p-adic Numbers

Hiten Dalmia

B. Sc. (Hons.) Mathematics, 3rd year

2232174

Contents

Abstract. In this paper we introduce the p-adic numbers. We start by introducing the p-adic norm and the metric induced from that norm. We also then go on to contruct the $\mathbb{Q}_p$ set, that is the set of all rational p-adic numbers and define addition and multiplication in this field.

1 Introduction

The p-adic numbers, where p is any prime number, come from an alternate way of defining the distance between two rational numbers. The standard distance function, the Euclidean metric, gives rise to the real numbers. While the real numbers are more natural to most of us, this paper aims to present the p-adic numbers as an alternate field that also forms a complete metric space much like the set of real numbers with the Euclidean metric.

The p-adic numbers are useful because they provide another toolset for solving problems, one which is sometimes easier to work with than the real numbers. They have applications in number theory, analysis, algebra, and more. One example is Hensel's lemma for finding roots of a polynomial. Another is Mahler's Theorem, a p-adic analog of the Stone-Weierstrass Theorem. Yet another is Monsky's Theorem, a theorem about triangulating squares whose proof makes use of 2-adic numbers.

2 Initial Definitons

We will work with metric spaces, usually (X, d), that have metrics induced from norms and for that we first introduce the concept of a norm.

The metries d we'll be dealing with will come from norms on a field F, which is a map denoted $||\ ||$ from F to the nonnegative real numbers such that

1. $||x|| = 0 \Leftrightarrow x = 0$
2. $||x \cdot y|| = ||x|| \cdot ||y||$
3. $||x + y|| = ||x|| + ||y||$

When we say that a metric d "comes from" (or "is induced by") a norm $||\ ||$, we mean that it is defined by: $d(x, y) = ||x - y||$.

A basic example of a norm on the rational number field $\mathbb{Q}$ is the absolute value $|x|$. The induced metric $d(x, y) = |x - y|$ is the usual concept of distance on the number line.

3 The p-adic Norm

Definition 1 *Let $p \in 2, 3, 5, 7, 11, 13, \ldots$ be any prime number. For any non-zero integer a, let the p-adic ordinal of a, denoted $ord_p a$, be the highest power of p which divides a, i.e., the greatest m such that $a == 0 (mod\ p^m)$.*

A few examples of the p-adic ordinal:

1. $\text{ord}_5\ 35 = 1$
2. $\text{ord}_5\ 250 = 3$

3. $\text{ord}_2\ 96 = 5$
4. $\text{ord}_2\ 97 = 0$

We must note the following properties of the p-adic ordinal:

1. $\text{ord}_p(a_1, a_2) = \text{ord}_p(a_2) + \text{ord}_p(a_2)$
2. $\text{ord}_p(\frac{a_1}{a_2}) = \text{ord}_p(a_2) - \text{ord}_p(a_2)$

Definition 2

$$|x|_p = \begin{cases} \frac{1}{p^{\text{ord}_p x}} & x \neq 0 \\ 0 & x = 0 \end{cases}$$

Theorem 1 $|\ |_p$ *is a norm on* $\mathbb{Q}$

Proof. Properties 1 and 2 follow from the definition of the function.

If $x = 0$ or $y = 0$, or if $x + y = 0$, Property 3 is trivial, so assume x, y, and $x + y$ are all nonzero. Let $x = a/b$ and $y = e/d$ be written in lowest terms. Then we have: $x + y = (ad + be)/bd$, and $\text{ord}_p(x + y) = \text{ord}_p(ad + be) - \text{ord}_p b - \text{ord}_p d$. Now the highest power of p dividing the sum of two numbers is at least the minimum of the highest power dividing the first and the highest power dividing the second. Hence

$$\begin{aligned} \text{ord}_p(x + y) &\geq \min(\text{ord}_p(ad), \text{ord}_p(bc)) - \text{ord}_p(b) - \text{ord}_p(d) \\ &= \min(\text{ord}_p(a) + \text{ord}_p(d), \text{ord}_p(b) + \text{ord}_p(c)) - \text{ord}_p(b) - \text{ord}_p(d) \\ &= \min(\text{ord}_p(a) - \text{ord}_p(b), \text{ord}_p(c) - \text{ord}_p(d)) \\ &= \min(\text{ord}_p(x), \text{ord}_p(y)) \end{aligned}$$

Tberefore, $|x+y|_p = p^{-\mathrm{ord}_p(x+y)} \leq \max(p^{-\mathrm{ord}_p(x)}, p^{-\mathrm{ord}_p(y)}) = \max(|x|_p, |y|_p)$, and this is $\leq |x|_p + |y|_p$.

