A first introduction to p-adic numbers

David A. Madore

Revised 7th december 2000

In all that follows, p will stand for a prime number. $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$ are the sets of respectively the natural numbers (i.e. non negative integers), integers, rational numbers, reals and complex numbers.

In some — but not all — of what follows, we assume the reader is familiar with the notions of "group", "ring" and "field". We assume throughout that the reader knows the basic facts about the b-adic representation (i.e. representation in base b) of integers and reals

Note: I did not aim here at writing a completely rigorous document, but only an easily understandable introduction for those who do not have any idea of what a p-adic is.

1 First definition

We will call p-adic digit a natural number between 0 and $p-1$ (inclusive). A p-adic integer is by definition a sequence $(a_i)_{i\in\mathbb{N}}$ of p-adic digits. We write this conventionally as

$$\cdots a_i \cdots a_2\, a_1\, a_0$$

(that is, the a_i are written from left to right).

If n is a natural number, and

$$n = \overline{a_{k-1}\, a_{k-2} \cdots a_1\, a_0}$$

is its p-adic representation (in other words $n = \sum_{i=0}^{k-1} a_i p^i$ with each a_i a p-adic digit) then we identify n with the p-adic integer (a_i) with $a_i = 0$ if $i \geq k$. This means that natural numbers are exactly the same thing as p-adic integer only a finite number of whose digits are not 0. Also note that 0 is the p-adic integer all of

whose digits are 0, and that 1 is the p-adic integer all of whose digits are 0 except the right-most one (digit 0) which is 1.

If $\alpha = (a_i)$ and $\beta = (b_i)$ are two p-adic integers, we will now define their sum. To that effect, we define by induction a sequence (c_i) of p-adic digits and a squence (ε_i) of elements of $\{0, 1\}$ (the "carries") as follows:

- ε_0 is 0.
- c_i is $a_i + b_i + \varepsilon_i$ or $a_i + b_i + \varepsilon_i - p$ according as which of these two is a p-adic digit (in other words, is between 0 and $p - 1$). In the former case, $\varepsilon_{i+1} = 0$ and in the latter, $\varepsilon_{i+1} = 1$.

Under those circumstances, we let $\alpha + \beta = (c_i)$ and we call $\alpha + \beta$ the sum of α and β. Note that the rules described above are *exactly* the rules used for adding natural numbers in p-adic representation. In particular, if α and β turn out to be natural numbers, then their sum as a p-adic integer is no different from their sum as a natural number. So $2 + 2 = 4$ remains valid (whatever p is — but if $p = 2$ it would be written $\cdots 010 + \cdots 010 = \cdots 100$).

Here is an example of a 7-adic addition:

$$\begin{array}{cccccccc} & \cdots & 2 & 5 & 1 & 4 & 1 & 3 \\ + & \cdots & 1 & 2 & 1 & 1 & 0 & 2 \\ \hline & \cdots & 4 & 0 & 2 & 5 & 1 & 5 \end{array}$$

This addition of p-adic integers is associative, commutative, and verifies $\alpha + 0 = \alpha$ for all α (recall that 0 is the p-adic integer all of whose digits are 0).

Subtraction of p-adic integers is also performed in exactly the same way as that of natural numbers in p-adic form. Since everybody reading this is assumed to have gone through first and second grade, we will not elaborate further : -).

Note that this subtraction scheme gives us the negative integers readily: for example, subtract 1 from 0 (in the 7-adics) :

$$\begin{array}{cccccccc} & \cdots & 0 & 0 & 0 & 0 & 0 & 0 \\ - & \cdots & 0 & 0 & 0 & 0 & 0 & 1 \\ \hline & \cdots & 6 & 6 & 6 & 6 & 6 & 6 \end{array}$$

(each column borrows a 1 from the next one on the left). So $-1 = \cdots 666$ as 7-adics. More generally, -1 is the p-adic all of whose digits are $p - 1$, -2 has all of its digits equal to $p - 1$ except the right-most which is $p - 2$, and so on. In fact, (strictly) negative integers correspond exactly to those p-adics all of whose digits except a finite number are equal to $p - 1$.

