Introduction to P-Adic Numbers

Labix

May 16, 2023

Abstract

Contents

1 Algebraic Properties

1.1 Two Formulations of p-adic Numbers

Definition 1.1.1: Coherrent Sequence

Let p be a prime. A coherrent sequence is a sequence $x_1, x_2, \dots$ of integers such that

$$x_{n+1} \equiv x_n \pmod{p^n}$$

for $n \in \mathbb{N} \setminus \{0\}$. Two coherrent sequences are said to be equivalent if

$$x_n \equiv y_n \pmod{p^n}$$

for $n \in \mathbb{N} \setminus \{0\}$.

Trivially the relation defines an equivalent relation in the set of all coherrent sequences.

Definition 1.1.2: p-adic Integers

Let p be a prime. A p-adic integer is an equivalence class of coherrent sequences.

Proposition 1.1.3

The set of all p-adic integers for a fixed prime p is an integral domain $\mathbb{Z}_p$ that contains the ring $\mathbb{Z}$.

Proof. Addition is trivial for sequences in general. Multiplication in this ring is defined by term by term multiplication. To see that it is an integral domain, we require that multiplication of any two non-zero element in $\mathbb{Z}_p$ to be non-zero. This can also be seen easily since $x_n y_n \equiv 0 \pmod{p^n}$ if and only if one of x_n or y_n is divisible by p^n. □

Now that we have defined p-adic integers through coherrent sequences, let us see an equivalent definition using power series.

Definition 1.1.4: p-adic Series

Let p be a prime number. A p-adic series is a series of the form

$$\sum_{k=0}^{\infty} a_k p^k$$

where every a_k is a rational number $\frac{n_k}{d_k}$ such that none of n_k and d_k is divisible by p.

Notice that if each a_k is an integer instead of a rational number, this is just a base p number.

Proposition 1.1.5

Every p-adic series with integer coefficients represents a p-adic integer.

Proof. Suppose that we are given a p-adic series $x = \sum_{k=0}^{\infty} a_k p^k$. Then define b_n by

$$b_n = \sum_{k=0}^{n-1} a_k p^k$$

Notice that taking modulo p^n on x gives precisely b_n. Thus $(b_1, b_2, \dots)$ as defined by the partial sums is a coherrent sequence. □

Proposition 1.1.6

Every p-adic integer represents a p-adic series with integer coefficients.

Proof. Suppose that we have a coherrent sequence $x = (x_1, x_2, \dots)$. By definition, we know that $x_{n+1} - x_n \equiv 0 \pmod{p^n}$. This means that $b_{n+1} = \frac{x_{n+1}-x_n}{p^n}$ is an integer. Setting $b_0 = a_0$, we have that

$$x = \sum_{k=0}^{\infty} b_k p^k$$

and we are done. □

Now we have established a correpsondence between these two system of integers. Taking the field of fractions with $\mathbb{Z}_p$ allows us to form p-adic series with coefficients in $\mathbb{Q}$.

Definition 1.1.7: p-adic Numbers

Define the field of fractions of $\mathbb{Z}_p$, the p-adic integers to be the p-adic numbers, denoted $\mathbb{Q}_p$.

Lemma 1.1.8

Let p be a prime. Then $\mathbb{Q}_p$ contains $\mathbb{Q}$ as a subring and $\mathbb{Z}_p$ contains $\mathbb{Z}$ as a subring.

1.2 Divisibility in $\mathbb{Z}_p$

Although division is properly defined for commutative rings, we will restate a bunch of definitions from commutative rings theory.

Definition 1.2.1: Divisibility

Let $x, y \in \mathbb{Z}_p$. We say that x divides y if there exists $k \in \mathbb{Z}_p$ such that $xk = y$. In this case we say that $x|y$.

Proposition 1.2.2

Let $k \in \mathbb{N}$. Then p^k divides $(x_1, x_2, \dots) \in \mathbb{Z}_p$ if and only if $p^k | x_k$.

Proof. Suppose that there exists some $y \in \mathbb{Z}_p$ such that $p^k y = x$. Then in particular, $p^k y_k = x_k$ thus $p^k | x_k$. Suppose for the contrary that $p^k | x_k$. Then by coherence, we have that $p^k | x_n$ for all $n < k$. Define a coherent sequence y by

$$y_n = \begin{cases} 0 & \text{if } n < k \\ \frac{x_n}{p^k} & \text{if } n \geq k \end{cases}$$

Then $p^k y = x$. Indeed for $n < k$, we must have $x_n \equiv x_k \equiv 0 \equiv p^k y_n \pmod{p^n}$. □

In this proof, the main thing to take away is that once there factor of p^k in x_k, it will naturall be in x_n for $n \geq k$ from the fact that $x_{k+1} \equiv x_k \pmod{p^k}$ etc. So we can properly divide out $\frac{x_n}{p^k}$ to get an integer. This allows y to be nonzero despite having a bunch of zeroes at the begining.

