What are $p$-adic Numbers?
What are They Used for?

U A Rozikov

Abstract. In this short paper we give a popular introduction to the theory of $p$-adic numbers. We give some properties of $p$-adic numbers distinguishing them to "good" and "bad". Some remarks about applications of $p$-adic numbers to mathematics, biology and physics are given.

1. $p$-Adic Numbers

$p$-adic numbers were introduced in 1904 by the German mathematician K Hensel. They are used intensively in number theory. $p$-adic analysis was developed (mainly for needs of number theory) in many directions, see, for example, [20, 50].

When we write a number in decimal, we can only have finitely many digits on the left of the decimal, but we can have infinitely many on the right of the decimal. They might “terminate” (and become all zeros after some point) but they might not. The $p$-adic integers can be thought of as writing out integers in base $p$, but one can have infinitely many digits to the left of the decimal (and none on the right; but the rational $p$-adic numbers can have finitely many digits on the right of the decimal). For example, the binary expansion of 35 is $1·2^5 + 1·2^2 + 0·2^1 + 0·2^0 + 1·2^{-1}$, often written in the shorthand notation 100101.

One has $1 = 0.111111111... = 0,(1)_2$. But what is $...111111,0_2 = (1)_2$? Compute $(1)_2 + 1$:

$$...111111,0_2 + ...000001,0_2 = ...000000,0_2$$

Hence $(1)_2 = -1$. This equality can be written as

$$\lim_{n \to \infty} \sum_{i=0}^{n-1} 2^i = \lim_{n \to \infty} (2^n - 1) = -1.$$ (1)

This limit equivalent to $\lim_{n \to \infty} 2^n = 0$. In real case one has $\lim_{n \to \infty} q^n = 0$ if and only if absolute value $|q|$ is less than 1. Remember that to define real numbers one considers all limit points of sequences of rational numbers, using the absolute value as metric.

To give a meaning of the limit (1), one has to give a new absolute value $| \cdot |$, on the set of rational numbers, such that $|2|_2 < 1$. This is done as follows. Let $Q$ be the field of rational numbers. Every rational number $x \neq 0$ can be represented in the form $x = p^r \frac{a}{m}$, where $r, a, m$ is a positive integer, $(p, n) = 1$, $(p, m) = 1$ and $p$ is a fixed prime number. The $p$-adic absolute value (norm) of $x$ is given by

$$|x|_p = \begin{cases} p^{-r}, & \text{for } x \neq 0, \\ 0, & \text{for } x = 0. \end{cases}$$

The $p$-adic norm satisfies the so called strong triangle inequality

$$|x + y|_p \leq \max\{|x|_p, |y|_p\},$$ (2)

and this is a non-Archimedean norm.

This definition of $|x|_p$ has the effect that high powers of $p$ become “small”, in particular $|2|_2 = 1/2^n$. By the fundamental theorem of arithmetic, for a given non-zero rational number $x$ there is a unique finite set of distinct primes $p_1, \ldots, p_r$ and a corresponding sequence of non-zero integers $a_1, \ldots, a_r$ such that $x = p_1^{a_1} \ldots p_r^{a_r}$. Then it follows that $|x|_p = p_1^{-a_1} \ldots p_r^{-a_r}$ for all $i = 1, \ldots, r$, and $|x|_p = 1$ for any other prime $p \notin \{p_1, \ldots, p_r\}$.

For example, take $63/550 = 2^{-1} \cdot 3^2 \cdot 5^{-2} \cdot 7^{-1}$ we have

$$\left| \frac{63}{550} \right|_p = \begin{cases} 2, & \text{if } p = 2, \\ 1/9, & \text{if } p = 3, \\ 25, & \text{if } p = 5, \\ 1/7, & \text{if } p = 7, \\ 11, & \text{if } p = 11, \\ 1, & \text{if } p \geq 13. \end{cases}$$

We say that two norms $\| \cdot \|_1$ and $\| \cdot \|_2$ on $Q$ are equivalent if there exists $\alpha > 0$ such that

$$\| \cdot \|_1^\alpha = \| \cdot \|_2.$$ (for all $x, y \in Q$ and $\alpha > 0$)

It is a theorem of Ostrowski (see [41]) that each absolute value on $Q$ is equivalent either to the Euclidean absolute value $| \cdot |$, the trivial absolute value, or to one of the $p$-adic absolute values for some prime $p$. So the only norms on
Q modulo equivalence are the absolute value, the trivial absolute value and the p-adic absolute value which means that there are only as many completions (with respect to a norm) of Q.

