The p-Adic Numbers

Lam Nguyen
University of Utah

1 The Ring of p-Adic Integers

1.1 p-Adic Integers

Given a natural number p and another natural number x, the **base p representation** of x is defined as $d_n \dots d_2 d_1 d_0$ where

$$x = d_0 + d_1 p + d_2 p^2 + \cdots + d_n p^n = \sum_{i=0}^{n} d_i p^i$$

and each $0 \leq d_i < b$ is an integer. The existence and uniqueness of such a representation is proven using the Euclidean Algorithm and induction. As long as n is finite, the series above will converge to the finite natural number x in the usual sense.

Let us now proceed formally and permit infinite sums of the form

$$\sum_{i=0}^{\infty} d_i p^i = d_0 + d_1 p + d_2 p^2 + \cdots$$

Maintaining the same conditions that $0 \leq d_i < p$ and p is a natural number, this infinite sum will not converge in general. However, when all but finitely many d_i equal zero, then we observe that the series converges to some natural number.

We now introduce new terminology to include the formal sums we showed above.

Definition 1.1. A **p-adic digit** is a natural number d such that $0 \leq d < p$, where p is prime. We call the sequence of p-adic digits $(d_i)_{i \in \mathbb{N}}$ a **p-adic integer**, which corresponds to the formal sum $\sum_{i=0}^{\infty} d_i p^i$. Conventinally, the **$p$-adic** representation of (d_i) is written as

$$\cdots d_i \cdots d_2 d_1 d_0.$$

Define $\mathbb{Z}_p$ as the set of all p-adic integers:

$$\begin{aligned} \mathbb{Z}_p &:= \{(d_i)_{i \in \mathbb{N}} : d_i \text{ is a } p\text{-adic digit}\} \\ &= \{\dots d_i \dots d_2 d_1 d_0 : d_i \text{ is a } p\text{-adic digit}\} \end{aligned}$$

Note that we will interchangeably use the sum $\sum_{i=0}^{\infty} d_i p^i$, sequence (d_i), or representation $\cdots d_i \cdots d_2 d_1 d_0$ to denote a p-adic integer.

There is a natural inclusion of the natural numbers into the p-adic integers $\mathbb{N} \to \mathbb{Z}_p$: if $x \in \mathbb{N}$, then

$$x = \sum_{i=0}^{n} d_i p^i \mapsto (d_0, d_1, \dots, d_n, 0, 0 \dots).$$

Observe the left hand side is a finite sum, so it is a natural number but not a p-adic integer. The right hand side is a p-adic integer since it corresponds to an infinte sum. Hence, all natural numbers are p-adic integers with finitely many nonzero terms. Some of the important natural numbers are 0 and 1 which map to

$$0 \mapsto (0, 0, 0, \ldots) \quad \text{and} \quad 1 \mapsto (1, 0, 0, \ldots)$$

for any prime p.

1.2 Arithmetic of p-Adic Integers

Despite the fact that we permit infinitely many digits, we can actually think about arithmetic with p-adic integers the same way we do with ordinary natural numbers in any base. When adding natural numbers, we add digit by digit and carry over 1 whenever the digit sum equals or exceeds the base. With natural numbers, this process terminates since we have finitely many digits. With p-adic integers, we perform this ad infinitum.

Formally, let $\cdots a_3a_2a_1a_0$ and $\cdots b_3b_2b_1b_0$ be p-adic integers. Addition is defined digit by digit: if $\cdots c_3c_2c_1c_0 = \cdots a_3a_2a_1a_0 + \cdots b_3b_2b_1b_0$, then

$$\begin{aligned} c_0 &\equiv a_0 + b_0 \pmod{p} \\ c_i &\equiv a_i + b_i + \epsilon_{i-1} \pmod{p} \end{aligned}$$

where $a_{i-1} + b_{i-1} = c_{i-1} + \epsilon_{i-1}p$. We call ϵ_{i-1} the *carry digit* and it is either 0 or 1. This simply formalizes the act of carrying over 1 to the left whenever the digit sums equals or exceeds the base. For example, adding two 5-adic integers looks like:

$$\begin{array}{cccccc} & \ldots & 3 & 4 & 1 & 2 & 1 \\ + & \ldots & 0 & 3 & 4 & 3 & 2 \\ \hline & \ldots & 4 & 3 & 1 & 0 & 3 \end{array}$$

