The p-Adic Numbers of Hensel
Author(s): C. C. MacDuffee
Source: *The American Mathematical Monthly*, Vol. 45, No. 8 (Oct., 1938), pp. 500-508
Published by: Taylor & Francis, Ltd. on behalf of the Mathematical Association of America
Stable URL: https://www.jstor.org/stable/2303739
Accessed: 24-10-2024 15:09 UTC

THE p-ADIC NUMBERS OF HENSEL*

C. C. MacDUFFEE, University of Wisconsin

1. Introduction. One cannot blame a respectable mathematician for looking twice at the equation

$$-1 = 4 + 4\cdot 5 + 4\cdot 5^2 + 4\cdot 5^3 + \cdots .$$

However, if we add 1 to both sides of this equation, we have

$$\begin{aligned} 0 &= 5 + 4\cdot 5 + 4\cdot 5^2 + 4\cdot 5^3 + \cdots \\ &= 0 + 5\cdot 5 + 4\cdot 5^2 + 4\cdot 5^3 + \cdots \\ &= 0 + \quad 0 + 5\cdot 5^2 + 4\cdot 5^3 + \cdots \\ &= 0 + \quad 0 + \quad 0 + 5\cdot 5^3 + \cdots \\ &= 0 + \quad 0 + \quad 0 + \quad 0 + \cdots \end{aligned}$$

with 0's as far out as we care to carry it.

It may also seem a trifle strange to write

$$2/3 = 4 + 1\cdot 5 + 3\cdot 5^2 + 1\cdot 5^3 + 3\cdot 5^4 + \cdots ,$$

where the coefficients beyond the first are alternately 1 and 3. Yet multiplying by 3 gives

$$\begin{aligned} 2 &= 12 + 3\cdot 5 + 9\cdot 5^2 + 3\cdot 5^3 + 9\cdot 5^4 + \cdots \\ &= \ 2 + \quad 0 + \quad 0 + \quad 0 + \quad 0 + \cdots . \end{aligned}$$

Furthermore

$$\sqrt{7} = 1 + 1\cdot 3 + 1\cdot 3^2 + 0\cdot 3^3 + 2\cdot 3^4 + \cdots .$$

For if we square this series, retaining only terms whose exponents are $\leqq 4$, we have

$$\begin{aligned} 7 &= 1 + 2\cdot 3 + 3\cdot 3^2 + 2\cdot 3^3 + 5\cdot 3^4 + \cdots \\ &= 1 + 2\cdot 3 + \quad 0 + \quad 0 + \quad 0 + \cdots . \end{aligned}$$

2. Justification of the p-adic numbers. No one will deny that the above examples put a heavy strain on our earlier conceptions of the terms *equality* and *convergence*. It is obvious that the statement

$$-1 = 4 + 4\cdot 5 + 4\cdot 5^2 + 4\cdot 5^3 + \cdots$$

is absurd if ordinary convergence is intended. The whole point to Hensel's theory is that this is not ordinary convergence, but a new type of convergence which, from the point of view of abstract algebra, is equally worthy of the name.

A relation of equality for a mathematical system Σ is defined as follows. Let a, b, and c be elements of Σ. Then

* Presented for the Slaught Memorial Volume of the MONTHLY.

1. Either $a=b$ or $a\neq b$ (Determinative property).
2. $a=a$ (Reflexive).
3. If $a=b$, then $b=a$ (Symmetric).
4. If $a=b$ and $b=c$, then $a=c$ (Transitive).

These four properties of equality are all that are needed in mathematics, and consequently constitute an abstract formulation of the concept.

When Hensel* introduced the p-adic numbers, his treatment was somewhat informal, but he had a perfectly sound feeling for what he was doing. The present vogue is to introduce the p-adic numbers by a method due to Kürschák,† similar to the well known development of the real numbers by Cauchy sequences.‡

Let $a, b, \cdots$ be rational numbers. A function ϕ is called a *valuation* if

1. $\phi(a)$ is a positive number or 0,
2. $\phi(a)>0$ for $a\neq 0$, $\phi(0)=0$,
3. $\phi(ab)=\phi(a)\cdot\phi(b)$,
4. $\phi(a+b)\leqq\phi(a)+\phi(b)$.

