p-adic numbers

Trond Digernes

CIMPA Research School
CIMAT, Guanajuato, Mexico
23–31 May, 2022

Outline

p-adic numbers

In number theory:

- The p-adic numbers were invented by Kurt Hensel in 1897.
- They have played an important role in number theory since then.

In physics:

- In 1987 mathematical physicist I. V. Volovich proposed the bold hypothesis that the field of p-adic numbers could be a useful tool to describe phenomena below the Planck scale.

Every positive real number a can be written in the form

$$\begin{aligned} a &= a_n 10^n + a_{n-1} 10^{n-1} + \cdots + a_0 \\ &\quad + a_{-1} 10^{-1} + a_{-2} 10^{-2} + \cdots + a_{-k} 10^{-k} \cdots \\ &= a_n 10^n + a_{n-1} 10^{n-1} + \cdots + a_0 + \sum_{k=1}^{\infty} a_{-k} 10^{-k}, \end{aligned}$$

where the digits a_k satisfy $0 \leq a_k \leq 9$.
We could have used any other positive integer as base – for example a prime number p – and obtained

$$a = a_n p^n + a_{n-1} p^{n-1} + \cdots + a_0 + \sum_{k=1}^{\infty} a_{-k} p^{-k},$$

where now $0 \leq a_k \leq p-1$ (the coefficients a_k are, of course, not the same in the two developments).

Notice that we have a finite integer part and (in general) an infinite decimal part.
The p-adic numbers soon to be defined, turns this around: We shall give meaning to expressions of the form

$$a = a_{-n}p^{-n} + a_{-n+1}p^{-n+1} + \cdots + a_0 + \sum_{k=1}^{\infty} a_k p^k,$$

where we now have a finite ”decimal part” and an infinite "integer part".
To accomplish this, we must define a new absolute value on the rational numbers.

For a given prime number p, any rational number $x = a/b$ can be written in the form

$$x = p^n \frac{a'}{b'} \quad \text{where} \quad \gcd(p, a') = \gcd(p, b') = 1.$$

The exponent n is called the p-adic valuation of x, and is often denoted by ν; with the above notation:

$$\nu(x) = n.$$

We define the p-adic absolute value $|x|_p$ of x by

$$|x|_p = p^{-\nu(x)}.$$

Absolute values

This is an absolute value on the field of rational numbers which in addition to the usual requirements for an absolute value:

(1) $$|x|_p \geq 0 \text{ og } |x|_p = 0 \iff x = 0$$

(2) $$|x + y|_p \leq |x|_p + |y|_p$$

(3) $$|xy|_p = |x|_p \cdot |y|_p$$

also satisfies a stronger version of requirement (2):

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

An absolute value which satisfies (2') is said to be *non-Archimedean* or *ultrametric*.

Completion

The absolute value $|\cdot|_p$ gives rise to a metric d_p on the field of rational numbers $\mathbf{Q}$ by setting

$$d_p(x,y) = |x-y|_p.$$

- When the field of rational numbers $\mathbf{Q}$ is completed with respect to the usual absolute value, we get the field of real numbers $\mathbf{R}$.
- When the field of rational numbers $\mathbf{Q}$ is completed with respect to the p-adic absolute value $|\cdot|_p$, we get the field of p-adic numbers. It is denoted by $\mathbf{Q}_p$.
- Ostrowski's Theorem says that any absolute value on $\mathbf{Q}$ is equivalent either to the usual absolute value, or to one of the p-adic absolute values.

Some strange (and bizarre) consequences of the non-Archimedean property

The non-Archimedean property has some unusual geometric consequences:

1. $|x|_p \neq |y|_p \Rightarrow |x+y|_p = \max(|x|_p, |y|_p)$.
   As a consequence *all triangles in a non-Archimedean geometry are isosceles.*
2. Any point in a ball is a center for that ball.
3. If two balls intersect, one is contained in the other.
4. $|nx|_p \leq |x|_p$ for all integers n.
5. *A calculus student's dream:*
   For a series $\sum_{n=0}^{\infty} a_n$ to converge it suffices that $\lim_{n\to\infty} a_n = 0$ (in stark contrast to the real case).