By defining p-adic addition as addition modulo p, it follows that p-adic addition is commutative and associative. Furthermore, $0 = \cdots 0000_p$ is the additive identity.

The subtraction scheme is similarly defined as we learned in grade school, where we have to borrow a 1 from the right in case the top digit is smaller than the bottom digit. Instead of a carry digit, we have a *borrow digit*. This process shows that every p-adic integer has an additive inverse. For example, the 5-adic inverse of 1 is

$$\begin{array}{ccccccc} & \ldots & 0 & 0 & 0 & 0 & 0 \\ \text{-} & \ldots & 0 & 0 & 0 & 0 & 1 \\ \hline & \ldots & 4 & 4 & 4 & 4 & 4 \end{array}.$$

We are simply borrowing a 1 from the right column ad infinitum. Hence $-\cdots 00001_5 = \cdots 44444_5$.

Lastly, recall the process of how we multiply natural numbers in grade school. The exact same process applies to p-adic integers. For example, multiplying two 5-adic integers looks like

$$\begin{array}{ccccccc} & \ldots & 2 & 0 & 4 & 4 & 1 \\ \times & \ldots & 1 & 2 & 3 & 3 & 4 \\ \hline & \ldots & 3 & 3 & 4 & 1 & 4 \\ & \ldots & 2 & 4 & 2 & 3 & \\ & \ldots & 4 & 2 & 3 & & \\ & \ldots & 3 & 2 & & & \\ & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ \hline & \ldots & 4 & 2 & 4 & 4 & 4 \end{array}$$

Since p-adic multiplication boils doing to multiplication modulo p, it is commutative and associative, with $\cdots 00001_p$ as the multiplicative identity.

1.3 Algebra of $\mathbb{Z}_p$

Observing that addition and multiplication are both defined as such, this suggests $\mathbb{Z}_p$ has a ring structure. We can do one better than that, which leads to the following proposition.

Proposition 1.2. *$\mathbb{Z}_p$ is an integral domain.*

Proof. The discussion above shows that $\mathbb{Z}_p$ is a commutative ring. We need to show that $\mathbb{Z}_p$ has no zerodivisors. Suppose $\alpha = \sum_{i=0}^{\infty} a_i p^i$ and $\beta = \sum_{i=0}^{\infty} b_i p^i$ are nonzero elements of $\mathbb{Z}_p$. Then α and β have a nonzero digit, say a_n and b_m. The product $\alpha\beta$ will have

$$c_{n+m} \equiv a_n b_m \pmod{p}$$

as its $(n+m)^{\text{th}}$ digit. As p-adic digits, a_n and b_m are not divisible by p. It follows that c_{n+m} is not divisible by p. Hence c_{n+m} is nonzero and consequently so is $\alpha\beta$. □

Unfortunately, $\mathbb{Z}_p$ is not a field. Not every p-adic integer has an inverse, but the condition for when there is an inverse is simply stated:

Lemma 1.3. *A p-adic integer $(d_i) = \sum_{i=0}^{\infty} d_i p^i$ is invertible if and only if $d_0 \neq 0$.*