Q.E.D.

Definition 3 *A norm is called a non-Archimedean norm if it follows the strong triangle inequality*

$$||x+y|| \leq max(||x||, ||y||)$$

A metric is called a non-Archimedean metric if it follows the strong triangle inequality

$$d(x+y) \leq max(d(x), d(y))$$

From Theorem **??**, the p-adic norm is a non-Archimedean norm on $\mathbb{Q}$.

The "trivial" norm is defined the norm $||\ ||$ such that $||0|| = 0$ and $||x|| = 1$ for $x \neq 0$.

The usual absolute value is also often denoted by $|\ |_\infty$

4 Ostrowski's Theorem

Theorem 2 *Every nontrivial norm $\|\cdot\|$ on $\mathbb{Q}$ is equivalent to $|\cdot|_p$, for some prime p or for $p = \infty$.*

Proof. *Case (i).* Suppose there exists a positive integer n such that $\|n\| > 1$. Let n_0 be the least such n. Since $\|n_0\| > 1$, there exists a positive real number α such that $\|n_0\| = n_0^\alpha$. Now write any positive integer n to the base n_0, i.e., in the form

$$n = a_0 + a_1 n_0 + a_2 n_0^2 + \cdots + a_s n_0^s, \quad \text{where } 0 \leq a_i < n_0 \text{ and } a_s \neq 0.$$

Then

$$\|n\| \leq \|a_0\| + \|a_1 n_0\| + \|a_2 n_0^2\| + \cdots + \|a_s n_0^s\|$$
$$= \|a_0\| + \|a_1\| \cdot n_0^{\alpha} + \|a_2\| \cdot n_0^{2\alpha} + \cdots + \|a_s\| \cdot n_0^{s\alpha}.$$

Since all of the a_i are $< n_0$, by our choice of n_0 we have $\|a_i\| \leq 1$, and hence

$$\|n\| \leq 1 + n_0^a + n_0^{2a} + \cdots + n_0^{sa} = n_0^{sa}(1 + n_0^{-a} + n_0^{-2a} + \cdots + n_0^{-sa})$$
$$\leq n_0^{sa} \left(\sum_{j=0}^{\infty} (1/n_0^{ja}) \right),$$

because $n \geq n_0^s$. The expression in brackets is a finite constant, which we call C. Thus,

$$\|n\| \leq Cn^a \quad \text{for all } n = 1, 2, 3, \ldots.$$

Now take any n and any large N, and put n^N in place of n in the above inequality; then take Nth roots. You get

$$\|n\| \leq \sqrt[N]{Cn^a}.$$

Letting $N \to \infty$ for n fixed gives $\|n\| \leq n^a$.

We can get the inequality the other way as follows. If n is written to the base n_0 as before, we have $n^{s+1} > n \geq n_0^s$. Since $\|n^{s+1}\| = \|n + n_0^s - n\| \leq \|n\| + \|n_0^s - n\|$, we have

$$\|n\| \geq \|n_0^{s+1}\| - \|n_0^s - n\|$$
$$\geq n_0^{s+1} - (n_0^{s+1} - n)^a,$$

since $\|n_0^{s+1}\| = n_0^{s+1}$, and we can use the first inequality (i.e., $\|n\| \leq n^a$) on the term that is being subtracted. Thus,

$$\|n\| \geq n_0^{s+1} - (n_0^{s+1} - n_0)^a \quad (\text{since } n \geq n_0^s)$$

$$= n_0^{s+1}\left[1 - \left(1 - \frac{1}{n_0}\right)^a\right] \geq C' n^a$$

for some constant C' which may depend on n_0 and a but not on n. As before, we now use this inequality for n^N, take Nth roots, and let $N \to \infty$, finally getting: $\|n\| \geq n^a$.