From (3) with $b=1$, we have $\phi(1)=1$. From (3) with $a=b=-1$, we have $\phi(-1)=1$. Then, with $a=-1$, we have $\phi(-b)=\phi(b)$.

Clearly ordinary absolute value, $\phi(a)=|a|$, is a valuation. Furthermore, the four properties listed above constitute an abstract formulation of the concept of absolute value in the sense that only these properties are needed for the development of the real numbers from the rational numbers by the method of regular sequences.

We recall that the ordinary integers or whole numbers $0, \pm 1, \pm 2, \pm 3, \cdots$ are called the *rational integers*, to distinguish them from algebraic integers such as $-\frac{1}{2}-\frac{1}{2}\sqrt{-3}$ which are not rational. A *rational prime* such as $\pm 2, \pm 3, \pm 5, \pm 7 \cdots$ is a rational integer neither 0 nor ± 1 such that, if it is resolved into a product of two rational integral factors, one of the factors must be 1 or -1. Two integers are *relatively prime*, or *prime to each other*, if their only common divisors are ± 1.

Let p be a fixed rational prime. Every rational number $a\neq 0$ is uniquely expressible in the form

$$a = (r/s)p^n, \qquad s > 0,$$

where r and s are rational integers prime to each other and to p, and n is a rational integer. We define

$$\phi(a) = p^{-n}, \qquad a \neq 0, \qquad \phi(0) = 0.$$

The function $\phi(a)$ is a valuation for the rational field.

Properties (1) and (2) are evident. If

* K. Hensel, Theorie der algebraischen Zahlen, Teubner, 1908.

† J. Kürschák, Journal fur die reine und angewandte Mathematik, vol. 142, 1913, pp. 211–253.

‡ See B. L. van der Waerden, Moderne Algebra, 2nd ed. I, Springer 1937, p. 221.

$$a = (r_1/s_1)p^m, \qquad b = (r_2/s_2)p^n,$$

where r_1, s_1, r_2, and s_2 are prime to p, then

$$ab = (r_1r_2/s_1s_2)p^{m+n},$$

where r_1r_2 and s_1s_2 are prime to p. Hence

$$\phi(ab) = p^{-m-n} = \phi(a)\cdot\phi(b).$$

Without loss of generality assume that $m \leqq n$. Then

$$a + b = \frac{r_1s_2 + r_2s_1p^{n-m}}{s_1s_2}\,p^m,$$

where s_1s_2 is prime to p, so that

$$\phi(a + b) \leqq p^{-m} = \phi(a),$$
$$\phi(a + b) \leqq \phi(a) + \phi(b).$$

Let p be a fixed prime, and let ϕ be defined relative to p. A sequence

$$\{a_i\} = (a_1, a_2, a_3, \cdots, a_i, \cdots)$$

of rational numbers is called *regular* if for every positive rational number ϵ there is a positive integer n_ϵ such that

$$\phi(a_i - a_j) < \epsilon \qquad i, j > n_\epsilon.$$

Denote by Ω_p the set of all regular sequences $\{a_i\}$. Two such sequences are defined to be *equal* if, for every ϵ, there is an n_ϵ such that

$$\phi(a_i - b_i) < \epsilon \qquad i > n_\epsilon.$$

Equality as defined above is determinative, reflexive, symmetric, and transitive.

The determinative property is evident. The reflexive property follows from the definition of regularity. Symmetry follows from the fact that $\phi(-a) = \phi(a)$. Transitivity follows from the "triangle property" $\phi(a+b) \leqq \phi(a)+\phi(b)$.