Proof. Let's first define *reduction modulo p* as the map $\varphi : \mathbb{Z}_p \to \mathbb{Z}/p\mathbb{Z}$ by

$$(d_i) = \sum_{i=0}^{\infty} d_i p^i \mapsto d_0 \pmod{p}.$$

We claim this is a ring homomorphism. Indeed, suppose $\alpha = (a_i)$ and $\beta = (b_i)$ are elements of $\mathbb{Z}_p$. Then $\alpha \mapsto a_0$ and $\beta \mapsto b_0$. Consider $\alpha + \beta$. Then by definition of p-adic addition, the first term is $a_0 + b_0 \pmod{p}$. Thus,

$$\varphi(\alpha + \beta) = a_0 + b_0 \pmod{p} = \varphi(\alpha) + \varphi(\beta).$$

Note that the addition on the RHS is also modulo p. Next, for $\alpha\beta$, the first term is $a_0 b_0 \pmod{p}$. Hence,

$$\varphi(\alpha\beta) = a_0 b_0 \pmod{p} = \varphi(\alpha)\varphi(\beta).$$

Lastly, for the multiplicative identity, we have $\varphi(\cdots 00001) = 1 \pmod{p}$. Therefore, φ is a ring homomorphism.

Using φ, we easily prove the forward direction of the lemma. Suppose (d_i) is invertible. Since φ is a ring homomorphism, $\varphi((d_i)) = d_0$ must also be invertible. This implies d_0 is a unit of $\mathbb{Z}/p\mathbb{Z}$, which means $d_0 \neq 0$.

Now, in the reverse direction, suppose $d_0 \neq 0$. We want to show that (d_i) is invertible. Recalling that multiplication is performed digit by digit modulo p, we can find an inverse $a_0 = d_0^{-1} \in \mathbb{Z}/p\mathbb{Z}^{\times}$ such that $d_0 a_0 \equiv 1 \pmod{p}$. If we write

$$(d_i) = \sum_{i=0}^{\infty} d_i p^i = d_0 + d_1 p + d_2 p^2 + \ldots = d_0 + p\delta,$$

where $\delta \in \mathbb{Z}_p$, then multiplying (d_i) by a_0 gives us

$$(d_i) \cdot a_0 = d_0 a_0 + p\delta a_0 = 1 + tp$$

where $t = \delta a_0 \in \mathbb{Z}_p$. If we show that $1 + tp$ is invertible, then we will have an inverse for (d_i) since

$$(d_i) \cdot a_0 \cdot (1 + pt)^{-1} = 1 \implies (d_i)^{-1} = a_0(1 + tp)^{-1}.$$

By the Binomial Theorem, we can write

$$(1 + tp)^{-1} = 1 - tp + (tp)^2 - \ldots = 1 + b_1 p + b_2 p^2 + \ldots$$

where b_i satisfy $0 \leq b_i \leq p - 1$. We can expand every term collect like terms modulo p to obtain these coefficients. Every term besides 1 must contain a factor of p, so the constant 1 term is never eliminated. Hence, $(1 + tp)^{-1}$ is always nonzero, so we have a found an inverse for $1 + tp$. □

2 The Field of p-Adic Numbers $\mathbb{Q}_p$

When working with the usual integers $\mathbb{Z}$, we can construct a field from the ring $\mathbb{Z}$ by considering its fraction field, which we will denote as $\text{Frac}(\mathbb{Z})$. This field is precisely the rational numbers $\mathbb{Q}$. The ease of defining such a field lies in the fact that $\mathbb{Z}$ is an integral domain. We have no problems defining multiplication of fractions since the denominators will never be zerodivisors (or zero, obviously, as a fraction with a zero denominator makes no sense to begin with).

