

# p-adic Numbers an Introduction

Donghyun Park

December 11, 2025

This post summarizes the book: "p-adic Numbers an Introduction" by Fernando Q. Gouvea [Gou20]

## Chapter 2. Foundations

### Definition

Definition : Absolute value on field  $\mathbb{k}$  is a function  $|\cdot| : \mathbb{k} \rightarrow \mathbb{R}^+$  that

-  $|x| = 0$  if and only if  $x = 0$

-  $|xy| = |x||y|$

-  $|x + y| \leq |x| + |y|$

If  $|x + y| \leq \max(|x|, |y|)$  holds then we call nonarchimedean.

Definition : for  $x \in \mathbb{Q}$ , define p-adic absolute value

$$|x|_p = p^{-v_p(x)}$$

and  $|0|_p = 0$

More generally, for a **valuation** defined on integral domain  $A$  which is  $v : A - \{0\} \rightarrow \mathbb{R}$ , satisfying

-  $v_p(xy) = v_p(x) + v_p(y)$

-  $v_p(x + y) \geq \min(v_p(x), v_p(y))$

extends to  $K$  a field of fractions and  $v(a/b) = v(a) - v(b)$  and the function  $|\cdot|_v : K \rightarrow \mathbb{R}^+$  that

$$|x|_v = e^{-v(x)}$$

is non-archimedean absolute value on  $K$ . This extends to general cases, such as rational functions  $\mathbb{F}(t)$  the  $v_\infty(f) = -\deg(f(t))$  or with the irreducible polynomial  $p(t) \in \mathbb{F}[t]$ , counting the multiplicity of  $p(t)$ .

**Theorem 1** (Theorem 2.2.4). *The absolute value on  $\mathbb{k}$  is non-archimedean if and only if  $|n|$  is bounded for  $n \in \mathbb{Z}$ .*

This is related to **Archimedean Property** : Given  $x, y \in \mathbb{k}$ ,  $x \neq 0$  there exists a positive integer  $n$  such that  $|nx| > |y|$ .

### Topology

Now, the distance function  $d(x, y) = |x - y|$  defines metric on  $\mathbb{k}$ . This topological space becomes strange when non-archimedean absolute value.

**Proposition 1** (Proposition 2.3.4).  *$\mathbb{k}$  a field and  $|\cdot|$  non-archimedean absolute value. If  $x, y \in \mathbb{k}$  and  $|x| \neq |y|$  then*

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

As a consequence two open balls intersect if and only if it is contained by other and the same for closed balls. In fact, it is totally disconnected.

## Algebra

For  $\mathbb{k}$  a field and non-archimedean absolute value, the subring

$$\mathcal{O} = \{x \in \mathbb{k} : |x| \leq 1\}$$

is a local ring and called **Valuation Ring**. Its maximal ideal is

$$\mathcal{B} = \{x \in \mathbb{k} : |x| < 1\}$$

We call **Valuation Ideal**

The quotient  $\kappa = \mathcal{O}/\mathcal{B}$  is a **Residue field** of  $|\cdot|$ .

For example, in p-adic absolute value,

$$\mathcal{O} = \{a/b \in \mathbb{Q} : p \nmid b\} = \mathbb{Z}_{(p)}$$

and its valuation ideal is  $p\mathbb{Z}_{(p)}$  with residual field  $\mathbb{F}_p$

## Chapter 3. The p-adic Numbers

We call absolute values being equivalent if it gives the same topology on a field  $\mathbb{k}$ . Equivalent to the statement :  $|x|_1 < 1$  if and only if  $|x|_2 < 1$ .

**Theorem 2** (Theorem 3.14 (Ostrowski)). *Every non-trivial absolute value on  $\mathbb{Q}$  is equivalent to  $|\cdot|_\infty$  or  $|\cdot|_p$  for some prime  $p$ .*

### Completion

We will complete  $\mathbb{Q}$  via the p-adic absolute value.