The p-adic absolute value defines a metric on Q. Two numbers x and y are p-adically closer as long as r is higher, such that p^r divides |x−y|. Amazingly, for p = 5 the result is that 135 is closer to 10 than 35.

The completion of Q with respect to p-adic norm defines the p-adic field which is denoted by Qp. Any p-adic number x ≠ 0 can be uniquely represented in the canonical form

\[ x = p^{\gamma(x)}(x_0 + x_1p + x_2p^2 + \cdots), \]

where \( γ = γ(x) ∈ \mathbb{Z} \) and \( x_j \) are integers, \( 0 ≤ x_j ≤ p−1, \) \( x_0 > 0, \) \( j = 0, 1, 2, \ldots \) (see more detail [31, 50, 54]). In this case \( |x|_p = p^{−γ(x)} \). The set of p-adic numbers contains the field of rational numbers Q but is different from it.

Using canonical form of p-adic numbers, similarly as real numbers, one makes arithmetic operations on p-adic numbers (see for example, [41]).

2. “Good” Properties of p-Adic Numbers

The ultra-metric triangle inequality, i.e. (2), underlies many of the interesting differences between real and p-adic analysis. The following properties of p-adic numbers make some directions of the p-adic analysis more simple than real analysis:

1. All triangles are isosceles.
2. Any point of ball \( D(a, r) = \{ x ∈ Q_p : |x−a|_p ≤ r \} \) is center. Each ball has an empty boundary. Two balls are either disjoint, or one is contained in the other.
3. \( |1|_p = |p|_p \), if \( p \neq 2, \) and \( p = 1 \mod 4 \).
4. A sequence \( \{ x_n \} \) in Qp is a Cauchy sequence if and only if \( |x_{n+1} − x_n|_p \rightarrow 0 \) as \( n \rightarrow ∞ \).

This has the useful corollary that a sum converges if and only if the individual terms tend to zero:

6. (A student’s dream) \( \sum_{n=0}^{∞} a_n < ∞ \) if and only if \( a_n → 0 \).

Since \( n! → 0 \) we have, for example,

\[ \sum_{n=0}^{∞} (−1)^n!/(n+2) = 1, \sum_{n=0}^{∞} (−1)^n!/(n^2 − 5) = −3. \]

The sum \( \sum_{n=0}^{∞} n! \) exists in every \( Q_p \). The following problem has been open since 1971.

Problem. Can \( \sum_{n=0}^{∞} n! \) be rational for some prime \( p \)?

It is not known if \( \sum_{n=0}^{∞} n! \neq 0 \) in every Qp.

7. For any \( x ∈ Q_p \), we have

\[ |x| \prod_{p \text{ prime}} |x|_p = 1. \]

This formula have been used to solve several problems in number theory, many of them using Helmut Hasse’s local-global principle, which roughly states that an equation can be solved over the rational numbers if and only if it can be solved over the real numbers and over the p-adic numbers for every prime \( p \).

3. “Bad” Properties of p-Adic Numbers

1. \( Q_p \) is not ordered.
2. \( Q_p \) is not comparable with \( R \), for example \( \sqrt{7} \notin Q_5 \), but \( i = \sqrt{-1} \in Q_5 \).
3. \( Q_p \) is not algebraically closed.

But \( |1|_p \) can be extended uniquely to the algebraic closure \( \bar{Q}_p \) and the completion of \( (Q_p^- \cup \Gamma_p) \) is called \( \bar{C}_p \), the field of the p-adic complex numbers. \( C_p \) is no locally compact, but separable and algebraically closed.

Now define the functions \( \exp_p(x) \) and \( \log_p(x) \). Given \( a ∈ Q_p \) and \( r > 0 \) put

\[ B(a, r) = \{ x ∈ Q_p : |x−a|_p < r \}. \]

The p-adic logarithm is defined by the series

\[ \log_p(x) = \log_p(1 + (x−1)) = \sum_{n=1}^{∞} (−1)^{n+1}/n \cdot (x−1)^n, \]

which converges for \( x ∈ B(1, 1) \).

The p-adic exponential is defined by

\[ \exp_p(x) = \sum_{n=0}^{∞} x^n/n!, \]

which converges for \( x ∈ B(0, p^{−1/(p−1)}) \).