2.1 Constructing $\mathbb{Q}_p$

Since we have shown that $\mathbb{Z}_p$ is an integral domain, it is perfectly valid to consider its fraction field $\text{Frac}(\mathbb{Z}_p)$. By analogy to the integers and rationals, we will conventionally define

$$\mathbb{Q}_p \coloneqq \text{Frac}(\mathbb{Z}_p) = \left\{ \frac{\alpha}{\beta} : \alpha, \beta \in \mathbb{Z}_p, \beta \neq 0 \right\}$$

Elements of $\mathbb{Q}_p$ are called the **p-adic numbers**. We define addition and multiplication of p-adic numbers in the usual way:

$$\frac{\alpha}{\beta} + \frac{\alpha'}{\beta'} = \frac{\alpha\beta' + \beta\alpha'}{\beta\beta'} \quad \text{and} \quad \frac{\alpha}{\beta}\frac{\alpha'}{\beta'} = \frac{\alpha\alpha'}{\beta\beta'}.$$

Likewise, we define the equivalence of fractions in the usual way:

$$\frac{\alpha}{\beta} \sim \frac{\alpha'}{\beta'} \iff \alpha\beta' = \beta\alpha'.$$

Now, the elements of $\mathbb{Z}_p$ are defined as the formal sums $\sum_{i=0}^{\infty} d_i p^i$. It turns out that elements of $\mathbb{Q}_p$ also have a similarly nice representation. At the moment, elements of $\mathbb{Q}_p$ are just fractions of infinite formal sums. To find a nicer representation, we are going to need a notion of size in $\mathbb{Q}_p$. The absolute value in $\mathbb{Q}$ and $\mathbb{R}$ is a way to measure size, but in $\mathbb{Z}_p$ and $\mathbb{Q}_p$, it does not help us at all. Elements of $\mathbb{Z}_p$ are infinite formal sums that hopelessly diverge from the perspective of real analysis. Putting them into fractions makes that situation even worse. It is then generally nonsensical to measure the size of a p-adic number. We must rethink what it means to be an absolute value and measure size.

2.2 Absolute Values and Valuations

Let F be a field and let $\mathbb{R}_{\geq 0}$ be the set of non-negative real numbers. An absolute value should give some idea of the size of an element in the field F. So we want to abstract the most essential properties we expect from an absolute value.

Definition 2.1. An **absolute value** on F is a function

$$|\cdot| : F \to \mathbb{R}_{\geq 0}$$

satisfying the following properties:

(a) $|x| = 0$ if and only if $x = 0$

(b) $|xy| = |x||y|$ for all $x, y \in F$

(c) $|x + y| \leq |x| + |y|$

We call the absolute value **non-archimedean** if it satisfies the following property:

(d) $|x + y| \leq \max\{|x|, |y|\}$

Otherwise, we say that the absolute value is **archimedean**.

While it is conventional to define the absolute value over a field, it suffices to define one over an integral domain. Properties a) and b) require that we have no zerodivisors, hence why we must have at least an integral domain and not just any ring. Hence, as we will soon see, we can begin defining absolute values for $\mathbb{Z}_p$ and $\mathbb{Q}_p$.

Before we get there, let's see some examples to get used to various absolute values. It is easy to check that the usual absolute value on $\mathbb{R}$ satisfies the first three properties and not the fourth, making it archimedean. It is convenient to call this one the **infinite absolute value**, written as $|\cdot|_\infty$.

Even more boring than the infinite absolute value is the **trivial absolute value** over any field F:

$$|x| = \begin{cases} 1 & x \neq 0 \\ 0 & x = 0 \end{cases}.$$

We see that property a) is satisfied by definition. Property b) is easy to see since all nonzero element, and consequently their products, has absolute value of 1. If either x or y are zero, then the product must then be zero. For property c), considering the possible cases of x and y, we get $0 \leq 0$ or $1 \leq 1$ when we evaluate the absolute values. This even implies property d). Hence, the trivial absolute value is, in fact, an absolute value that is non-archimedean.

To obtain more interesting absolute values that will bring us to closer to defining one over $\mathbb{Q}_p$, we introduce the notion of valuations. We first note that given any $n \in \mathbb{Z}$ and prime $p \in \mathbb{Z}$, we can write

$$n = p^v n'$$

where $\gcd(p, n') = 1$. By the Fundamental Theorem of Arithmetic, this factorization, and hence v, is unique. Of course, v is zero if $\gcd(p, n) = 1$, but that does not detract from that v is still unique. Since v depends on p and n, we define a new function $v = v_p(n)$ that gives the multiplicity of p in the factorization of n.