The theory now proceeds as in the usual treatment of real numbers as regular sequences. We define

$$\{a_i\} + \{b_i\} = \{a_i + b_i\}, \qquad \{a_i\}\cdot\{b_i\} = \{a_ib_i\}.$$

The sum and product of regular sequences are regular. The set Ω_p of all regular sequences, with equality, addition, and multiplication as we have defined them, is a field of characteristic zero—that is, it is a field which contains a subfield isomorphic with the rational field. Indeed, two fields Ω_p and Ω_q where p and q are distinct primes are non isomorphic so that we obtain infinitely many essentially different fields, each, of course, different from the real field. But like the real field every Ω_p is perfect—that is, incapable of further extension by means of regular sequences based on a valuation which extends the valuation by which Ω_p was defined.

It is one of the standard procedures in analysis to show that every real number can be represented as an infinite decimal—that is, a series of the type

$$a_{-\nu}\left(\frac{1}{10}\right)^{-\nu} + \cdots + a_0 + a_1\left(\frac{1}{10}\right) + a_2\left(\frac{1}{10}\right)^2 + \cdots$$

or the negative of such a series, with $0 \leqq a_i < 10$. This process can be carried over intact to the p-adic fields. It may be proved that every regular p-adic sequence is equal in the p-adic sense to a sequence

$$p^{-\nu}\{d_i\}, \qquad \{d_i\} = (a_0,\ a_0 + a_1 p,\ a_0 + a_1 p + a_2 p^2, \cdots), \qquad 0 \leqq a_i < p.$$

That is, every p-adic number may be represented by a power series

$$a_{-\nu}p^{-\nu} + \cdots + a_0 + a_1 p + a_2 p^2 + \cdots, \qquad 0 \leqq a_i < p.$$

Just as the infinite decimal is automatically convergent in the Cauchy sense, so is the above series automatically convergent in the p-adic sense.

It is to be emphasized that for every rational prime p there is a field Ω_p quite comparable with the field of real numbers, but not isomorphic with it, nor with any other Ω_p. The field Ω_2 is the field of all *diadic* numbers, Ω_3 of all *triadic* numbers, Ω_5 of all *pentadic* numbers, etc. Once the field has been selected, all calculations remain in this field. We cannot add or multiply a triadic number and a pentadic number, for instance.

3. Solution of equations. Now that we understand the meaning of a statement such as

$$\sqrt{7} = 1 + 1\cdot 3 + 1\cdot 3^2 + 0\cdot 3^3 + 2\cdot 3^4 + \cdots,$$

it remains to show how any desired number of terms of the expansion can be derived.

First we note that every p-adic number

$$a_{-\nu}p^{-\nu} + \cdots + a_0 + a_1 p + a_2 p^2 + \cdots, \qquad 0 \leqq a_i < p,$$

is the sum of a rational number

$$a_{-\nu}p^{-\nu} + \cdots + a_{-1}p^{-1}$$

and a number

$$a_0 + a_1 p + a_2 p^2 + \cdots$$

having no negative exponents, which is called an *integral p-adic number*, or a *p-adic integer*.

Two p-adic integers

$$\alpha = a_0 + a_1 p + a_2 p^2 + \cdots, \qquad 0 \leqq a_i < p,$$
$$\beta = b_0 + b_1 p + b_2 p^2 + \cdots, \qquad 0 \leqq b_i < p,$$

are equal in the p-adic sense, according to the definition of §2, if for every $\epsilon > 0$

there is an n_ϵ such that for $i > n_\epsilon$,

$$\phi((a_0 - b_0) + (a_1 - b_1)p + (a_2 - b_2)p^2 + \cdots + (a_i - b_i)p^i) < \epsilon.$$

Suppose that $a_0 = b_0$, $a_1 = b_1$, $\cdots$, and that k is the first integer for which $a_k \neq b_k$, so that $a_k - b_k$ is prime to p. Then

$$\phi((a_k - b_k)p^k + (a_{k+1} - b_{k+1})p^{k+1} + \cdots + (a_i - b_i)p^i) = 1/p^k,$$

so that if we take $\epsilon < 1/p^k$, the condition that $\alpha = \beta$ is not met. Thus *if* $\alpha = \beta$, *corresponding coefficients are equal.* The converse is evident.