Let \( x ∈ B(0, p^{−1/(p−1)}) \), then

\[ |\exp_p(x) − 1|_p = |x|_p, \log_p(1 + x) = |x|_p, \log_p(\exp_p(x)) = x, \exp_p(\log_p(1 + x)) = 1 + x. \]

4. Some “good” functions become “bad”. For example \( \exp(x) \) is very “good” function on \( R \), but as we seen above \( \exp_p(x) \) is defined only on ball \( B(0, p^{−1/(p−1)}) \).
4. Remarks about Applications

When the \( p \)-adic numbers were introduced they considered as an exotic part of pure mathematics without any application (see for example [41, 42, 50, 56] for applications of \( p \)-adic numbers to mathematics). Since \( p \)-adic numbers have the interesting property that they are said to be close when their difference is divisible by a high power of \( p \) the higher the power the closer they are. This property enables \( p \)-adic numbers to encode congruence information in a way that turns out to have powerful applications in number theory including, for example, in the famous proof of Fermat’s Last Theorem by Andrew Wiles (see [42, Chap. 7]).

What is the main difference between real and \( p \)-adic space-time? It is the Archimedean axiom. According to this axiom any given large segment on a straight line can be surpassed by successive addition of small segments along the same line. This axiom is valid in the set of real numbers and is not valid in \( \mathbb{Q}_p \). However, it is a physical axiom which concerns the process of measurement. To exchange a number field \( R \) to \( \mathbb{Q}_p \) is the same as to exchange axiomatics in quantum physics (see [31, 56]).

In 1968 two pure mathematicians, A Monna and F van der Blij, proposed to apply \( p \)-adic numbers to physics. In 1972 E Beltrametti and G Cassinelli investigated a model of \( p \)-adic valued quantum mechanics from the positions of quantum logic. Since 80th \( p \)-adic numbers are used in applications to quantum physics. \( p \)-adic strings and super strings were the first models of \( p \)-adic quantum physics (see, for example, [17, 29, 50, 54]). The interest of physicists to \( p \)-adic numbers is explained by the attempts to create new models of space-time for the description of (fantastically small) Planck distances.

There are some evidences that the standard model based on real numbers is not adequate to Planck’s domain. On the other hand, some properties of fields of \( p \)-adic numbers seem to be closely related to Planck’s domain. In particular, the fields of \( p \)-adic numbers have no order structure.

The pioneer investigations on \( p \)-adic string theory induced investigations on \( p \)-adic quantum mechanics and field theory (see the books [31, 54, 55]). This investigations induce a development of \( p \)-adic mathematics in many directions: theory of distributions [6, 31], differential and pseudodifferential equations [32, 56], theory of probability [31, 56] spectral theory of operators in a \( p \)-adic analogue of a Hilbert space [7, 8, 33].

The representation of \( p \)-adic numbers by sequences of digits gives a possibility to use this number system for coding of information. Therefore \( p \)-adic models can be used for the description of many information processes. In particular, they can be used in cognitive sciences, psychology and sociology. Such models based on \( p \)-adic dynamical systems [3–5].

The study of \( p \)-adic dynamical systems arises in Diophantine geometry in the constructions of canonical heights, used for counting rational points on algebraic varieties over a number field, as in [21].

There most recent monograph on \( p \)-adic dynamics is Anashin and Khrennikov [9]; nearly a half of Silverman’s monograph [52] also concerns \( p \)-adic dynamics.

Here are areas where \( p \)-adic dynamics proved to be effective: computer science (straight line programs), numerical analysis and simulations (pseudorandom numbers), uniform distribution of sequences, cryptography (stream ciphers, \( T \)-functions), combinatorics (Latin squares), automata theory and formal languages, genetics. The monograph [9] contains the corresponding survey. For a newer results see recent papers and references therein: [10, 14, 15, 28, 36, 37, 38, 48, 51]. Moreover, there are studies in computer science and cryptography which along with mathematical physics stimulated in 1990th intensive research in \( p \)-adic dynamics since it was observed that major computer instructions (and therefore programs composed of these instructions) can be considered as continuous transformations with respect to the 2-adic metric, see [11, 12].

