A Survey of p-Adic Numbers

Sílvia Casacuberta Puig

April 28, 2020

1 Introduction to p-Adic Numbers

1.1 The Ring $\mathbb{Z}_p$

Historically, p-adic numbers were introduced by Kurt Hensel in 1897. Hensel explored the analogies between primes $p \in \mathbb{Z}$ and linear polynomials $x - \alpha \in \mathbb{C}[x]$, noting that both $\mathbb{Z}$ and $\mathbb{C}[x]$ are unique factorization domains. Given a degree n polynomial $P(x)$ and any number $\alpha \in \mathbb{C}$, we can write

$$P(x) = \sum_{i=0}^{n} a_i (x - \alpha)^i,$$

with $a_i \in \mathbb{C}$. Similarly, given a positive integer m and a prime p, we can write m in base p:

$$m = \sum_{i=0}^{n} a_i p^i,$$

with $a_i \in \mathbb{Z}$ and $0 \leq a_i < p$. Such expansions are relevant because they give *local* information, that is, they tell us if $P(x)$ vanishes at α, and to what order, and the same holds for m and its divisibility by p. Expansions by means of powers of p are called *p-adic expansions*.

Definition 1. A *p-adic integer* α is a formal infinite series

$$\alpha = a_0 + a_1 p + a_2 p^2 + \cdots$$

with $0 \leq a_i < p$.

The abelian group of p-adic integers is denoted by $\mathbb{Z}_p$. Alternatively, $\mathbb{Z}_p$ is the inverse (or projective) limit [4] of the sequence of natural projections

$$\cdots \longrightarrow \mathbb{Z}/p^3\mathbb{Z} \longrightarrow \mathbb{Z}/p^2\mathbb{Z} \longrightarrow \mathbb{Z}/p\mathbb{Z}.$$

Thus, an element of $\mathbb{Z}_p$ can be viewed as a sequence $(x_0, x_1, x_2 \ldots)$ where $x_n \in \mathbb{Z}/p^{n+1}\mathbb{Z}$ for all n and $x_n \equiv x_{n-1} \pmod{p^n}$, and we have an isomorphism of abelian groups

$$\mathbb{Z}_p \cong \lim_{\leftarrow} \mathbb{Z}/p^k\mathbb{Z}.$$

Moreover, $\mathbb{Z}_p$ is a ring, and $\mathbb{Z} \subset \mathbb{Z}_p$. An integer $n \in \mathbb{Z}$ is invertible in $\mathbb{Z}_p$ if and only if p does *not* divide n.

1.2 Hensel's Lemma

To solve equations in $\mathbb{Z}_p$, the most well-known method follows from Hensel's lemma [4], which is similar to Newton's method in spirit:

Lemma 1 (Hensel)**.** *Let $f(x) \in \mathbb{Z}[x]$ and $n \in \mathbb{N}$. Suppose that $f(a) \equiv 0 \pmod{p^n}$ for some $a \in \mathbb{Z}$, but $p \nmid f'(a)$, where f' is the derivative of f. Then there exists a unique $b \in \mathbb{Z}/p^{n+1}\mathbb{Z}$ such that $f(b) \equiv 0 \pmod{p^{n+1}}$ and $b \equiv a \pmod{p^n}$.*

In fact, Hensel's lemma is more general and extends to the completion of any field K with respect to a valuation, as we will discuss later.

1.3 The Field $\mathbb{Q}_p$

Once we have defined $\mathbb{Z}_p$, the definition of $\mathbb{Q}_p$ follows naturally.

Definition 2. The *field of p-adic numbers* $\mathbb{Q}_p$ is the field of fractions of $\mathbb{Z}_p$.

To build $\mathbb{Q}_p$, one adjoins an inverse of p to $\mathbb{Z}_p$. Therefore, we can view a p-adic number as an expansion

$$a = b_n p^n + b_{n+1} p^{n+1} + \cdots ,$$

where $0 \leq b_i < p$, but $n \in \mathbb{Z}$ instead of $\mathbb{N}$. Again, we have an inclusion of $\mathbb{Q}$ into $\mathbb{Q}_p$.

1.4 Hasse–Minkowski Theorem

After knowing how to solve equations in the p-adics, one might want to compare the roots of a polynomial in $\mathbb{Q}$ with those in $\mathbb{Q}_p$. We know that if there exist roots in $\mathbb{Q}$, then there also exist roots in $\mathbb{Q}_p$ for every p. Speaking again of *global* and *local*, this fact about $\mathbb{Q}$ and $\mathbb{Q}_p$ implies that a "global" root is also a "local" root for every p. What about the converse? The goal would be to patch together local roots in order to obtain a global root. For example, the following proposition is a case in which this procedure works [3]:

Proposition 1. *A number $x \in \mathbb{Q}$ is a square if and only if it is a square in $\mathbb{Q}_p$ for every p.*

This local-global concept is attributed to Hasse, who suggested the following principle [3]:

Local-Global Principle: *If there is a global solution then there are (local) p-adic solutions for all p. In some cases the converse is also true.*

For example, the Hasse–Minkowski Theorem presents a case in which the converse holds [3]:

Theorem 1 (Hasse–Minkowski)**.** *Let $f(x_1, \ldots, x_n) \in \mathbb{Q}[x_1, \ldots, x_n]$ be a quadratic form, i.e., a homogeneous polynomial of degree 2 in n variables. Then, the equation*

$$f(x_1, \ldots, x_n) = 0$$

has non-trivial solutions in $\mathbb{Q}$ if and only if it has non-trivial solutions in $\mathbb{Q}_p$ for each p.

