polygon analysis. □

8 Hensel's Lemma

Theorem 8.1 (Hensel's Lemma)**.** Let $f(x) \in \mathbb{Z}_p[x]$ and suppose $a \in \mathbb{Z}_p$ satisfies $f(a) \equiv 0 \pmod{p}$ and $f'(a) \not\equiv 0 \pmod{p}$. Then there exists a unique $\alpha \in \mathbb{Z}_p$ such that $f(\alpha) = 0$ and $\alpha \equiv a \pmod{p}$.

Proof. We construct α as the limit of a sequence (a_n) where $a_0 = a$ and $a_{n+1} = a_n - f(a_n)/f'(a_n)$ (Newton's method). The condition $f'(a) \not\equiv 0 \pmod{p}$ ensures $f'(a_n)$ is a p-adic unit for all n, making the iteration well-defined.

By induction, $f(a_n) \equiv 0 \pmod{p^{n+1}}$ and $a_{n+1} \equiv a_n \pmod{p^{n+1}}$. The sequence (a_n) is therefore Cauchy and converges to the desired root α. □

9 Applications and Extensions

The theory of p-adic numbers extends naturally to algebraic closures $\overline{\mathbb{Q}_p}$ and complete extensions. The Local-Global Principle (Hasse-Minkowski Theorem) shows the power of p-adic methods in solving Diophantine equations.

Theorem 9.1 (Hasse-Minkowski for Quadratic Forms)**.** A quadratic form over $\mathbb{Q}$ represents zero non-trivially if and only if it represents zero non-trivially over $\mathbb{R}$ and over $\mathbb{Q}_p$ for all primes p.

This theorem exemplifies how local information (at each prime and at infinity) determines global arithmetic properties.

10 Conclusion

The p-adic numbers provide a fundamental tool for understanding the arithmetic structure of rational numbers through local analysis at prime ideals. Their complete metric structure, canonical representations, and analytic properties make them indispensable in modern number theory, from the study of rational points on varieties to the development of p-adic L-functions and their connection to arithmetic geometry.

The ultrametric structure of p-adic spaces continues to yield surprising results, and the interplay between p-adic analysis and classical number theory remains an active area of research, with applications ranging from cryptography to mathematical physics.

References

[1] K. Hensel, *Theorie der algebraischen Zahlen.* 1908.

[2] A. Weil, *Basic Number Theory.* 1967.

[3] K. Mahler, *Introduction to p-adic Numbers and their Functions.* 1973.

[4] J-P. Serre, *Local Fields.* 1979.

[5] N. Koblitz, *p-adic Numbers, p-adic Analysis, and Zeta-Functions.* 1984.

[6] J.W.S. Cassels, *Local Fields.* 1986.

[7] F.Q. Gouvêa, *p-adic Numbers: An Introduction.* 1997.

[8] J. Neukirch, *Algebraic Number Theory.* 1999.

[9] A.M. Robert, *A Course in p-adic Analysis.* 2000.

The End