

# $p$ -adic numbers

## 1 $p$ -adic numbers

Let  $m$  be an integer,  $m > 1$ . An  $m$ -adic number is an expression  $a = \sum_{i=i_0}^{\infty} a_i m^i$  where the digits  $a_i$  are in  $\{0, 1, \dots, m-1\}$ . Clearly, the  $m$ -adic numbers form a ring. An  $m$ -adic number  $a$  is called an  $m$ -adic integer if  $a_i = 0$  for  $i < 0$ . Clearly, the  $m$ -adic integers form a ring.

Let  $p$  be prime. The  $p$ -adic numbers form a field called  $\mathbf{Q}_p$ . The  $p$ -adic integers form a ring called  $\mathbf{Z}_p$ . An element  $z \in \mathbf{Z}_p$  is a unit (i.e., has an inverse in this ring) iff  $z_0 \neq 0$ .

Every nonzero  $p$ -adic number  $x$  can be written uniquely as  $p^e z$  where  $z$  is a unit in  $\mathbf{Z}_p$ . Define the  $p$ -adic norm  $|\cdot|_p$  by  $|x|_p = p^{-e}$  if  $x = p^e z \neq 0$  and  $|0|_p = 0$ . Let  $|\cdot|_{\infty}$  be the ordinary absolute value. Then for any nonzero rational number  $r$  we have  $\prod_v |r|_v = 1$  if  $v$  runs over  $\infty$  and all primes  $p$ . Just like  $\mathbf{R}$  is the completion of  $\mathbf{Q}$  for the norm  $|\cdot|_{\infty}$ , the fields  $\mathbf{Q}_p$  are the completions of  $\mathbf{Q}$  for the norms  $|\cdot|_p$ .

(The *completion* of a metric space is obtained by adding new points that are the limits of Cauchy sequences.)

For the metric  $d(x, y) = |x - y|_p$ , the partial sums of  $a = \sum_{i=i_0}^{\infty} a_i m^i$  converge to  $a$ .

**Example** Let  $m = 10$ . Write a 10-adic integer as a (possibly left-infinite) sequence of decimal digits. We have  $\dots 99999 = -1$ , for example because  $\dots 99999 + 1 = 0$  (or because, summing a geometric progression,  $\dots 99999 = 9/(1 - 10) = -1$ ).

**Example** Let  $m = 10$ . We can find two nonzero 10-adic integers  $\dots 32$  and  $\dots 25$  with product 0 by making sure that one is divisible by arbitrarily high powers of 2 and the other by arbitrarily high powers of 5. This is achieved by growing longer and longer tails, each time prefixing a digit with the property that there are infinitely many powers of 2 (or 5) that end with the tail thus obtained.

**Example** Compute  $1/10$  in the 5-adic numbers:  $\frac{1}{10} = \dots 2222.3$ . Compute  $1/7$  in the 5-adic integers:  $\frac{1}{7} = \dots 2412032412033$ . Clearly, the rational numbers are precisely the  $p$ -adic numbers that are eventually periodic.

In order to solve equations over the  $p$ -adic numbers, one first solves them mod  $p$ , and then lifts the obtained solution(s) to solutions mod  $p^i$  for all  $i$ .

For example,  $x^2 = 2$  has no solutions in  $\mathbf{Q}_5$  since it has no solutions mod 5. (So,  $\mathbf{Q}_5$  is not algebraically closed.) But  $x^2 = -1$  has two solutions in  $\mathbf{Q}_5$ . First

of all,  $2^2 = 3^2 = -1 \pmod{5}$ . Next, if  $x^2 + 1 = 0 \pmod{5^i}$  where  $i > 0$ , say  $x^2 + 1 = a \cdot 5^i$ , put  $y = x + c \cdot 5^i$ . Then  $y^2 + 1 = x^2 + 1 + 2cx \cdot 5^i = (a + 2cx) \cdot 5^i \pmod{5^{i+1}}$ , and we can pick  $c$  (in a unique way) so as to make this  $0 \pmod{5^{i+1}}$ . This argument works more generally, and the lemma describing it is called Hensel's Lemma.

Both  $\mathbf{Z}_p$  and  $\mathbf{Q}_p$  have the cardinality of the continuum, that is, of  $\mathbf{R}$ . The ring  $\mathbf{Z}_p$  (with product topology) is compact. The field  $\mathbf{Q}_p$  is locally compact.

The various extensions  $\mathbf{Q}_p$  of  $\mathbf{Q}$  are independent in the sense that given numbers  $x_p \in \mathbf{Q}_p$  and  $x_\infty \in \mathbf{R}$  there is a sequence  $(r_i)_i$  of rational numbers such that for each  $v$  this sequence has limit  $x_v$  in  $\mathbf{Q}_v$  (with  $\mathbf{Q}_\infty = \mathbf{R}$ ).