P-adic numbers and p-adic analysis

András Földesi

January, 2026

P-adic norm

Definition (p-adic norm)

Let p be any prime number. For any nonzero integer a let $ord_p a$ be the highest power of p which divides a. Now for any nonzero rational number $x = a/b$ let $\mathrm{ord}_p x = \mathrm{ord}_p a - \mathrm{ord}_p b$. It is easy to see that this is well-defined.
Now the map $|\ |_p$ on $\mathbb{Q}$ is called p-adic norm and is defined as follows:

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

P-adic norm

Proposition

The map $|\ |_p$ is a norm on $\mathbb{Q}$, furthermore, it satisfies the following stronger version of the triangle inequality, meaning that the p-adic norm is a non-Archimedean norm:

$$\forall x, y \in \mathbb{Q} : |x + y|_p \leq \max(|x|_p, |y|_p).$$

Theorem (Ostrowski)

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

Completion of $\mathbb{Q}$

Similarly as we get the real numbers from the rational numbers, we will take the Cauchy secquences in $\mathbb{Q}$ according to $|\ |_p$ and define the equivalence classes:

$$\{a_i\} \sim \{b_i\} \Leftrightarrow |a_i - b_i| \to 0.$$

This set of equivalence classes will be denoted $\mathbb{Q}_p$.

Proposition

The p-adic norm extends to $\mathbb{Q}_p$.

Definition

For $a, b \in \mathbb{Q}_p$ $a \equiv b \pmod{p^i}$ if and only if $|a - b|_p \leq p^{-i}$.

Completion of $\mathbb{Q}$

Theorem

Every $a \in \mathbb{Q}_p$, given that $|a|_p \leq 1$, has exactly one representative Cauchy sequence $\{a_i\}$, $a_i \in \mathbb{Z}$ that:

- $0 \leq a_i < p_i$ for $i = 1, 2, 3...$
- $a_i \equiv a_{i+1} \pmod{p^i}$ for $i = 1, 2, 3...$

Corollary

Every $a \in \mathbb{Q}_p$ can be expressed as:

$$a = b_0 p^{-i} + ... + b_{i-1} p^{-1} + b_i + b_{i+1} p + ..., \quad \forall j \in \mathbb{N} : b_j \in \{0, 1, ..., p-1\}$$

for some $i \in \mathbb{N}$.

Completion of $\mathbb{Q}$

Definition

Let $\mathbb{Z}_p = \{x \in \mathbb{Q}_p : |x|_p \leq 1\}$, we call $\mathbb{Z}_p$ the set of p-adic integers. It can be checked that $\mathbb{Z}_p$ is a subring of $\mathbb{Q}_p$.

Remark

Instead of the set $\{0, ..., p-1\}$ we can take any set $S = \{a_0, ..., a_{p-1}\}$ of p-adic integers that has the property $a_i \equiv i \pmod{p}$ for $i = 0, ..., p-1$, and then there is also a unique representative $\sum_{j=-i}^{\infty} b_j p^j,\ b_j \in S$ of any equivalence class in $\mathbb{Q}_p$.

Completion of $\mathbb{Q}$

Theorem (Hensel's lemma)

Let $p(x) = a_n x^n + \ldots + a_0$ be a polynomial with coefficients in $\mathbb{Z}_p[x]$, and let $p'(x) = n a_n x^{n-1} + \ldots + a_1$ be its formal derivative. Now if there exists $b_0 \in \mathbb{Z}_p$ so that $p(b_0) \equiv 0 \pmod{p}$, and $p'(b_0) \not\equiv 0 \pmod{p}$, then there exists a unique $b \in \mathbb{Z}_p$ such that $p(b) = 0$ and $b \equiv b_0 \pmod{p}$.

The algebraic closure of $\mathbb{Q}_p$

Proposition

Let L be a finite field extension of $\mathbb{Q}_p$ then there is at most one norm that extends the p-adic norm.

Theorem

Define the following map on $\overline{\mathbb{Q}_p}$:

$$|x| = |N_x|_p^{1/n},$$

where N_x is the constant term and n is the degree of the minimal polynomial of x over $\mathbb{Q}_p$, this is a non-Archimedean norm extending the p-adic norm defined on $\mathbb{Q}_p$.

The algebraic closure of $\mathbb{Q}_p$

Definition

Let L be a finite extension of $\mathbb{Q}_p$ of order n. For $x \in L$ define

$$\mathrm{ord}_p(x) = -\log_p |x|_p = -\frac{1}{n}|N_x|.$$

This agrees with the definition of ord_p on $\mathbb{Q}_p$.