Proofs of elementary properties I

1. We may assume $|x|_p > |y|_p$.

$$|x|_p > |y|_p \Longrightarrow |x|_p = |x+y-y|_p \leq \max(|x+y|_p, |y|_p)$$
$$= |x+y|_p \leq \max(|x|_p, |y|_p) = |x|_p \Longrightarrow |x+y|_p = |x|_p.$$

2. Set $B(a,r) = \{x : |x-a|_p \leq r\}$, and assume $b \in B(a,r)$. We must show that $B(a,r) = B(b,r)$.

$$x \in B(a,r) \Longrightarrow |x-b|_p = |x-a+a-b|_p$$
$$\leq \max(|x-a|_p, |a-b|_p) \leq r \Longrightarrow x \in B(b,r),$$

i.e., $B(a,r) \subset B(b,r)$. By symmetry we also get the reverse inclusion, and hence equality.

Proofs of elementary properties II

3. Assume $B(a, r_1) \cap B(b, r_2) \neq \emptyset$ with $r_1 \leq r_2$. We claim that $B(a, r_1) \subset B(b, r_2)$. To prove this, pick a $z \in B(a, r_1) \cap B(b, r_2)$, and proceed as follows:

$$x \in B(a, r_1) \Longrightarrow |x - b|_p = |x - a + a - z + z - b|_p$$
$$\leq \max(|x - a|_p, |a - z|_p, |z - b|_p) \leq \max(r_1, r_1, r_2) = r_2$$
$$\Longrightarrow x \in B(b, r_2),$$

i.e., $B(a, r_1) \subset B(b, r_2)$.

In $\mathbf{Q}_p$ a sufficient condition for a series $\sum_{k=0}^{\infty} a_k$ to converge is that $\lim_{k\to\infty} a_k = 0$. This follows from the ultrametric property. Namely, let $\epsilon > 0$ be given and let N be such that $|a_k| < \epsilon$ for $k \geq N$. Setting $s_n = \sum_{k=0}^{n} a_k$, then with $m > n \geq N$ we have

$$|s_m - s_n| = |a_{n+1} + \cdots + a_m| \leq \max(|a_{n+1}| + \cdots |a_m|) < \epsilon.$$

It follows that the sequence of partial sums (s_n) is Cauchy, hence it converges in the complete space $\mathbf{Q}_p$. In particular, any series of the form $\sum_{k=n}^{\infty} x_k p^k$ where $n \in \mathbf{Z}$ and $0 \leq x_k \leq p-1$ converges because $|x_k p^k| \leq p^{-k} \to 0$ as $k \to \infty$, and thus defines an element of $\mathbf{Q}_p$.
Conversely, any element of $\mathbf{Q}_p$ can be written in this form. More precisely we have the following:

Canonical form I

Theorem (Canonical form)

Every $x \in \mathbf{Q}_p$ with can be written uniquely as

$$x = p^{\nu(x)}(x_0 + x_1 p + x_2 p^2 + x_3 p^3 + \cdots) \tag{1}$$

$$= p^{\nu(x)} \sum_{k=0}^{\infty} x_k p^k, \qquad 0 \leq x_k \leq p-1, \qquad x_0 \neq 0. \tag{2}$$

This is called the *canonical form* of x.

Canonical form II

Proof.

First we observe that the set of series (2) forms a field: adding, multiplying and dividing such series are defined in the natural way, and subtraction is also possible (see slide 16). So it constitutes a subfield of $\mathbf{Q}_p$. To show that it is all of $\mathbf{Q}_p$, we only need to show that it is complete.