It can then be verified that p-adic integers, under addition, form an abelian group.

We now proceed to describe multiplication. First note that if n is a natural number and α a p-adic integer, then we have a naturally defined $n\alpha = \alpha + \cdots + \alpha$ (n times, with $0\alpha = 0$ of course). If n is negative, we let, of course, $n\alpha = -((-n)\alpha)$. This limited multiplication satisfies some obvious equalities, such as $(m+n)\alpha = m\alpha + n\alpha$, $n(\alpha+\beta) = n\alpha + n\beta$, $m(n\alpha) = (mn)\alpha$, and so on (for those with some background in algebra, this is not new: any abelian group is a $\mathbb{Z}$-module). Note also that multiplying by $p = \cdots 0010$ is the same as adding a 0 on the right.

Multiplying two *p-adic integers* on the other hand requires some more work. To do that, we note that if $\alpha_0, \alpha_1, \alpha_2, \ldots$ are p-adic integers, with α_1 ending in (at least) one zero, α_2 ending in (at least) two zeroes, and so on, then we can define the sum of all the α_i, even though they are not finite in number. Indeed, the last digit of the sum is just the last digit of α_0 (since $\alpha_1, \alpha_2, \ldots$ all end in zero), the second-last is the second-last digit of $\alpha_0 + \alpha_1$ (because $\alpha_2, \alpha_3, \ldots$ all end in 00), and so on: every digit of the (infinite) sum can be calculated with just a finite sum. Now we suppose that we want to multiply α and $\beta = (b_i)$ two p-adic integers. We then let $\alpha_0 = b_0\alpha$ (we know how to define this since b_0 is just a natural number), $\alpha_1 = pb_1\alpha$, and so on: $\alpha_i = p^i b_i \alpha$. Since α_i is a p-adic integer multiplied by p^i, it ends in i zeroes, and therefore the sum of all the α_i can be defined.

This procedure may sound complicated, but, once again, it is still exactly the same as we have all learned in grade school to multiply two natural numbers. Here is an example of a 7-adic multiplication:

$$
\begin{array}{cccccccc}
 & \cdots & 2 & 5 & 1 & 4 & 1 & 3 \\
\times & \cdots & 1 & 2 & 1 & 1 & 0 & 2 \\
\hline
 & \cdots & 5 & 3 & 3 & 1 & 2 & 6 \\
+ & \cdots & 0 & 0 & 0 & 0 & 0 & \\
+ & \cdots & 1 & 4 & 1 & 3 & & \\
+ & \cdots & 4 & 1 & 3 & & & \\
+ & \cdots & 2 & 6 & & & & \\
+ & \cdots & 3 & & & & & \\
\hline
 & \cdots & 3 & 1 & 0 & 4 & 2 & 6
\end{array}
$$

(of course, it is relatively likely that I should have made some mistake somewhere).

We now have a set of p-adic integers, which we will call $\mathbb{Z}_p$, with two binary operations on it, addition and multiplication. It can be checked — but we will

not do it — that $\mathbb{Z}_p$ is then a commutative ring (for those who don't know what that means, it means that addition is associative and commutative, that zero exists and satisfies the properties we wish it to satisfy, that multiplication is associative and commutative, and distributive over addition, and that 1 exists and satisfies the properties we wish it to satisfy (namely $1\alpha = \alpha$ for all α)).

Now, how about division? First, the bad news: division of p-adics is *not* performed in the same way as division of integers or reals. In fact, it can't always be performed. For example, $1/p$ has no meaning as a p-adic integer — that is, the equation $p\alpha = 1$ has no solution — since multiplying a p-adic integer by p always gives a p-adic integer ending in 0. There is nothing really surprising here: $1/p$ can't be performed in the integers either.