2 p-Adic Valuation and Absolute Value

A very important concept in p-adics and which will allow a lot of machinery running is the definition of the p-adic valuation and absolute value. First we define the absolute value for an arbitrary field.

Definition 3. An *absolute value* on a field K is a function $|\cdot| : K \to \mathbb{R}^+$ satisfying

1. $|x| = 0$ if and only if $x = 0$;
2. $|xy| = |x||y|$ for all $x, y \in K$;
3. $|x + y| \leq |x| + |y|$ for all $x, y \in K$.

Moreover, we say that an absolute value on K is *non-Archimedean* if it satisfies the condition

$$|x + y| \leq \max\{|x|, |y|\}$$

for all $x, y \in K$.

We now define the p-adic valuation on $\mathbb{Z}$ and $\mathbb{Q}$:

Definition 4. Given a prime number $p \in \mathbb{Z}$, the *p-adic valuation* on $\mathbb{Z}$ is the function

$$v_p : \mathbb{Z} \smallsetminus \{0\} \longrightarrow \mathbb{R}$$

defined as follows: for each $n \neq 0 \in \mathbb{Z}$, let $v_p(n)$ be the unique positive integer satisfying

$$n = p^{v_p(n)} n'$$

with $p \nmid n'$. We can extend v_p to $\mathbb{Q}$ as follows: if $x = a/b \in \mathbb{Q}^\times$, then

$$v_p(x) = v_p(a) - v_p(b).$$

The following are fundamental properties of the p-adic valuation [1]:

Lemma 2. *For all $x, y \in \mathbb{Q}$, we have:*

1. $v_p(xy) = v_p(x) + v_p(y)$;
2. $v_p(x + y) \geq \min\{v_p(x), v_p(y)\}$.

Note that the above definition of p-adic valuation is quite similar to the definition of absolute value of a field. This suggests the following essential definition in p-adic theory:

Definition 5. For any $x \in \mathbb{Q}$, define the *p-adic absolute value* of x by

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

if $x \neq 0$, and $|0|_p = 0$.

Moreover, we have [3]:

Proposition 2. *The function $|\cdot|_p$ is a non-Archimedean absolute value on $\mathbb{Q}$.*

In fact, we have this very nice theorem by Ostrowski [6] that characterizes all the possible absolute values in $\mathbb{Q}$. Two absolute values are defined to be *equivalent* if they give rise to the same open sets.

Theorem 2 (Ostrowski)**.** *Let $|\cdot|$ be a non-trivial absolute value on $\mathbb{Q}$. Then:*

1. *If $|\cdot|$ is Archimedean, then $|\cdot|$ is equivalent to $|\cdot|_\infty$ (that is, the standard absolute value in the reals).*
2. *If $|\cdot|$ is non-Archimedean, then $|\cdot|$ is equivalent to $|\cdot|_p$ for exactly one prime p.*

3 Cauchy Sequences and Completion of $\mathbb{Q}$

In this section we describe a different way of defining $\mathbb{Q}_p$ using analysis. We first recall the definition of a Cauchy sequence.

Definition 6. A sequence of elements x_n in a field K with an absolulte value is a *Cauchy sequence* if for every $\epsilon > 0$ one can find a natural number M such that

$$|x_n - x_m| < \epsilon$$

whenever $m, n \geq M$.

With this concept, we can define the completion of a field:

Definition 7. A field K is called *complete* with respect to an absolute value if every Cauchy sequence of elements in K has a limit in K.

These two concepts allow us to define $\mathbb{Q}_p$ in an alternative way [7]:

Theorem 3. *The field of p-adic numbers $\mathbb{Q}_p$ is a completion of $\mathbb{Q}$ with respect to the p-adic metric induced by $|\cdot|_p$.*

In other words, every Cauchy sequence converges in $\mathbb{Q}_p$, and $\mathbb{Q}_p$ is universal among fields with this property containing $\mathbb{Q}$ as a metric subspace with the p-adic metric.

