Proceedings of the 3rd International Conference on Computing Innovation and Applied Physics
DOI: 10.54254/2753-8818/25/20240919

The development of P-adic numbers theoretically and their use in number theory

JUNZHE HAO

+44 7926542993 vita student accommodation Cannon Park, room D111, Coventry, United Kingdom, CV47DU, undergraduate in University of warwick, graduate from Suzhou Foreign language school

Junzhe.Hao@warwick.ac.uk

Abstract. Stemming from the need to formalize the divisibility of rational numbers, p-adics provide a unique mathematical perspective rooted in prime number theory. This article provides a comprehensive discussion of p-adic numbers, including their research background, definition, properties, theory, and extensions. This study first elucidates the historical background and significance of p-adic numbers, emphasizing their key role in number theory and its applications. At the heart of this research is a deep dive into the precise definition of p-radical numbers, revealing their unique, often counterintuitive, distance measure. We look at their fundamental characteristics, demonstrate their illogical characteristics, and discuss how they affect transcendental number theory, Diophantine equations, and algebraic number theory. Furthermore, this article explores the theoretical foundations of p-radical numbers and their extensions, emphasizing their integral role in advanced mathematical structures such as p-radical analysis and p-radical geometry. By covering these aspects, this study aims to highlight the lasting impact of p-adic on modern mathematics, reshape our understanding of divisibility, and advance mathematical inquiry into new and uncharted territory.

Keywords: p-adic number, prime, number theory.

1. Introduction

The study of p-adic numbers has been a cornerstone of the field of number theory, providing deep insights into the divisibility of rational numbers and a unique framework for understanding the complex interplay of prime numbers in mathematics [1, 2]. This article examines the definitions, characteristics, and theoretical underpinnings of p-adic numbers.

In the field of mathematics based on integers and rational numbers, p-adic numbers emerged as a significant extension, providing a novel perspective on number theory. Their significance lies not only in their intrinsic mathematical beauty but also in their practical use. P-adics have applications in many branches of mathematics, including algebraic number theory, Diophantine equations, and transcendental number theory, by revealing the structure of divisibility within rational numbers [3, 4, 5, 6].

This research seeks to elucidate the theoretical framework underpinning p-adic numbers, revealing their unique properties and their role in advancing our understanding of number theory. By delving into their definitions, properties, and theoretical implications, we aim to provide a comprehensive overview of p-adic numbers and their enduring relevance in contemporary mathematical research.

DOI: 10.54254/2753-8818/25/20240919

2. Motivation

$\sqrt{3}$ is an irrational number which can be expressed by:

$$\sqrt{3} = 1.73205080757\ldots = 1 + 7\times10^{-1} + 3\times10^{-2} + 2\times10^{-3}\ldots \tag{1}$$

How can express this irrational number into a sequence xk of rational numbers? let's consider a quadratic congruence:

$$x^2 \equiv 3\bmod 13^k, \tag{2}$$

and $k = 1,2,3\ldots$ for $k = 1$, the solutions are $x = x_1 \equiv \pm 4(\bmod 13)$ for $k = 2$, it can also find the solution that is $x_2 = x_1 + 13y = \pm 4 + 13y$. Let $x1 = 4$, check the equation:

$$\begin{gathered}(4+13y)^2 = 16+104y+13^2y^2 \equiv 16+104y \equiv 3(\bmod 13)^2 \\ 13(1+8y) \equiv 0\bmod 13^2\end{gathered}, \tag{3}$$

the only solution of y is $y \equiv 8\bmod 13$, so $x_2 = 4 + 13\times 8 = 108$.

With a similar method, it can keep deducing $x3, x4$ an,d so on. Now there is some sort of "sequence" that xk satisfies that can be discovered, $x^2 \equiv 3\bmod 13^k$ but no particular x satisfies for all n.

Then the paper needs to define a kind of number called p-adic number, which can show the relationship of Z_p elements in the group for each prime number [7].

3. Basic lemmas

Lemma 3.1. The following form is the only way to express any non-zero rational number:

$$p^v\frac{m}{n}, \tag{4}$$

where n, m, and n are all integers, p is a prime number, and neither m nor n is divisible by p. P-adic valuation of the rational number is referred to as v.