However, what is mildly surprising is that division by p is essentially the only division which cannot be performed in the p-adic integers. This statement (in technical terms "$\mathbb{Z}_p$ is a *local* ring") will not be made precise for the moment; however, we give a concrete example. Suppose p is odd (in other words, $p \neq 2$). And let α be the p-adic integer all of whose digits are equal to $(p-1)/2$ except the last one which is $(p+1)/2$. By performing 2α (in other words, $\alpha + \alpha$), it is clear that every digit will be zero except the last one which is 1. So $2\alpha = 1$, in other words $\alpha = 1/2$.

For example, with our usual example of $p = 7$ we show that the number $\alpha = \cdots 333334$ is the number "one half" by adding it to itself:

$$\begin{array}{rccccccc} & \cdots & 3 & 3 & 3 & 3 & 3 & 4 \\ + & \cdots & 3 & 3 & 3 & 3 & 3 & 4 \\ \hline & \cdots & 0 & 0 & 0 & 0 & 0 & 1 \end{array}$$

Thus, in the 7-adic integers, "one half" is an *integer*. And so are "one third" ($\cdots 44445$), "one quarter" ($\cdots 1515152$), "one fifth" ($\cdots 541254125413$), "one sixth" ($\cdots 55556$), "one eighth" ($\cdots 0606061$), "one ninth" ($\cdots 3613613614$), "one tenth" ($\cdots 462046205$), "one eleventh" ($\cdots 162355043116235504312$) and so on. But "one seventh", "one fourtneenth" and so on, are not 7-adic integers.

We now give a way to calculate the inverse (and therefore the quotient) of p-adic integers. Suppose α is a p-adic integer ending in zero (such numbers are called *small* for reasons we will describe later). Then α^i ends in at least i zeros. Therefore, as we have seen, we can calculate $\beta = 1 + \alpha + \alpha^2 + \cdots$ even though it has an infinite number of terms. Multiplying this by $(1-\alpha)$ and expanding out (we shall admit that all the appropriate properties of addition are preserved when dealing with infinite sums) we find that $(1-\alpha)\beta = 1 - \alpha + \alpha - \alpha^2 + \alpha^2 - \cdots = 1$. Therefore we are able to calculate the inverse of $1 - \alpha$, which may be, as is easy

to see, any p-adic integer ending in 1. To summarize: p-adic integers ending in 0 have no inverse; those ending in 1 can be inverted with the formula described above. To inverse a p-adic integer α ending in a digit d other than 0 and 1, we find the (unique) digit f such that df is congruent to 1 mod p (i.e. is equal to 1 plus a multiple of p). In that case, $f\alpha$ ends in 1 so can be inverted, and we then have $1/\alpha = f/(f\alpha)$. To find f for small values of p, I have no better advice than checking successively all digits. Perhaps computer scientists can suggest an altogether faster method for inverting p-adics.

Up to now we have only described p-adic integers, and not p-adic numbers. We now proceed to define the latter. The relation between the set (ring) $\mathbb{Z}_p$ of p-adic integers and the set (field) $\mathbb{Q}_p$ of p-adic numbers is the same as between the set (ring) $\mathbb{Z}$ of integers and the set (field) $\mathbb{Q}$ of rationals. Namely, the second is obtained by taking quotients of an element of the first by a non zero element of the same — or, which amounts to the same, by adding new inverses to some elements of the first. In the case of the rationals, an inverse has to be added to every prime number p. In our case, however, we are fortunate, and adding an inverse to p only will suit our needs. We therefore proceed to do that.

We now define a <u>p-adic number</u> to be a $\mathbb{Z}$-indexed sequence $(a_i)_{i\in\mathbb{Z}}$ of p-adic digits such that $a_i = 0$ for sufficiently small i (explicitly: there exists $i_0 \in \mathbb{Z}$ such that $a_i = 0$ for $i < i_0$). Such numbers are also written from right to left, with a "p-adic dot" after decimal 0. So our condition says: there are a finite number of non zero digits on the right of the p-adic point. We consider p-adic integers as p-adic numbers by identifying $(a_i)_{i\in\mathbb{N}}$ with $(a_i)_{i\in\mathbb{Z}}$ where $a_i = 0$ for $i < 0$, in other words by adding zeros to the right of the point. If $\alpha = (a_i)$ is a p-adic number such that $a_i = 0$ for $i < i_0$ (and we can certainly suppose $i_0 \leq 0$ so we do) then the p-adic number α' obtained by shifting every decimal of α by $-i_0$ places to the left is a p-adic integer. We write $\alpha = \alpha' p^{i_0}$ (or $\alpha = \alpha'/p^{-i_0}$).