**Lemma 1** (Lemma 3.2.3). *The field  $\mathbb{Q}$  with p-adic absolute value is not complete.*

*Proof.* Construct sequence by following : for the equation  $X^2 \equiv a \pmod{p^n}$  that is coherent  $x_0, x_1, \dots$  then it is Cauchy sequence but do not converge to the point in  $\mathbb{Q}$ .  $\square$

So we complete  $\mathbb{Q}$  with p-adic absolute value. It exists and

**Theorem 3** (Theorem 3.2.14). *There exists a field  $\mathbb{Q}_p$  with a non-archimedean absolute value  $|\cdot|_p$  such that*

- There exists an inclusion  $\mathbb{Q} \hookrightarrow \mathbb{Q}_p$  and absolute value induced by  $|\cdot|_p$  on  $\mathbb{Q}$  via this inclusion is the p-adic absolute value.
- Image of  $\mathbb{Q}$  under the inclusion is dense in  $\mathbb{Q}_p$
- $\mathbb{Q}_p$  is complete with respect to the absolute value  $|\cdot|_p$
- $\mathbb{Q}_p$  satisfying above condition is unique up to isomorphism.

## Chapter 4. Exploring $\mathbb{Q}_p$

Exploring the structure of  $\mathbb{Q}_p$ , the valuation ring is called **p-adic integers**

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

with valuation ideal

$$p\mathbb{Z}_p = \{x \in \mathbb{Q}_p : |x|_p < 1\}$$

satisfies:

**Proposition 2** (Proposition 4.2.2).

$$\mathbb{Q} \cap \mathbb{Z}_p = \mathbb{Z}_{(p)} = \left\{ \frac{a}{b} \in \mathbb{Q} : p \nmid b \right\}$$

- $\mathbb{Z} \hookrightarrow \mathbb{Z}_p$  is dense image.
- For  $x \in \mathbb{Z}_p$ , there exists a Cauchy sequence  $(\alpha_n) \in \mathbb{Z}$  converging to  $x$  that  $0 \leq \alpha_n \leq p^n - 1$  and

$$\alpha_n \equiv \alpha_{n-1} \pmod{p^{n-1}}$$

And further structure is,  $x \in \mathbb{Q}_p$  then for some  $n \geq 0$ ,  $p^n x \in \mathbb{Z}_p$ . So we first know **p-adic integers : the sequence of coherent integer series** and all the elements are  $1/p^m$  of p-adic integers.

Also, the topology of  $\mathbb{Q}_p$  is first **totally disconnected**, and **locally compact** since  $\mathbb{Z}_p$  is **compact**. To see this,  $\mathbb{Z}_p$  can be covered by finite number of  $p^{-n}$  radii balls. It is,

$$a + p^n \mathbb{Z}_p$$

is each of  $p^{-n}$  radii ball centered at  $a = 0, 1, \dots, p^n - 1$

Back to the structure of  $\mathbb{Q}_p$ , we saw  $\mathbb{Z}_p$  can be seen as a coherent sequence. We can write

$$x = b_0 + b_1 p + b_2 p^2 + \dots$$

for  $x \in \mathbb{Z}_p$ . Moreover, since  $x \in \mathbb{Q}_p$ , for some  $m$ ,  $p^m x \in \mathbb{Z}_p$  so

$$x = b_{-m} p^{-m} + \dots + b_{-1} p^{-1} + b_0 + b_1 p + \dots$$

for  $x \in \mathbb{Q}_p$ . These representations make us easy to handle quite 'abstract' p-adic numbers.

## Hensel's Lemma

**Theorem 4** (Theorem 4.5.1 (Hensel's Lemma I)).  $F(X) = a_0 + a_1 X + a_2 X^2 + \dots + a_n X^n$  a polynomial with coefficients  $\mathbb{Z}_p$ . If there exists a p-adic integer  $\alpha_1 \in \mathbb{Z}_p$  such that

$$F(\alpha_1) \equiv 0 \pmod{p\mathbb{Z}_p}$$

and

$$F'(\alpha_1) \not\equiv 0 \pmod{p\mathbb{Z}_p}$$

Then there exists a unique p-adic integer  $\alpha \in \mathbb{Z}_p$  such that  $\alpha \equiv \alpha_1 \pmod{p\mathbb{Z}_p}$  and  $F(\alpha) = 0$ .