Thus, $\|n\| = n^a$. It easily follows from Property (2) of norms that $\|x\| = |x|^a$ for all $x \in \mathbb{Q}$. Such a norm is equivalent to the absolute value $|\cdot|$, this concludes the proof of the theorem in Case (i).

Case (ii). Suppose that $\|n\| \leq 1$ for all positive integers n. Let n_0 be the least n such that $\|n\| < 1$; n_0 exists because we have assumed that $\|\cdot\|$ is nontrivial.

n_0 must be a prime, because if $n_0 = n_1 \cdot n_2$ with n_1 and n_2 both $< n_0$, then

$$\|n_1\| = \|n_2\| = 1, \quad \text{and so } \|n_0\| = \|n_1\| \cdot \|n_2\| = 1.$$

So let p denote the prime n_0. We claim that $\|q\| = 1$ if q is a prime not equal to p. Suppose not; then $\|q\| < 1$, and for some large N we have $\|q^N\| = \|q\|^N < \frac{1}{2}$. Also, for some large M we have $\|p^M\| < \frac{1}{2}$. Since p^M and q^N are relatively prime, have no common divisor other than 1—we can find integers n and m such that:

$$mp^M + nq^N = 1.$$

But then

$$1 = \|1\| = \|mp^M + nq^N\| \leq \|mp^M\| + \|nq^N\| = \|m\|\|p^M\| + \|n\|\|q^N\|,$$

by Properties (2) and (3) in the definition of a norm. But $\|m\|, \|n\| \leq 1$, so that

$$1 \leq \|p^M\| + \|q^N\| < \frac{1}{2} + \frac{1}{2} = 1,$$

a contradiction. Hence $\|q\| = 1$.

We're now virtually done, since any positive integer a can be factored into prime divisors:

$$a = p_1^{b_1} p_2^{b_2} \cdots p_r^{b_r}.$$

Then

$$\|a\| = \|p_1\|^{b_1} \|p_2\|^{b_2} \cdots \|p_r\|^{b_r}.$$

But the only $\|p_i\|$ which is not equal to 1 will be $\|p\|$ if one of the p_i's is p. Its corresponding b_i will be $\operatorname{ord}_p a$. Hence, if we let $\rho = \|p\| < 1$, we have

$$\|a\| = \rho^{\operatorname{ord}_p a}.$$

It is easy to see using Property (2) of a norm that the same formula holds with any nonzero rational number x in place of a. Such a norm is equivalent to $|\cdot|_p$, this concludes the proof of Ostrowski's theorem.

5 Properties of the p-adic norm

Theorem 3 *(Isoceles Triange Principle)*

Let us take three points such that they form a triangle x, y, z and for simplicity let us take $z = 0$.

The non-Archimedean triangle inequality says:

$$\|x - y\| \leq \max(\|x\|, \|y\|).$$

Suppose first that the "sides" x and y have different "length," say $\|x\| < \|y\|$. The third side $x - y$ has length

$$\|x - y\| \leq \|y\|.$$

But

$$\|y\| = \|x - (x - y)\| \leq \max(\|x\|, \|x - y\|).$$

Since $\|y\|$ is not $\leq \|x\|$, we must have $\|y\| \leq \|x - y\|$, and so $\|y\| = \|x - y\|$.

Theorem 4 *Every member of an open ball is its center.*

We define the open ball of radius r (r is a positive real number) with center a (a is an element in the field F) to be

$$S(a, r) = \{x \in F \mid \|x - a\| < r\}.$$

Suppose $\|\cdot\|$ is a non-Archimedean norm. Let b be any element in $S(a, r)$. Then

$$S(a, r) = S(b, r),$$

i.e., every point in the ball is a center. As

$$x \in S(a, r) \implies \|x - a\| < r \implies \|x - b\| = \|(x - a) + (a - b)\|$$

$\leq \max(\|x - a\|, \|a - b\|) < r \implies x \in S(b, r)$, and the reverse implication is proved in the exact same way.