p-adic numbers can then be added as follows: if $\alpha = \alpha' p^i$ with α' a p-adic intger, and $\beta = \beta' p^j$ ditto, and suppose moreover $i \leq j \leq 0$, then we let $\alpha + \beta = (\alpha' + \beta' p^{j-i})p^i$ — note that $\alpha' + \beta' p^{j-i}$ is indeed a p-adic integer. This is just a complicated way of saying that we add as usual, starting from the furthest (rightmost) column where there is a non zero digit. Multiplication is easier: under the same notations (except that the condition $i \leq j$ is no longer necessary) we let $\alpha\beta = \alpha'\beta' p^{i+j}$. This says that we multiply "as usual", ignoring the p-adic dot, and then we place the dot in the "obvious" place where it should be.

The set $\mathbb{Q}_p$ of p-adic numbers, with this addition and multiplication, forms a field — in other words, all the properties of a ring are satisfied, and moreover every nonzero element has a multiplicative inverse.

2 Second definition — topology and metric

If n is an integer, recall that its p-adic valuation is the exponent of the greatest power of p that divides n. It is written $v_p(n)$. By convention, $v_p(0) = \infty$. If $r = a/b$ is a rational, its p-adic valuation is defined as $v_p(r) = v_p(a) - v_p(b)$.

For example, the 7-adic valuation of 7 is 1. That of 14 is also 1, as are those of 21, 28, 35, 42 or 56. The 7-adic valuation of 49, on the other hand, is 2, as is that of 98. And the 7-adic valuation of 343 is 3. The 2-adic valuation of an integer is 0 iff it is odd, it is *at least* 1 iff it is even, at least 2 iff the integer is multiple by 4, and so on. The 7-adic valuation of $1/7$ is -1, and so are those of $3/7$, $1/14$, $5/56$. The 7-adic valuation of $1/2$ or $8/3$ is 0. The 7-adic valuation of $7/3$ or $14/5$ is 1. The 7-adic valuation of $48/49$ is -2.

We now define the p-adic absolute value of a rational number r to be $|r|_p = p^{-v_p(r)}$. For example, $|p|_p = \frac{1}{p}$, $|1|_p = 1$, $|2p|_p = \frac{1}{p}$ if p is odd, and $|\frac{1}{p^2}| = p^2$.

We then define the p-adic distance between two rationals r, r' to be $|r' - r|_p$. It is relatively straightforward to check that this indeed defines a distance on the rationals. The rationals are not complete for that distance, in other words, every Cauchy sequence is not convergent. It is possible to define the p-adic numbers as the completion of the p-adic rationals under this metric. General theorems on topological fields ensure that this defines a field, the field of p-adic numbers.

To make the equivalence of both definitions clearer, we say that the valuation of a p-adic number (a_i) is the smallest i_0 (possibly positive) such that $a_i = 0$ for all $i < i_0$. With this terminology, a p-adic integer is exactly a p-adic number with non negative valuation. And a small p-adic integer (one which ends in 0) is one whose valuation is (strictly) positive. It is not hard to check that this definition coincides with the aforementioned one for integers, hence for rationals.

As for rationals, we define the p-adic absolute value and distance by $|\alpha|_p = p^{-v_p(\alpha)}$. Note that the p-adic absolute value of a p-adic number is **real** number (it is also a p-adic, and in fact a rational, but ought not be considered as such). Then $\mathbb{Q}_p$ is a metric space, and the two following facts can be proven:

- $\mathbb{Q}_p$ is complete.
- $\mathbb{Q}$ is dense in $\mathbb{Q}_p$.

Also note that $\mathbb{Z}_p$ is the unit ball with center 0 in $\mathbb{Q}_p$.