It must employ the fundamental theorem of mathematics to prove this lemma. It asserts that, regardless of the arrangement of the prime components, every positive integer greater than 1 may be written in a particular form as a multiplication of prime integers. For example, $1000 = 2\times2\times2\times5\times5\times5 = 23\times53$. Obviously, the formula of nonzero rational number can be directly deduced from the fundamental theorem of arithmetic.

Lemma 3.2. The only way to express each non-zero rational number r with a valuation v is as $r = ap^v + s$ follows: where an is an integer such that and s is a rational number with value greater than v:

$$0 < a < p, \tag{5}$$

Lemma 3.2 can be deduced from the first lemma. By lemma 2.1, $r = p^v\frac{m}{n}$, the modular inverse of n can be expressed as q such that $nq = 1 + ph$, where q and h are both integer. Then substitute $1/n = q - p(hm/n)$. into the formula of r and get:

$$r = ap^v + p^{v+1}\frac{kn-hm}{n} \tag{6}$$

which is lemma 2.2 states [8].

DOI: 10.54254/2753-8818/25/20240919

4. p-adic integer Z_p

4.1. p-adic numberd

Definition 4.1 (p-adic series). A power series expression of a mathematical series is known as a p-adic series:

$$\sum_{i=v}^{\infty} r_i p^i , \tag{7}$$

where v is an integer, and the coefficients r_i are rational numbers that satisfy one of the following conditions:

1. The coefficient r_i is zero.

2. The coefficient r_i is a nonzero rational number whose denominator is not divisible by the prime number p [9].

Every single rational number can be express as a single term of p-adic number. We can go further defining p-adic number and p-adic integer through p-adic series.

Definition 4.2 (p-adic number). Every p-aidc series represents a p-adic number, which is defined as a normalized p-adic series.

p-adic seris $\sum_{i=v}^{\infty} r_i p^i$ is normalized if either all r_i are integers such that $0 \le ai < p, av > 0$, or all ai are zero for all i. If all ai are zero then it is called zero series.

4.2. Zp

Definition 3.3 (p-adic integer). A p-adic integer α is defined by a sequence of integers xk that $k \ge 1$ expressed as:

$$\sum_{i=v}^{\infty} r_i p^i \alpha = \{x_k\}_{k=1}^{\infty} = \{x_1, x_2, x_3, \ldots\} . \tag{8}$$

And it satisfies the condition below:

$$x_{k+1} \equiv x_k \bmod p^k, \forall k \ge 1. \tag{9}$$

Simply speaking, each term is congruent to the previous term in the sequence modulo power of k of $x_{k+1} \equiv x_k \bmod p^k$ the prime number p. Only if, two sequences $\{xk\}$ and $\{yk\}$ determine the same p-adic integer α if and for all $k \ge 1$: The set of all p-adic integers is denoted by Zp, and it consists of all sequences of integers satisfying these conditions. Every integer is a p-adic integer. The rational numbers in the form of $(apk)/b$ with b coprime with p with $k \ge 0$ are p-adic integers too [10].

Example 3.1. It can take p = 5. Here are several elements in $Z5$:

$$\begin{gathered} \alpha = \{36, 36, 36, \ldots\} = \{1, 11, 36, 36, \ldots\}, \\ \beta = \{-1, -1, -1, \ldots\} = \{4, 24, 124, \ldots\}. \end{gathered} \tag{10}$$

There is another way to express a p-adic number. From the condition, $x_k \equiv y_k \bmod p^k$, it can deduce that and where ai is integer $x_k = a_{k-1} p^{k-1} + x_{k-1}$, $x_2 = a_1 p + x_1$, and $0 < ai < p - 1$. The sequence ai is called p-adic digits. Then it can deduce that:

$$x_k = a_0 + a_1 p + a_2 p^2 + \ldots + a_{k-1} p^{k-1} . \tag{11}$$

For example 3.1, $\alpha = 36 = 1 + 2 \times 5 + 1 \times 52$, so the 5-adic digits are 1, 2, 1, 0, 0....

DOI: 10.54254/2753-8818/25/20240919

5. Properties of p-adic integer

5.1. Ring Z_p

By the multiplication and addition, it can find that $(Zp,\cdot,+)$ form a commutative ring:

$$\{xk\} + \{yk\} = \{xk + yk\}; \{xk\} \cdot \{yk\} = \{xk \cdot yk\}, \tag{12}$$

where xk and yk are p-adic integer. Here are several proposition of commutative ring Zp [1].