If we define the closed ball of radius r with center a to be

$$S(a, r) = \{x \in F \mid \|x - a\| \leq r\},$$

for non-Archimedean $\|\cdot\|$, we similarly find that every point in $S(a, r)$ is a center.

6 Building the field of p-adic numbers

Let S be the set of sequences $\{a_i\}$ of rational numbers such that, given $\varepsilon > 0$, there exists an N such that $|a_i - a_{i'}|_p < \varepsilon$ if both

$i, i' > N$. We call two such Cauchy sequences $\{a_i\}$ and $\{b_i\}$ equivalent if $|a_i - b_i|_p \to 0$ as $i \to \infty$. We define the set $\mathbb{Q}_p$ to be the set of equivalence classes of Cauchy sequences.

For any $x \in \mathbb{Q}$, let $\{x\}$ denote the "constant" Cauchy sequence all of whose terms equal x. It is obvious that $\{x\} \sim \{x'\}$ if and only if $x = x'$. The equivalence class of $\{0\}$ is denoted simply by 0.

We define the norm $|\cdot|_p$ of an equivalence class a to be $\lim_{i\to\infty} |a_i|_p$, where $\{a_i\}$ is any representative of a. The limit exists because

(1) If $a = 0$, then by definition $\lim_{i\to\infty} |a_i|_p = 0$.

(2) If $a \neq 0$, then for some $\varepsilon > 0$ and for every N, there exists an $i_N > N$ with $|a_{i_N}|_p > \varepsilon$.

If we choose N large enough so that $|a_i - a_{i'}|_p < \varepsilon$ when $i, i' > N$, we have:

$$|a_i - a_{i'}|_p < \varepsilon \quad \text{for all } i, i' > N.$$

Since $|a_{i_N}|_p > \varepsilon$, it follows by Theorem 3 that $|a_i|_p = |a_{i'}|_p$. Thus, for all $i > N$, $|a_i|_p$ has the constant value $|a_i|_p$. This constant value is then $\lim_{i\to\infty} |a_i|_p$.

6.1 Defining Arithmetic Operations on the p-adic numbers

Given two equivalence classes a and b of Cauchy sequences, we choose any representatives $\{a_i\} \in a$ and $\{b_i\} \in b$, and define $a \cdot b$ to be the equivalence class represented by the Cauchy sequence $\{a_i b_i\}$. If we had chosen another $\{a_i'\} \in a$ and $\{b_i'\} \in b$, we would have

$$|a_i b_i' - a_i' b_i|_p = |a_i(b_i' - b_i) + b_i(a_i' - a_i)|_p \leq \max(|a_i(b_i' - b_i)|_p, |b_i(a_i' - a_i)|_p);$$

as $i \to \infty$, the first expression approaches $|a|_p \cdot \lim |b'_i - b_i|_p = 0$, and the second expression approaches $|b|_p \cdot \lim |a'_i - a_i|_p = 0$. Hence $\{a'_i b'_i\} \sim \{a_i b_i\}$.

We similarly define the sum of two equivalence classes of Cauchy sequences by choosing a Cauchy sequence in each class, defining addition term-by-term, and showing that the equivalence class of the sum only depends on the equivalence classes of the two summands.

For multiplicative inverses we have to be a little careful because of the possibility of zero terms in a Cauchy sequence. However, it is easy to see that every Cauchy sequence is equivalent to one with no zero terms (for example, if $a_i = 0$, replace a_i by $a'_i = p^i$). Then take the sequence $\{1/a_i\}$. This sequence will be Cauchy *unless* $|a_i|_p \to 0$, i.e., unless $\{a_i\} \sim \{0\}$. Moreover, if $\{a_i\} \sim \{a'_i\}$ and no a_i or a'_i is zero, then $\{1/a_i\} \sim \{1/a'_i\}$.

7 Bibliography

1. Neal Koblitz (1991) - p-adic Numbers, p-adic Analysis, and Zeta Functions, Second Edition.

2. Alexa Pomerantz, An Introduction to the p-adic Numbers.