Now if

$$\alpha = a_0 + a_1 p + a_2 p^2 + \cdots, \qquad 0 \leqq a_i < p,$$

then clearly

$$\begin{aligned}
&\alpha \equiv a_0 \pmod{p},\\
&\alpha \equiv a_0 + a_1 p \pmod{p^2},\\
&\alpha \equiv a_0 + a_1 p + a_2 p^2 \pmod{p^3},\\
&\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\\
&\alpha \equiv a_0 + a_1 p + \cdots + a_{i-1} p^{i-1} \pmod{p^i}.
\end{aligned}$$

Thus the coefficients $a_0, a_1, a_2, \cdots$, in the expansion of α can be successively determined from the residues of α modulo p^i, $i = 1, 2, \cdots$. In other words, $\alpha = \beta$ *if and only if*

$$\alpha \equiv \beta \pmod{p^i}$$

for every positive integer i.

Let $f(x)$ be a polynomial with rational integral coefficients, and let p be a fixed rational prime. We wish to find out if $f(x) = 0$ has a solution α in Ω_p, and to determine an arbitrary number of its coefficients.

First, suppose that $f(x) = 0$ has an integral p-adic solution, *e.g.*,

$$\alpha = a_0 + a_1 p + a_2 p^2 + a_3 p^3 + \cdots, \qquad 0 \leqq a_i < p.$$

Denote

$$\alpha_{n-1} = a_0 + a_1 p + a_2 p^2 + \cdots + a_{n-1} p^{n-1}.$$

Thus α is a solution of $f(x) = 0$ in Ω_p if and only if

$$f(\alpha) \equiv 0 \pmod{p^i} \qquad (i = 1, 2, 3, \cdots);$$

that is to say, if and only if each of the infinitely many congruences

$$\begin{aligned}
&f(\alpha_0) \equiv 0 \pmod{p},\\
&f(\alpha_1) \equiv 0 \pmod{p^2},\\
&f(\alpha_2) \equiv 0 \pmod{p^3},\\
&\cdots\cdots\cdots\cdots
\end{aligned}$$

$$f(\alpha_{n-1}) \equiv 0 \pmod{p^n},$$
$$\cdots\cdots\cdots\cdots$$

holds.

The problem is now reduced to a familiar one in congruences. Whether $f(x) \equiv 0 \pmod{p}$ has a solution or not is usually best determined by trial. If there is a solution, there is a solution α_0, $0 \leqq \alpha_0 < p$.

Now there is a well known step-by-step process for finding a solution (mod p^{n+1}) when a solution (mod p^n) is known.* Suppose that

$$\alpha_{n-1} = a_0 + a_1 p + a_2 p^2 + \cdots + a_{n-1} p^{n-1}, \qquad f(\alpha_{n-1}) \equiv 0 \pmod{p^n}.$$

We wish to find a_n so that

$$\alpha_n = \alpha_{n-1} + a_n p^n, \qquad f(\alpha_n) \equiv 0 \pmod{p^{n+1}}.$$

By the binomial theorem,

$$\begin{aligned} f(\alpha_n) &= f(\alpha_{n-1}) + a_n f'(\alpha_{n-1}) p^n + \cdots \\ &\equiv f(\alpha_{n-1}) + a_n f'(\alpha_{n-1}) p^n \pmod{p^{n+1}}, \end{aligned}$$

where f' denotes the derivative. Since $f(\alpha_{n-1}) \equiv 0 \pmod{p^n}$, there exists an integer h_{n-1} such that

$$f(\alpha_{n-1}) \equiv h_{n-1} p^n \pmod{p^{n+1}}, \qquad 0 \leqq h_{n-1} < p.$$

Hence a_n can be determined from the congruence

$$a_n f'(\alpha_{n-1}) p^n + h_{n-1} p^n \equiv 0 \pmod{p^{n+1}},$$

which is equivalent to the congruence

$$a_n f'(\alpha_{n-1}) + h_{n-1} \equiv 0 \pmod{p}. \tag{1}$$

Clearly a_n will exist unless $f'(\alpha_{n-1}) \equiv 0$, $h_{n-1} \not\equiv 0 \pmod{p}$. If it exists, it can be chosen in the interval $0 \leqq a_n < p$.