Recall that units in a ring are precisely those that have a multiplicative inverse inside the ring.

Lemma 1.2.3

If $x \in \mathbb{Z}_p$, then x is a unit if and only if p does not divide x.

Proof. Suppose that $p|x$. From the above proposition we see that $p|x_1$. This means that the first element in the coherrent squence is 0. Now since $x_2 \equiv x_1 \pmod{p}$, we have that $x_2 \equiv 0 \pmod{p}$. Moreover, since $x_{n+1} \equiv x_n \pmod{p^n}$, it is easy to see by induction that x_n for all n will contain a factor of p and thus $p|x$ would be imply that x is the additive identity of $\mathbb{Z}_p$, the coherrent sequence $(0, 0, \dots)$ and thus does not have an inverse and is not a unit.

Now suppose that p does not divide x. By the same argument, since p does not divide x_1, p will not divide x_n for all $n \in \mathbb{N}$. This would imply that p^n also does not divide x_n. By modular arithmetic there exists y_n such that $x_n y_n \equiv 1 \pmod{p^n}$. Thus $(y_1, y_2, \dots)$ will be an inverse of x. □

Corollary 1.2.4

Any non-zero element of $\mathbb{Z}_p$ has the form $p^m u$ where $m \in \mathbb{N}$ and $u \in \mathbb{Z}_p$ is a unit.

1.3 $\mathbb{Q}_p$ as an Euclidean Domain

Now that we have derived some properties of units in $\mathbb{Z}_p$, we proceed to define a valuation on $\mathbb{Q}_p$ so that it forms an Euclidean domain. Recall that in order for $\mathbb{Q}_p$ to be an Euclidean domain, we need to define a valuation.

Definition 1.3.1: p-adic valuation

Define the p-adic valuation to be a function $v_p : \mathbb{Q}_p \to \mathbb{N}$ defined by

$$v_p(x) = \max\{k \in \mathbb{N} | p^k \text{ divides } x\}$$

if $x \in \mathbb{Z}_p$. For $\frac{x}{y} \in \mathbb{Q}_p$, define the p-adic valuation to be

$$v_p\left(\frac{x}{y}\right) = v_p(x) - v_p(y)$$

With this proposition, $\mathbb{Z}_p$ naturally inherits properties of PID as well as UFD.

Proposition 1.3.2

Let p be a prime. Then $\mathbb{Q}_p$ is an Euclidean domain with Euclidean valuation defined by the function $v_p(x)$.

Proof. We show that the norm defined above satifies the properties of a Euclidean valuation. Let $a, b \in \mathbb{Z}_p$. If $a|b$ then there exists $k \in \mathbb{Z}_p$ such that $ka = b$. Then trivially $v_p(0) = 0 < v_p(b)$ and we are done. If a does not divide b then □

Proposition 1.3.3

Let $x, y \in \mathbb{Q}_p$. Then the following are true.

- $v_p(xy) = v_p(x) + v_p(y)$
- $v_p(x + y) \geq \min\{v_p(x), v_p(y)\}$

2 Topological Properties

2.1 Norm

Definition 2.1.1: p-adic Norm

Define the p-adic norm for $x \in \mathbb{Q}_p$ to be

$$|x|_p = \frac{1}{p^{v_p(x)}}$$

Define $|0|_p = 0$ for convention.

The idea behind the notion is that the distance is measured by how large of a power of p can divide x. The larger the power, the closer it is to 0.

Proposition 2.1.2

The p-adic norm on $\mathbb{Q}_p$ satisfies the properties of a norm and thus $\mathbb{Q}_p$ is a normed space.

Recall that the notion of a Valuation and that of a norm is slightly different. The codomain of valuations are natural numbers while that of norms are non-negative real numbers.

Definition 2.1.3: Non-Archimedean Norm

We say that a norm $|\cdot| : X \to \mathbb{R}^+ \cup \{0\}$ is non-achimedean if for all $x, y \in X$, we have the ultrametric inequality

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

Otherwise we say that it is Archimedean.