Proof by constructing the convergent series:

$$\alpha_{n+1} = \alpha_n - \frac{F(\alpha_n)}{F'(\alpha_n)}$$

similar to Newton Method, however  $(\alpha_n)$  is coherent so converges to  $\mathbb{Z}_p$ . This can be seen in the aspect of **dynamics**

The usage of Hensel's Lemma is first **root of unity**. We can find existence of **primitive m-th root of unity**, by using  $F(X) = X^m - 1$ .  $F'(\lambda) = 0$  if  $\lambda \equiv 0 \pmod{p}$  or  $p \mid m$  : the first one cannot hold so,

**Proposition 3** (Proposition 4.6.1). If  $p \nmid m$  then there exists a primitive m-th root of unity in  $\mathbb{Q}_p$  if and only if  $m \mid p - 1$

Another usage is **Square root**

**Proposition 4** (Proposition 4.6.2).  $p \neq 2$  a prime,  $b \in \mathbb{Z}_p^\times$ . If there exists  $\alpha_1 \in \mathbb{Z}_p$  that  $\alpha_1^2 \equiv b \pmod{p\mathbb{Z}_p}$  then  $b$  is square of an element of  $\mathbb{Z}_p^\times$

proof using  $f(X) = X^2 - b$ .

So, we know all the squares in  $\mathbb{Q}_p$ . It is:  $x = p^{2n} y^2$  with  $n \in \mathbb{Z}$  and  $y \in \mathbb{Z}_p^\times$  a p-adic unit. So the quotient group by squares are order 4. Is  $p$  order is even or odd and p-adic unit is square or not.

## Hensel's Lemma for Polynomials

**Theorem 5** (Theorem 4.7.2 (Hensel's Lemma for Polynomials)).  $f(X) \in \mathbb{Z}_p[X]$  a polynomial and assume  $g_1(X), h_1(X) \in \mathbb{Z}_p[X]$  such that

- $g_1(X)$  monic
- $g_1(X)$  and  $h_1(X)$  reduced into polynomial in  $\mathbb{F}_p[X]$  by modulo  $p$  for each coefficients, then is relatively prime modulo  $p$
- $f(X) \equiv g_1(X)h_1(X) \pmod{p}$  coefficient-wise

Then there exists  $g(X), h(X) \in \mathbb{Z}_p[X]$  that

- $g(X)$  monic
- $g(X) \equiv g_1(X) \pmod{p}$  and  $h(X) \equiv h_1(X) \pmod{p}$
- $f(X) = g(X)h(X)$

## Local-Global Principle

We will use  $\mathbb{Q}_p$  to analyze Diophantine equation. The existence of solutions in  $\mathbb{Q}$  can be detected by studying roots on  $\mathbb{Q}_p$  which are local solutions.

Instances:

- $X^2 + Y^2 + Z^2 = 0$  in  $\mathbb{Q}_\infty = \mathbb{R}$  ; no nontrivial solution
- $X^2 - 3Y^2 = 0$  in  $\mathbb{Q}_7$  ; no nontrivial solution

Local-Global Principle might fail :

- $(X^2 - 2)(X^2 - 17)(X^2 - 34) = 0$  has roots in  $\mathbb{Q}_p$  but not in  $\mathbb{Q}$
- $X^4 - 17 = 2Y^2$  has roots in  $\mathbb{Q}_p$  but not in  $\mathbb{Q}$ .

**Theorem 6** (Theorem 4.8.2 (Hasse-Minkowski)). *For the quadratic form*

$$F(X_1, \dots, X_n) = \sum_{i,j} c_{ij} X_i X_j \in \mathbb{Q}[X_1, \dots, X_n]$$

*the equation  $F(X_1, \dots, X_n) = 0$  has non-trivial solutions in  $\mathbb{Q}$  if and only if it has non-trivial solutions in  $\mathbb{Q}_p$  for  $p \leq \infty$ .*

In this book, considers restricted case (but quite a large class of equation) :

$$aX^2 + bY^2 + cZ^2 = 0$$

We can find the solution in  $\mathbb{Q}_p$  if

- $p = \infty$  :  $a, b, c$  do not have the same sign
  - $p$  odd prime :  $p \nmid abc$  then solution exists and if  $p \mid a$  :  $b + r^2c \equiv 0 \pmod{p}$  for some  $r \in \mathbb{Z}$
  - $p = 2$  :  $a, b, c$  all odd then two sum must be divisible by 4, and if  $a$  even  $b + c$  or  $a + b + c$  divisible by 8
- By Hasse-Minkowski, if above condition guarantees solution in  $\mathbb{Q}$ .

## References

- [Gou20] Fernando Q. Gouvêa. *p-adic Numbers: An Introduction*. 3rd. Universitext. Cham, Switzerland: Springer, 2020. ISBN: 978-3-030-47294-8. DOI: 10.1007/978-3-030-47295-5.