In order that

$$x^2 = 7$$

be solvable in triadic numbers, it is first necessary that 7 be a quadratic residue† modulo 3. This condition is met, for both 1 and 2 are solutions of $x^2 \equiv 7 \pmod{3}$. Let us take the first solution. Then $\alpha_0 = a_0 = 1$.

$$f(x) = x^2 - 7, \qquad f(\alpha_0) = -6 \equiv 3 \pmod{9}, \qquad h_0 \equiv 1 \pmod{3},$$
$$f'(x) = 2x, \qquad f'(\alpha_0) \equiv 2 \pmod{3}.$$

Then (1) becomes

---

* L. E. Dickson, Introduction to the theory of numbers, University of Chicago Press, 1929, p. 16, ex. 4.

† Dickson, *l.c.*, p. 30.

$$2a_1 + 1 \equiv 0 \pmod 3,$$

which has the solution $a_1 = 1$. Thus $\alpha_1 = 1 + 1 \cdot 3 = 4$ is a solution of $x^2 \equiv 7 \pmod 9$.

The second step gives $\alpha_1 = 4$,

$$f(\alpha_1) = 9, \qquad h_1 = 1, \qquad f'(\alpha_1) = 8 \equiv 2 \pmod 3,$$
$$2a_2 + 1 \equiv 0 \pmod 3, \qquad a_2 = 1, \qquad \alpha_2 = 1 + 1 \cdot 3 + 1 \cdot 3^2.$$

Two more steps give

$$\alpha_4 = 1 + 1 \cdot 3 + 1 \cdot 3^2 + 0 \cdot 3^3 + 2 \cdot 3^4,$$

which was checked in §1.

The other value of a_0, namely 2, is the first term of another triadic solution,

$$\beta = 2 + 1 \cdot 3 + 1 \cdot 3^2 + 2 \cdot 3^3 + 0 \cdot 3^4 + \cdots .$$

There are no other triadic solutions of $x^2 = 7$.

The equation

$$x^2 + x + 1 = 0,$$

whose roots in the complex field are not real has no solution in pentadic numbers, since

$$x^2 + x + 1 = 0 \pmod 5$$

has no solution. However, it has two heptadic solutions,

$$\alpha = 2 + 4 \cdot 7 + 6 \cdot 7^2 + \cdots ,$$
$$\beta = 4 + 2 \cdot 7 + 0 \cdot 7^2 + \cdots$$

with the usual relations $\alpha^2 = \beta$ and $\beta^2 = \alpha$. It is incorrect to think of these solutions as being complex numbers—they belong to the field Ω_7.

So far we have looked only for integral p-adic solutions of $f(x) = 0$. But if the leading coefficient of $f(x)$ is divisible by p while not all of the other coefficients are divisible by p, $f(x) = 0$ may have a p-adic solution which is not integral. But this situation involves no difficulty, for a simple transformation reduces this case to the preceding.

Consider the equation

$$9x^2 = 7, \qquad \Omega_3.$$

This has no integral triadic solution, since

$$9x^2 - 7 \equiv 0 \pmod 3$$

has no solution. But a transformation $3x = y$ yields an equation $y^2 = 7$ which we have solved in Ω_3. Then the given equation has as solutions the fractional triadic numbers

$$\alpha = \quad 3^{-1} + 1 + 1 \cdot 3 + 0 \cdot 3^2 + 2 \cdot 3^3 + \cdots ,$$
$$\beta = 2 \cdot 3^{-1} + 1 + 1 \cdot 3 + 2 \cdot 3^2 + 0 \cdot 3^3 + \cdots .$$

4. Rational numbers in Ω_p. The close analogy of the p-adic series with infinite decimals is well exemplified in the behavior of the rational numbers. A rational number r/s with r prime to s can be expressed as a finite decimal if and only if every prime factor of s is 2 or 5. A positive rational number r/s with r prime to s can be expressed by a finite p-adic series if and only if s is a power of p.