Lemma 2.1.4

The p-adic norm is a non-achimedean norm on $\mathbb{Q}_p$.

Theorem 2.1.5: Ostrowski's Theorem

Every nontrivial norm on $\mathbb{Q}$ is equivalent to either the standard norm or one of the p-adic norms.

2.2 Metric Properties

Recall that norms give rise to metrics.

Proposition 2.2.1

The function $d_p : \mathbb{Z}_p \times \mathbb{Z}_p \to \mathbb{R}^+ \cup \{0\}$ defined by

$$d_p(x, y) = |x - y|_p$$

is a metric on $\mathbb{Z}_p$. Similarly, the the function $d_p : \mathbb{Q}_p \times \mathbb{Q}_p \to \mathbb{R}^+ \cup \{0\}$ defined by

$$d_p(x, y) = |x - y|_p$$

is a metric on $\mathbb{Q}_p$.

Proposition 2.2.2

The metric space $\mathbb{Z}_p$ is a completion of $\mathbb{Z}$ with respect to the p-adic metric. Similaarly, the metric space $\mathbb{Q}_p$ is a completion of $\mathbb{Q}$ with respect to the p-adic metric.

Think of coherrent sequences in $\mathbb{Q}_p$ as rational approximations to irrational numbers as in the completion of $\mathbb{Q}$ by $\mathbb{R}$. Recall that irrational numbers can be defined alternatively by a sequence of converging rational numbers. This is why $\mathbb{Q}_p$, as a sequence of rational numbers, is also doing some sort of approximation to fill in the gaps of the sparse $\mathbb{Q}$, just in a different way as $\mathbb{R}$.

2.3 Topological Properties

Theorem 2.3.1

Let $B_r(x)$ be an open ball in $\mathbb{Q}_p$. Then $B_r(x)$ is also closed.

Corollary 2.3.2

$\mathbb{Z}_p$ is both an open and closed subset of $\mathbb{Q}_p$.

2.4 Geometry of $\mathbb{Q}_p$

Theorem 2.4.1

In $\mathbb{Q}_p$, all triangles are isoceles.

Lemma 2.4.2

No three distinct points in $\mathbb{Q}_p$ are collinear.

2.5 Relation to Hensel's Lemma

We can reformulate Hensel's lemma with the p-adic norm.

Proposition 2.5.1: Hensel's Lemma

Let $f \in \mathbb{Z}_p[x]$. Suppose that there exists $x \in \mathbb{Z}_p$ and $k \in \mathbb{Z}$ such that

$$|f'(x)|_p = p^{-k}$$

and $p^{2k+1}|f(x)$. Then there exists a unique $y \in \mathbb{Z}_p$ such that

$$f(y) = 0 \text{ and } y \equiv x \pmod{p^{k+1}}$$

In practise, we build the root from the ground up, which is we start from the case $k = 0$. This gives the following special case of Hensel's lemma.

Lemma 2.5.2

Let $f \in \mathbb{Z}_p[x]$. Suppose that there exists $x \in \mathbb{Z}_p$ such that $f(x) \equiv 0 \pmod{p}$ and $f'(x)$ not congruent to 0 modulo p. Then there exists a unique $y \in \mathbb{Z}_p$ such that $f(y) = 0$ and $y \equiv x \pmod{p}$.

Proof. Take $k = 0$ in Hensel's lemma. □

We give a procedure in calculating the actual roots of the polynomial based on the constructive proof of Hensel's lemma. I tacitly assume that we start from the ground up.

Step1: Break apart the congruence into coprime congruences if the modulo in question is not the power of a prime. Step 2: Find the actual $x \in \mathbb{Z}_p$ that satisfies Hensel's lemma. Rename it to a_1 (or b_1 depending on the following method used).
Step 3: Compute a_{k+1} using the recursion formula

$$a_{k+1} \equiv a_k - f(a_k)[f'(a_1)]^{-1} \pmod{p^{k+1}}$$

or

$$b_{k+1}f'(b_k) \equiv -\frac{f(b_k)}{p^k} \pmod{p}$$

Step 4: If you used the first formula, then a_n will be your answer to the particular modulo if the question asks for $f \in \mathbb{Z}[x]$ modulo p^n. If you used the second formula, then
$b = b_1 + b_2p + b_3p^2 + \cdots + b_np^{n-1}$ will be your answer to the particular modulo.
Step 5: Combine the different answers into one single answer that solves the original question using the Chinese Remainder Theorem.