Definition

Now $\{\mathrm{ord}_p(x) : x \in L\} \subset \frac{1}{n}\mathbb{Z}$, so there exists $e|n : \{\mathrm{ord}_p(x) : x \in L\} = \frac{1}{e}\mathbb{Z}$, we will call e the *index of ramification* of L over $\mathbb{Q}_p$.
The extension L is called *unramified* if the index of ramification is 1 and *totally ramified* if it is n.

The algebraic closure of $\mathbb{Q}_p$

Proposition

Let L be a finite extension of $\mathbb{Q}_p$. Let

$$A = \{x \in L : |x|_p \leq 1\}$$

$$M = \{x \in L : |x|_p < 1\}$$

. Then A is a local ring, which is the integral closure of $\mathbb{Q}_p$ in L with the unique maximal ideal M. Furthermore A/M is a finite extension of $\mathbb{F}_p$.

Proposition

Using the notations from the preceding proposition, let f be the the degree of the extension A/M over $\mathbb{F}_p$, then $n = ef$, where e is the index of ramification of L over $\mathbb{Q}_p$.

The algebraic closure of $\mathbb{Q}_p$

Proposition

If L is a totally ramified extension of $\mathbb{Q}_p$ and for $\alpha \in L$ $\mathrm{ord}_p(\alpha) = 1/e$, then α is the root of an *Eisenstein polynomial*:

$$x^e + a_{e-1}x^{e-1} + \ldots + a_0 = 0, a_i \in \mathbb{Z}_p,$$

where $a_i \equiv 0 \pmod{p}$ for all i, and $a_0 \not\equiv \pmod{p^2}$. Conversely, if α is the root of an Eisenstein polynomial over $\mathbb{Q}_p$ then $\mathbb{Q}_p(\alpha)$ is totally ramified over $\mathbb{Q}_p$ of degree e.

Proposition

There is exactly one unramified extension L_f^{unram} of $\mathbb{Q}_p$ of degree f, that can be obtained by adjoining a primitive $(p^f - 1)$th root of 1. If L is an extension of $\mathbb{Q}_p$ of degree n, index of ramification e and residue field degree f, then $L = L_f^{unram}(\alpha)$, where α satisfies an Eisenstein polynomial with coefficients in L_f^{unram}.

The algebraic closure of $\mathbb{Q}_p$

Corollary

If L is a finite extension of $\mathbb{Q}_p$ of degree n, index of ramification e and residue field of degree f, and if π is chosen so that $\mathrm{ord}_p(\pi) = 1/e$, then every $\alpha \in L$ can be written uniquely in the form:

$$\sum_{i=m}^{\infty} a_i \pi^i,$$

where $m = e\mathrm{ord}_p(\alpha)$ and each a_i satisfies $a_i^{p^f} = a_i$ (the elements of L satisfying this are called Teichmüller representatives).

Completeness of $\overline{\mathbb{Q}_p}$

Theorem

The field $\overline{\mathbb{Q}_p}$ is not complete.

Definition

Take the equivalence classes of Cauchy sequences in $\overline{\mathbb{Q}_p}$, denote this set as Ω.

Theorem

Ω is algebraically closed.

P-adic power series

Let $f(x)$ be a p-adic power series:

$$f(x) = \sum_{n=0}^{\infty} a_n x^n, \ a_n \in \Omega,$$

and this will converge on the set $\{x \in \Omega : \ |x|_p < r\}$, where

$$r = \frac{1}{\limsup |a_n|_p^{1/n}}.$$

Proposition

A sum $\sum_{n=0}^{\infty} a_n, \ a_n \in \Omega$ converges if and only if $\lim_{n\to\infty} |a_n| \to 0$.

Corollary

If $f(x) = \sum_{n=0}^{\infty} a_n x^n, \ a_n \in \Omega$ then $f(x)$ is either converges or diverges on the whole $\{x \in \Omega : |x|_p = r\}$ set, where r is the radius of convergence.

P-adic power series

Definition

Let $D_a(r^-) = \{x \in \Omega : \ |x-a|_p < r\}$ be the *open disk* around a with radius r.
Let $D_a(r) = \{x \in \Omega : \ |x-a|_p \leq r\}$ be the *closed disk* around a with radius r.
It is important that these sets are both open and close in a topological sense, the terms "open" and "closed" only refer to the analogy with the Archimedean case.
In the followings $D(r) = D_0(r)$, $D(r^-) = D_0(r^-)$.
Let R be a ring, then $R[[x]]$ is the ring of formal power series with coefficients in R.