So suppose (x_n) with $x_n = \sum a_{kn} p^k$ is Cauchy. Then for each m there exists an N such that $|x_{n_1} - x_{n_2}|_p < p^{-m}$ if $n_1, n_2 > N$. But this can only happen if $a_{kn_1} = a_{kn_2}$ for $k \leq m$. Thus the sequences (a_{kn}) are eventually constant in n for each k. It follows that the limit $a_k = \lim_{n\to\infty} a_{kn}$ exists for every k, and that $\lim_{n\to\infty} x_n = \sum a_k p^k$. □

Notice that the above theorem on canonical form says that *all* p-adic numbers can be written in the form (2). In particular, this is true for negative rational numbers. For example, for $x = -1$ we have

$$-1 = \sum_{k=0}^{\infty}(p-1)p^k.$$

This is so because

$$\sum_{k=0}^{\infty}(p-1)p^k = (p-1)\sum_{k=0}^{\infty}p^k = (p-1)\frac{1}{1-p} = -1,$$

where we have used the usual formula for a convergent geometric series with factor p (the series converges because $|p| = \frac{1}{p} < 1$).

More generally: If

$$a = \sum_{k=n}^{\infty} a_k p^k$$

in standard form, then the standard form of $-a$ is given by

$$-a = \sum_{k=n}^{\infty} b_k p^k, \quad \text{where } b_n = p - a_n \text{ and } b_k = p - 1 - a_k \text{ for } i > n.$$

Total disconnectedness

Set $B_k(a) = \{x \in \mathbf{Q}_p || x - a|_p \leq p^k\}$: the closed ball of radius p^k centered at a, and $B_k^o(a) = \{x \in \mathbf{Q}_p || x - a|_p < p^k\}$: the open ball of radius p^k centered at a. Since $B_k^o(a) = B_{k-1}(a)$, all balls are both open and closed. I tfollows that $\mathbf{Q}_p$ is a totally disconnected metric space.
The balls $B_k(0)$ are additive subgroups of $\mathbf{Q}_p$, and for $k \leq 0$ they are also subrings. The special ball $B_0(0)$ is denoted by $\mathbf{Z}_p$, and is called the set of p-adic integers. Thus

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

It is a compact subring of $\mathbf{Q}_p$. Clearly, the positive rational integers $\mathbf{Z}_+$, and hence also the whole ring of rational integers $\mathbf{Z}$, are contained in $\mathbf{Z}_p$ as a dense subset.

Local compactness

$p\mathbf{Z}_p = B_{-1}(0)$ is a subgroup of $\mathbf{Z}_p$, and the quotient is the cyclic group $Z_p = \mathbf{Z}/p\mathbf{Z}$ of order p (in particular, $\mathbf{Z}_p/p\mathbf{Z}_p \simeq \mathbf{Z}/p\mathbf{Z}$). It follows that $\mathbf{Z}_p$ is the disjoint union of p cosets of $p\mathbf{Z}_p$, i.e., of p balls of radius p^{-1}. More generally, for $m > n$ we have that every ball $B_m(a)$ is the disjoint union of p^{m-n} balls of radius p^n. It follows that all balls are totally bounded, hence compact, since they also are closed in the complete metric space $\mathbf{Q}_p$. Thus we have established that $\mathbf{Q}_p$ is totally disconnected, locally compact group.

Characters I

For $x \in \mathbf{Q}_p$, denote by $\{x\}_p$ the fractional part of x:

$$\{x\}_p = \begin{cases} 0 & \text{if } x = 0 \text{ or } \nu \geq 0 \\ p^{\nu}(x_0 + x_1 p + \cdots + x_{|\nu|-1} p^{|\nu|-1}) & \text{if } \nu < 0 \end{cases}$$

where $\nu = \nu(x)$. We define the *basic character* χ_1 of $\mathbf{Q}_p$ by

$$\chi_1(x) = \exp(2\pi i \{x\}_p).$$

This is a continuous additive character of $\mathbf{Q}_p$.