In [33, 53] \( p \)-adic field have arisen in physics in the theory of superstrings, promoting questions about their dynamics. Also some applications of \( p \)-adic dynamical systems to some biological, physical systems has been proposed in [3, 4, 5, 22, 23, 33, 35]. Other studies of non-Archimedean dynamics in the neighborhood of a periodic point and of the counting of periodic points over global fields using local fields appear in [39, 47]. It is known that the analytic functions play important role in complex analysis. In the \( p \)-adic analysis
the rational functions play a role similar to that of analytic functions in complex analysis [49]. Therefore, there naturally arises a question on study the dynamics of these functions in the $p$-adic analysis. On the other hand, these $p$-adic dynamical systems appear while studying $p$-adic Gibbs measures [26, 24, 44–46]. In [18, 19] dynamics on the Fatou set of a rational function defined over some finite extension of $\mathbb{Q}_p$ have been studied, besides, an analogue of Sullivan’s no wandering domains theorem for $p$-adic rational functions which have no wild recurrent Julia critical points was proved. In [27] the behaviour and ergodicity of a $p$-adic dynamical system $f(x) = x^a$ in the fields of $p$-adic numbers $\mathbb{Q}_p$ and complex $p$-adic numbers $\mathbb{C}_p$ was investigated. Firstly, the problem of ergodicity of perturbed monomial dynamical systems which was posed in these papers and which stimulated intensive research, was solved in [13]. Secondly, quite recently a far-going generalisation of the problem for arbitrary 1-Lipschitz transformations of 2-adic spheres was also solved in [16]. Finally, we note that not only polynomial and rational $p$-adic dynamical systems has been studied: In past decade, a significant progress was achieved in a study of a very general $p$-adic dynamical systems like non-expansive, locally analytic, shift-like, etc.

It is also known [33, 41, 43, 56] that a number of $p$-adic models in physics cannot be described using ordinary Kolmogorov’s probability theory. In [34] an abstract $p$-adic probability theory was developed by means of the theory of non-Archimedean measures. Applications of the non-Kolmogorov theory of probability can be considered not only in physics, but in many other sciences, especially in biology and possibly in sociology. The general principle of statistical stabilisation of relative frequencies is a new possibility to find a statistical information in the chaotic (from the real point of view) sequences of frequencies [31, 1, 2].

We refer the reader to [30, 24, 44–46] where various models of statistical physics in the context of $p$-adic fields are studied.

A non-Archimedean analogue of the Kolmogorov theorem was proved in [25]. Such a result allows to construct wide classes of stochastic processes and the possibility to develop statistical mechanics in the context of $p$-adic theory.

References


U A Rozikov is a professor in Institute of Mathematics, Tashkent, Uzbekistan. He graduated from the Samarkand State University (1993). He obtained PhD (1995) and Doctor of Sciences in physics and mathematics (2001) degrees from the Institute of Mathematics, Tashkent. He is known for his works on the theory of Gibbs measures of models on trees of statistical mechanics (recently he published a book: *Gibbs Measures on Cayley Trees* (World Scientific, 2013)). He developed a contour method to study the models on trees and described complete set of periodic Gibbs measures. Rozikov has (with F Mukhamedov) an important contribution to non-Archimedean theory of phase transitions and dynamical systems. He has important results on non-Volterra quadratic operators. N Ganikhodjaev and Rozikov gave a construction of a quadratic operator which connects phases of the models of statistical mechanics with models of genetics. His most recent works are devoted to evolution algebras of sex-linked populations. He was invited to several leading universities and research centres in the UK, France, Italy, Germany, Spain etc. His (more than 100) papers are published in front-line journals.
I've no idea what this is about, but I'm guessing that Susskind is somehow drawing inspiration from two facts: p-adic integers can be represented using a tree diagram vaguely reminiscent of the logo for the Stanford theoretical physics group on their website. The p-adic integers, unlike the usual integers, are compact, so you can put a finite measure on them. It's hard to believe that any of the special features of these mathematical structures will make the problems of eternal inflation go away, but who knows… Coincidentally, I've spent a lot of time recently learning about the p-adics, with... P-adic integers correspond to power series expansions, p-adic numbers to Laurent series. In particular, two p-adic numbers are considered to be close when their difference is divisible by a high power of p: the higher the power, the closer they are. This property enables p-adic numbers to encode congruence information in a way that turns out to have powerful applications in number theory including, for example, in the famous proof of Fermat's Last Theorem by Andrew Wiles.[1]. This is what allows the development of calculus on Qp, and it is the interaction of this analytic and algebraic structure that gives the p-adic number systems their power and utility. The p in "p-adic" is a variable and may be replaced with a prime (yielding, for instance, "the 2-adic numbers") or another placeholder variable (for expressions such as "the â”-adic numbers").