P-adic power series

Lemma

All $f(x) \in \mathbb{Z}_p[[x]]$ converges in $D(1^-)$.

Lemma

All $f(x) \in \Omega[[x]]$, which converges on a disk $D = D(r^-)$ or $D(r)$ is continuous on D.

P-adic power series

The *p-adic logarithm*:

$$\log_p(1+x) := \sum_{n=1}^{\infty} \frac{(-1)^{n+1}}{n} x^n, \quad D(1^-).$$

The *p-adic exponential*:

$$\exp_p(x) := \sum_{n=1}^{\infty} \frac{1}{n!} x^n, \quad D(p^{-1/(p-1)}).$$

The *p-adic binomial expansion*:

$$B_{a,p}(x) = (1+x)^a := \sum_{n=1}^{\infty} \frac{a(a-1)...(a-n+1)}{n!} x^n, \quad D(p^{-1/(p-1)}).$$

P-adic power series

Proposition

If $a \in \mathbb{Z}_p$ then $B_{a,p} \in \mathbb{Z}_p[[x]]$, and so it converges on $D(1^-)$.

Proposition

The functions $\log_p$ and $\exp_p$ give mutually inverse isomorphisms between the multiplicative group of $D_1(p^{-1/(p-1)})$ and the additive group of $D_0(p^{-1/(p-1)})$.

Proposition

There exists a unique extension f of $\log_p$ to $\Omega^\times$ such that:

- $f(xy) = f(x) + f(y)$ for all $x, y \in \Omega^\times$
- $f(p) = 0$.

We will use the notation $\log_p$ for this f from now on.

Newton polygons

Definition

Let $f(x) = 1 + \sum_{i=1}^{n} a_i x^n \in q + x\Omega[x]$ be a polynomial of degree n and constant term 1. Then the *Newton polygon* of f is the convex hull of the set $\{(0,0)\} \bigcup \{(i, \mathrm{ord}_p a_i) : i = 1, ..., n\}$, i.e. the highest polygonal line joining $(0,0)$ and $(n, \mathrm{ord}_p a_n)$, that passes on or below all of the points in this set.
The *vertices* of the Newton polygon are the points $(i, \mathrm{ord}_p a_i)$, where the slope changes. If e segment joins the points (i, m) and (i', m'), then its *slope* is $(m' - m)/(i' - i)$, and the *length of the slope* is $i' - i$.

Lemma

Let $f(x) = (1 - x/\alpha_1)...(1 - x/\alpha_n) \in \Omega[x]$, where $\alpha_i,\ i = 1, ..., n$ are the roots of f. Let $\lambda_i = \mathrm{ord}_p 1/\alpha_i$. If λ is a slope of the Newton polygon of f with length l, then precisely l of the λ_i are equal to λ.

Newton polygons

Definition

Let $f(x) = 1 + \sum_{i=1}^{\infty} a_i x^i \in 1 + x\Omega[[x]]$ be a power series. Let $f_n(x) = 1 + \sum_{i=1}^{n} a_i x^i \in 1 + x\Omega[x]$ be the nth partial sum of $f(x)$. The *Newton polygon* of f is the limit of the Newton polygons of the f_n.

Lemma

Let b be the least upper bound of all slopes of the Newton polygon of $f \in 1 + x\Omega[[x]]$, then the radius of convergence of f is p^b (if $b = \infty$ then f converges everywhere on Ω).

Newton polygons

p-adic Weierstrass Preparation Theorem

Let $f \in 1 + x\Omega[[x]]$. Suppose that f converges on $D(p^\lambda)$. Let N be the horizontal length of all segments of Newton polygon having slope less than or equal to λ, if that is finite. Otherwise, the Newton polygon has last slope λ, then let N be the greatest i for which $(i, \mathrm{ord}_p a_i)$ lies on the Newton polygon (it exists due to the convergence on $D(p^\lambda)$). Then there exists $h(x) = 1 + \sum_{i=1}^{n} b_i x^i \in 1 + x\Omega[x]$ and $g(x) \in 1 + x\Omega[[x]]$, such that g converges and is nonzero on $D(p^\lambda)$ and $h(x) = f(x)g(x)$ on $D(p^\lambda)$. Furthermore h is uniquely determined by these properties, and its Newton polygon coincides with the Newton polygon of f until $(N, \mathrm{ord}_p a_N)$.