Proposition 5.1.1. Zp is an integral domain, which means Zp is a nonzero commutative ring that the product of two nonzero elements in the ring is nonzero.

Proposition 5.1.2. The p-adic numbers of valuation zero are the units of Zp. A unit u of a ring means that there exists v in the ring satisfies $uv = vu = 1$.

Proposition 5.1.3. Let $\alpha = xk \in Zp$. Then

$$\alpha \notin U\left(\mathrm{Z}_p\right) \Leftrightarrow p|\ \alpha \Leftrightarrow x_k \equiv 0 \bmod p \Leftrightarrow x_1 \equiv 0 \bmod p \Leftrightarrow x_k \equiv 0 \bmod p \forall k \geq 1,$$
$$p^n|\ \alpha \Leftrightarrow x_n \equiv 0 \quad \bmod p^n \Leftrightarrow x_k \equiv 0 \quad \bmod p^n \forall k \geq n, n \geq 1. \tag{13}$$

Proposition 5.1.4. Rp is a ring and $Z \subset Rp \subset Zp, Z \subset Rp \subset Q$. Then $Rp = Zp \cap Q$.

5.2. Field Q_p

It can define a field under a fraction of p-adic integer since Zp can form a commutative ring.

$$\mathrm{Q}_p = \left\{\alpha|\ \alpha, \beta \in \mathrm{Z}_p, \beta \neq 0\right\}\ , \tag{14}$$

where Zp is a subring and Q is subfield.

Furthermore, it can also define a norm on the set Qp.

Definition 5. 2 .1. Let p be prime integer. It can define p-adic norm of nonzero $x \in Qp$ to be;

$$|x|_p = p^{-v_p(x)}, \tag{15}$$

where $|0|p = 0$ and vp is the valuation of x.

Here are several propositions for the p-adic norm [8].

Proposition 5.2.1. Strong triangle inequality is satisfied for each p-adic norm on Qp, meaning that for each x and y, $|x + y|p \leq max\{ |x|p, |y|p \}$.

Theorem 5.2.1. (Ostrowski's theorem) exceptionally high absolute value standard for rational numbers Q is equivalent to a p-adic absolute value or the common real absolute value.

The idea of the theorem is that if the norm of any whole number is at least 1, then the size of any real number can be measured by raising its absolute value to some positive power. But if the size of a whole number is less than 1, then the least number n must to be the prime number p such that

$$\mathrm{P}x\,\mathrm{P}_p = \mathrm{P}p\,\mathrm{P}^{v_p(x)} \tag{16}$$

6. Extention of p-adic numbers

p-adic number is not only useful in number theory but also in other fields. In theoretical physics, p-adic numbers have been used to explore certain aspects of string theory and quantum mechanics. They have been proposed as a framework for understanding the non-archimedean aspects of these theories. n computer science, p-adic numbers can be used in algorithms for solving various mathematical problems, including those related to number theory and cryptography. They can also be used in computer algebra systems for symbolic mathematics.

DOI: 10.54254/2753-8818/25/20240919

7. Conclusion

In summary, p-adic numbers grew out of a desire to delve deeper into number theory, and they provide a unique way of measuring numerical magnitude, especially in the presence of prime numbers. This unique perspective, rich in properties and applications, enables p-adic numbers to become valuable tools in fields ranging from number theory to cryptography, providing new insights and expanding our mathematical horizons. In essence, p-adic numbers embody the evolving nature of mathematics, constantly reshaping our understanding of numerical phenomena.

References

[1] Gouvêa FQ 1997 Universitext Springer Berlin Heidelberg
[2] Bachman G 1964 Academic Press ISBN 0-12-070268-1
[3] Lee B, Peter GO 2023 Physics Reports 233 1 1-66 ISSN 0370-1573.
[4] Gouvêa, Fernando Q 1997 Springer ISBN 3-540-62911-4 Zbl 0874.11002
[5] Harrington, Charles I 2011 Honors Theses 992
[6] Robert A M 2000 Spri. Sci. Business Media
[7] Katok S 2007 American Mathematical Soc.
[8] Murty M R 2009 American Mathematical Soc.
[9] Hazewinkel M 2009 Handbook of Algebra North Holland 6 342
[10] Cassels JWS 1986 Cambridge University Press 3 0595 12006