Characters II

If $y \in \mathbf{Q}_p$, then χ_y, defined by

$$\chi_y(x) = \chi_1(yx),$$

is also a continous character. The claim is that these exhaust all the continuous characters of $\mathbf{Q}_p$, and that the mapping $y \mapsto \chi_y$ is an isomorphism between the additive group $\mathbf{Q}_p$ and its Pontryagin dual group $\widehat{\mathbf{Q}_p}$. More precisely we have:

Self-duality of $\mathbf{Q}_p$ I

Theorem

The mapping $y \in \mathbf{Q}_p \mapsto \chi_y \in \widehat{\mathbf{Q}_p}$ described above is a topological group isomorphism between the locally compact additive group $\mathbf{Q}_p$ and its Pontryagin dual group $\widehat{\mathbf{Q}_p}$.

We recall that the Pontryagin dual group of $\mathbf{Q}_p$ consists of the continuous characters of $\mathbf{Q}_p$ under multiplication, equipped with the compact-open topology.
Below we mention the main steps involved in proving this theorem.

Self-duality of $\mathbf{Q}_p$ II

The first step is the following lemma:

Lemma

If $\chi \in \widehat{\mathbf{Q}_p}$, there is an integer k such that $\chi = 1$ on $B_k(0)$.

Proof.

Since χ is continuous, there is an integer k such that χ maps $B_k(0)$ into the neighborhood $U = \{z \in \mathbf{T} : |z - 1| < 1\}$ of 1 in the unit circle $\mathbf{T}$. But $B_k(0)$ is a subgroup of $\mathbf{Q}_p$, so its image under χ is a subgroup of $\mathbf{T}$. But the only subgroup of $\mathbf{T}$ which is contained in the set U is the trivial subgroup. Hence $\chi = 1$ on $B_k(0)$. □

Self-duality of $\mathbf{Q}_p$ III

The next steps are listed without proof. For details see the book by Folland [1].

Lemma

Suppose $\chi \in \widehat{\mathbf{Q}_p}, \chi(1) = 1$ *and* $\chi(p^{-1}) \neq 1$. *There is a sequence* $(a_k)_0^\infty$ *with* $a_0 \in \{1, \ldots, p-1\}$ *and* $a_k \in \{0, \ldots, p-1\}$ *for* $k \geq 1$ *such that* $\chi(p^{-m}) = \exp(2\pi i \sum_1^m a_{m-k} p^{-k})$ *for* $m = 1, 2, 3, \cdots$.

Self-duality of $\mathbf{Q}_p$ IV

Lemma

If $\chi \in \widehat{\mathbf{Q}_p}, \chi(1) = 1$ *and* $\chi(p^{-1}) \neq 1$, *there is a* $y \in \mathbf{Q}_p$ *with* $|y|_p = 1$ *such that* $\chi = \chi_y$.

After these lemmas one checks that the mapping $y \mapsto \chi_y$ is a group isomorphism between $\mathbf{Q}_p$ and $\widehat{\mathbf{Q}_p}$, and that it is a homeomorphism when $\widehat{\mathbf{Q}_p}$ is equipped with the compact-open topology.

Examples with *p*-adic numbers

We conclude with a couple of examples illustrating some features of the *p*-adic numbers. The examples illustrate how *p*-adic solutions may show up naturally in the following situations:

- Solving a sequence of congruences.
- Using iterations to solve a fixed point problem.

The examples are taking from Gouvêa's book [2].

Solving congruences

If we wish to investigate whether there are integer solutions to an equation

$$P(x) = 0$$

where $P(x)$ is a polynomial with integer coefficients, we can proceed as follows: Determine the coefficients x_i in the development $x = x_0 + x_1 p + \cdots + x_n p^n$ one by one by successively solving the congruenses

$$\begin{aligned} P(x) &\equiv 0 \mod p^1 \\ P(x) &\equiv 0 \mod p^2 \\ &\vdots \\ P(x) &\equiv 0 \mod p^n \end{aligned}$$

This process can have the following outcomes:

1. We get a contradiction after a finite number of steps: No solution.
2. We get $x_i = 0$ for $i > n$: We have a solution.
3. The process continues indefinitely, and we get a seemingly meaningless solution of the form

$$x = \sum_{i=0}^{\infty} x_i p^i. \tag{3}$$

Here two things can happen:

1. The solution (3) represents a (rational) integer, and we have a solution also in this case.
2. The solution (3) represents a p-adic integer, and we have a p-adic solution which is not a rational number (and not a real number, either).