Definition 2.2. The **p-adic valuation** on $\mathbb{Z}$ is the function

$$v_p : \mathbb{Z} \to \mathbb{R}$$

defined as follows: for each nonzero integer $n \in \mathbb{Z}$, let $v_p(n)$ satisfying

$$n = p^{v_p(n)} n' \quad \text{with} \quad p \nmid n'.$$

If $n = 0$, set $v_p(0) = +\infty$. We extend v_p to $\mathbb{Q}$ as follows: if $x = a/b \in \mathbb{Q}$, $b \neq 0$, then

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

Definition 2.3. The p**-adic valuation extended to** $\mathbb{Z}_p$ is equivalently defined to the p-adic valuation on $\mathbb{Z}$. That is, let α be a p-adic integer such that the smallest power of p is $k > 0$:

$$\begin{aligned}\alpha = \sum_{i=k}^{\infty} d_i p^i &= d_k p^k + d_{k+1} p^{k+1} + \dots \\ &= p^k(d_k + d_{k+1} p + \dots) \\ &= p^k \sum_{i=k}^{\infty} d_i p^{i-k}\end{aligned}$$

Then $v_p(\alpha) = k$. If $k = 0$, then $v_p(\alpha) = 0$. As usual, $v_p(0) = +\infty$. Hence, the p-adic valuation on $\mathbb{Z}_p$ gives the smallest power of p in the expansion.

The valuation on $\mathbb{Z}_p$ will be useful for us later on, but for now, let's focus on $\mathbb{Z}$ and $\mathbb{Q}$. We can think of v_p as counting function, counting how many divisors of p a number has. If the number is rational, the valuation is determined by the formula

$$x = p^{v_p(x)} \cdot \frac{a}{b} \qquad p \nmid ab,$$

i.e. v_p counts the multiplicity of p when x is in lowest terms. Let's see examples to get a feel for p-adic valuations.

Example 2.4. Compute a) $v_5(400)$, b) $v_7(902)$, c) $v_3(123/48)$, and d) $v_{11}(1/22)$.

(a) Since $400 = 5^2 \cdot 16$, then $v_5(400) = 2$.

(b) We have that $7 \nmid 902$, so $v_7(902) = 0$.

(c) We have $123 = 3 \cdot 41$ and $48 = 3 \cdot 16$, so $v_3(123) = 1$ and $v_3(48) = 1$. Hence, $v_3(123/48) = v_3(123) - v_3(48) = 0$.

(d) Lastly, $v_{11}(1) = 0$ and $v_{11}(22) = 1$ so $v_{11}(1/22) = -1$.

So for a fixed prime p, an integer with a higher power of p receives a higher valuation than one with few powers of p. For rational numbers, the valuation depends on the numerator and denominator. Numbers with more powers of p in the numerator than the denominator receive a positive valuation, which increases as the valuation of the numerator. Conversely, if the denominator has a higher valuation than the numerator, the number receives a negative valuation, which decreases as the valuation of the denominator increases.

The valuation nearly gives us an alternative notion of size in terms of the multiplicity of a prime factor. Now we say nearly because the valuation does not satisfy the absolute value properties. Most obviously, the valuation can be negative, but an absolute value must be non-negative. The following two properties of the valuation also indicate why it is not absolute value but almost:

Lemma 2.5. *For all x and y in $\mathbb{Q}$, we have*

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

(b) $v_p(x + y) \geq \min\{v_p(x), v_p(y)\}$.