There is a nice convergence criterion for series in $\mathbb{Q}_p$, which is clearly not true in $\mathbb{R}$ (as the harmonic series would be a counterexample):

Lemma 3. *An infinite series $\sum a_n$ in $\mathbb{Q}_p$ converges if and only if $\lim_{n\to\infty} a_n = 0$.*

Now we can prove many of the fundamental properties of $\mathbb{Q}_p$, as in [7]:

Proposition 3. *Let $\mathbb{Q}_p$ be the field of p-adic numbers. Then:*

1. *The unit ball $\{\alpha \in \mathbb{Q}_p : |\alpha|_p \leq 1\}$ is equal to $\mathbb{Z}_p$.*
2. *The p-adic units are $\mathbb{Z}_p^\times = \{\alpha \in \mathbb{Z}_p : |\alpha|_p = 1\}$.*
3. *The only non-zero ideals of $\mathbb{Z}_p$ are the principal ideals*

$$p^k\mathbb{Z}_p = \{\alpha \in \mathbb{Q}_p : v_p(\alpha) \geq k\}.$$

4. *$\mathbb{Z}$ is dense in $\mathbb{Z}_p$, and $\mathbb{Q}$ is dense in $\mathbb{Q}_p$.*

4 Algebraic Extensions of $\mathbb{Q}_p$

While the completion $\mathbb{R}$ of $\mathbb{Q}$ with respect to the ordinary absolute value has only one non-trivial algebraic extension, namely $\mathbb{C}$, this is not true for $\mathbb{Q}_p$, which has finite field extensions of arbitrarily large degrees. We can prove some properties shared by these finite field extensions [3]:

Theorem 4. *Let K be a finite field extension of $\mathbb{Q}_p$. Then $|\cdot|_p$ can be continued in exactly one way to K, and K is complete with respect to this continuation. Denoting this continuation also by $|\cdot|_p$, we have that*

$$|\alpha|_p = |N_{K/\mathbb{Q}_p(\alpha)}|_p^{1/[K:\mathbb{Q}_p]},$$

with our usual definition of the norm N.

To prove the above theorem, one would first note that *if* there exists an absolute value $|\cdot|$ on K extending the absolute value on $\mathbb{Q}_p$, then it is complete with respect to $|\cdot|$. It then follows that $|\cdot|$ is indeed unique, and from this fact we would show that $|\cdot|$ does exist by providing a construction. The norm N plays an essential role in the construction, since if $|\cdot|$ is an absolute value on K then the function $x \to |\sigma(x)|$ is also an absolute value on K, where $\sigma \in \mathrm{Aut}(K/F)$. The norm emerges from the product of all the $\sigma(x)$, as we saw in Chapter 2 of Marcus' book. See Chapter 5 in [3] for a more detailed discussion of the completion of K.

Moreover, given a finite field extension K of $\mathbb{Q}_p$, one can define the ring of p-adic integers of K as

$$\mathcal{O}_{p,K} := \{\alpha \in K : |\alpha|_p \leq 1\}.$$

From here, we start seeing many similarities with our course, and we can define in a similar way as in Chapter 4 of Marcus' book the residue class field of K, the ramification index e, and the residue class degree f. In order to define the residue class field of K, we first define a maximal ideal $m_{p,K}$ of $\mathcal{O}_{p,K}$, given by

$$m_{p,K} := \{\alpha \in K : |\alpha|_p < 1\}.$$

The residue class field of K is then

$$\mathcal{O}_{p,K}/m_{p,K}.$$

Note that, while not obvious, the maxiality of $m_{p,K}$ follows from the definition of $\mathcal{O}_{p,K}$.

Theorem 5. *Let $K, \mathcal{O}, e, f$ be as above. Then:*

1. $[K : \mathbb{Q}_p] = e \cdot f$.
2. *Any element of $\mathcal{O}_{p,K}$ is the root of a monic polynomial with coefficients in $\mathbb{Z}_p$.*
3. *Conversely, if $x \in K$ is the root of a monic polynomial with coefficients in $\mathbb{Z}_p$, then $x \in \mathcal{O}_{p,K}$.*

We conclude with a nice classification theorem for finite totally ramified extensions of $\mathbb{Q}_p$ shown in [7]. Recall that a polynomial

$$f(x) = x^m + a_{m-1}x^{m-1} + \cdots + a_0 \in \mathbb{Z}_p[x]$$

is called an *Eisenstein polynomial* if $a_i \in p\mathbb{Z}_p$ for all i, and $a_0 \notin p^2\mathbb{Z}_p$.

Theorem 6. *If f is an Eisenstein polynomial, then $\mathbb{Q}_p[x]/f(x)$ is totally ramified.*

References

[1] R. B. Ash, *Abstract Algebra: The Basic Graduate Year*, Chapter 7 from lecture notes at the University of Illinois, 2011.

[2] J.-H. Evertse, *p-Adic Numbers*, 2001.

[3] F. Q. Gouvea, *p-Adic Numbers: an Introduction*, Springer-Verlag, 1997 (2nd ed.).

[4] K. Martin, *(Quaternion) Algebras in Number Theory*, Chapter 1 from lecture notes at the University of Oklahoma, 2017.

[5] D. A. Marcus, *Number Fields*, Universitext, Springer, New York, 2018 (2nd ed.).

[6] J. S. Milne, *Algebraic Number Theory*, 2017.

[7] F. Oggier, *Introduction to Algebraic Number Theory*, Lecture notes at Nanyang Technological University, 2009–2010.