We illustrate this method with an example from Gouvêa's book [2]: solving the equation $x^2 = 25$. For definiteness, take $p = 3$. Of course, in this case we know what the answers are – namely $x = \pm 5$ – and both of these solutions will satisfy all the congruences. But let's pretend we didn't know this, and that we simply solved the congruences by hand, insisting that the solutions be written in the form (2) on slide 13.

For the first solution $x = 5$ we get

$$\begin{aligned} x &\equiv 5 \equiv 2 \pmod 3 \\ x &\equiv 5 = 2 + 3 \pmod 9 \\ x &\equiv 5 = 2 + 3 \pmod{27} \end{aligned}$$

etc.,

and nothing changes after this since we have obtained the 3-adic expansion of $x = 5 = 2 + 1 \times 3$.

For $x = -5$ we get

$$x \equiv -5 \equiv 1 \pmod 3$$
$$x \equiv -5 \equiv 4 = 1 + 3 \pmod 9$$
$$x \equiv -5 \equiv 22 = 1 + 3 + 2 \times 9 \pmod{27}$$
$$x \equiv -5 \equiv 76 = 1 + 3 + 2 \times 9 + 2 \times 27 \pmod{81}$$

etc.

We convince ourselves that we get an infinite expansion as follows

$$x = -5 = 1 + 1 \times 3 + 2 \times 3^2 + 2 \times 3^3 + 2 \times 3^4 + \cdots$$
$$= 4 + 2 \sum_{k=2}^{\infty} 3^k$$

We check that the expression on the right hand side above gives the correct solution:

$$4+2\sum_{k=2}^{\infty}3^k=4+2\cdot 3^2\sum_{k=0}^{\infty}3^k=4+18\cdot\frac{1}{1-3}=4-9=-5.$$

Fixed point techniques

Just as an illustration, we look at the following silly example: solving the equation $1 + 3x = x$ by regarding it as a fixed point problem for the map $f(x) = 1 + 3x$ in the complete metric space $\mathbf{Q}_3$. Let's first make sure that f is a contraction:

$$|f(y) - f(x)|_3 = |3y - 3x|_3 = |3|_3|y - x|_3 = \frac{1}{3}|y - x|_3,$$

so f is a contraction with factor $\frac{1}{3}$. General theory then tells us that f has a fixed point, and that this can be found by repeatedly applying f to an arbitrary chosen initial guess. If we take $x_0 = 1$ as our initial guess, and iterate according to the scheme $x_{n+1} = f(x_n) = 1 + 3x_n$, we get:

$$
\begin{aligned}
x_0 &= 1 \\
x_1 &= 1 + 3x_0 = 1 + 3 \\
x_2 &= 1 + 3x_1 = 1 + 3 + 3^2 \\
&\vdots \\
x_n &= 1 + 3 + 3^2 + \cdots + 3^n
\end{aligned}
$$

So the fixed point, and the solution, is

$$x = \lim_{n\to\infty} x_n = \sum_{k=0}^{\infty} 3^k = \frac{1}{1-3} = -\frac{1}{2},$$

which, of course, we could have obtained by less fancy methods!

References

Folland, Gerald B.
A course in abstract harmonic analysis
Studies in Advanced Mathematics
CRC Press, Boca Raton, FL, 1995
ISBN: 0-8493-8490-7

Gouvêa, Fernando Q.
p-adic numbers
Springer-Verlag, Berlin, 1997.
ISBN: 3-540-62911-4