A decimal is finite or periodic if and only if it is equal to a rational number. Analogously

A p-adic series is finite or periodic if and only if it is equal to a rational number.

It will be sufficiently general to consider the series

$$\alpha = A + p^k B + p^{k+l} B + p^{k+2l} B + \cdots,$$

where

$$A = a_0 + a_1 p + \cdots + a_{k-1} p^{k-1}, \qquad 0 \leqq a_i < p,$$
$$B = b_0 + b_1 p + \cdots + b_{l-1} p^{l-1}, \qquad 0 \leqq b_i < p.$$

We shall call B the *period* of α. Then

$$\alpha - A = p^k B + p^l [p^k B + p^{k+l} B + \cdots] = p^k B + p^l [\alpha - A];$$

that is,

$$\alpha = A + \frac{p^k B}{1 - p^l},$$

which is clearly rational.

To prove the converse, first suppose that $\alpha = r/s$ is a negative proper rational fraction, r prime to s, s prime to p and positive. There exist positive integers l such that

$$p^l \equiv 1 \pmod{s}$$

by Euler's theorem. Let l be the smallest such integer—that is, l is the exponent to which p belongs* modulo s. Let

$$1 - p^l = ms, \qquad m < 0, \qquad mr > 0.$$

Then

$$\alpha = r/s = mr/(1 - p^l).$$

Since α is proper, mr is expressible in the form

$$mr = B = b_0 + b_1 p + \cdots + b_{l-1} p^{l-1}, \qquad 0 \leqq b_i < p.$$

Then

$$\alpha = B + p^l B + p^{2l} B + \cdots$$

is periodic.

* Dickson, *l.c.*, p. 16.

If α is positive, it can be written as the sum of a polynomial in p and a negative proper fraction. The development of $-\alpha$ can be obtained by subtracting the development of α from

$$0 = p\cdot 1 + (p-1)\cdot p + (p-1)\cdot p^2 + (p-1)\cdot p^3 + \cdots$$

Neither of these operations will destroy the eventual periodicity of the series.

The methods of this paragraph are quicker and more effective for rational numbers than the more general method of §3.

5. Generalizations. The ideas which were disclosed in the development of the p-adic numbers have inspired much modern research. Hensel* himself extended the theory far beyond the simple p-adic fields: to g-adic rings where g is not a prime, to p-adic extensions of algebraic fields, and to functions over such fields and rings. The concepts of valuation and p-adic extension are of great importance in the modern theory of linear algebras,† and their ramifications are still being explored.

A NOTE ON THE USE OF THE LAPLACE TRANSFORMATION

H. P. THIELMAN, College of St. Thomas

In recent years a great deal of work has centered around the Laplace transform of a function $F(t)$.‡ In this note we shall prove an elementary theorem concerning such a transform, and show how it may be used in evaluating some definite integrals.

By definition the Laplace transform of $F(t)$ is the function $f(\alpha)$ given by the formula

$$f(\alpha) = \int_0^\infty e^{-\alpha t}F(t)dt.$$

We shall first prove the following:

THEOREM: *If $f(\alpha)$ is the Laplace transform of $F(t)$, then*

$$\int_0^\infty f(\alpha)d\alpha = \int_0^\infty \frac{F(t)}{t}\,dt,$$

provided these integrals exist.

The proof of this theorem goes as follows: From the hypothesis that the second one of the last two integrals exists, it follows that the integral

---

* K. Hensel, Zahlentheorie, Berlin 1913. Mathematische Zeitschrift, vol. 2, 1918, pp. 433–452.

† Deuring, Algebren, Ergebnisse der Mathematik, vol. 4, Springer, 1935, p. 99.

‡ D. V. Widder, The inversion of the Laplace integral and the related moment problem, Transactions of the American Mathematical Society, vol. 36, 1934, p. 107; Necessary and sufficient conditions for the representation of a function by a doubly infinite Laplace integral, Bulletin of the American Mathematical Society, vol. 40, 1934, p. 321. H. T. Davis, The Theory of Linear Operators, Principia Press, Bloomington, Indiana, 1936, pp. 24, 25, 28 ff.