Proof. We simply the definition. Suppose x and y are integers. Write $x = p^{v_p(x)} x'$ and $y = p^{v_p(y)} y'$ where $p \nmid x', y'$. Since we can interchange x and y whenever necessary, assume $v_p(x) \leq v_p(y)$. Then

$$xy = p^{v_p(x)} x' p^{v_p(y)} y' = p^{v_p(x)+v_p(y)} x'y'$$

where $p \nmid x'y'$ by Euclid's Lemma from number theory. This proves part (a). We also have

$$x' + y' = p^{v_p(x)}x' + p^{v_p(y)}y' = p^{v_p(x)}(x' + p^{v_p(y)-v_p(x)})y'.$$

Hence, $v_p(x+y) \geq v_p(x) = \min\{v_p(x), v_p(y)\}$. This completes the proof for integers. For fractions, if $x = t/q$ and $y = r/s$, then

$$\begin{aligned} v_p(xy) = v_p\left(\frac{tr}{qs}\right) &= v_p(tr) - v_p(qs) \\ &= v_p(t) + v_p(r) - v_p(q) - v_p(s) \\ &= v_p\left(\frac{t}{q}\right) + v_p\left(\frac{r}{s}\right). \end{aligned}$$

Similarly,

$$\begin{aligned} v_p(x+y) = v_p\left(\frac{ts+rq}{qs}\right) &= v_p(ts+rq) - v_p(qs) \\ &\geq \min\{v_p(ts), v_p(rq)\} - v_p(qs) \\ &= \min\{v_p(ts) - v_p(qs), v_p(rq) - v_p(qs)\} \\ &= \min\left\{v_p\left(\frac{t}{s}\right), v_p\left(\frac{q}{s}\right)\right\} \end{aligned}$$

□

This lemma suggests how we can turn the valuation into an absolute value. Property (b) is similar to the non-archimedean property, which is $|x+y| \leq \max\{|x|, |y|\}$. If we simply reverse the sign, we get

$$-v_p(x+y) \leq \max\{-v_p(x), -v_p(y)\}$$

Property (a) is a sum while the absolute value requires a product, so let's just put the valuation into an exponent, e.g.

$$p^{v_p(xy)} = p^{v_p(x)}p^{v_p(y)}.$$

Combining the negation and the exponentiation, we arrive at a brand new absolute value.

Definition 2.6. For any $x \in \mathbb{Q}$, the **p-adic absolute value** of x is defined as

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

if $x \neq 0$. Otherwise, set $|0|_p = 0$.

Definition 2.7. The **p-adic absolute value on $\mathbb{Z}_p$** is defined the same way. If $\alpha = \sum_{i=1}^{\infty} d_i p^i \in \mathbb{Z}_p$, then

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

where

$$\alpha = p^{v_p(\alpha)} \sum_{i=v_p(\alpha)}^{\infty} d_i p^i.$$

Proposition 2.8. *The function $|\cdot|_p$ is a non-archimedean absolute value.*

Proof. Everything follows either by definition or by applying Lemma 2.5. □

Let's see some examples of computing the p-adic absolute value.

Example 2.9. To better understand how p-adic absolute values compare, let's fix $p = 5$ and compute $|16|_5, |50|_5, |125|_5, |1/50|_5$, and $|1/625|_5$.

$$\begin{aligned}
|16|_5 &= 5^{-v_5(16)} = 5^0 = 1 \\
|50|_5 &= 5^{-v_5(50)} = 5^{-2} = \frac{1}{25} \\
|125|_5 &= 5^{-v_5(125)} = 5^{-3} = \frac{1}{125} \\
\left|\frac{1}{50}\right|_5 &= 5^{-v_5(1/50)} = 5^2 = 25 \\
\left|\frac{1}{125}\right|_5 &= 5^{-v_5(1/125)} = 5^3 = 125
\end{aligned}$$

From this example, we can immediately draw some qualitative conclusions. Any numbers with no factors of p have the same "size" of 1. Numbers with more factors of p in the numerator become smaller in "size". However, numbers with more factors in the denominator become larger in "size".

2.3 p-Adic Number Representation

Using the p-adic valuation and absolute value, the field $\mathbb{Q}_p$ become less mysterious. Currently, $\mathbb{Q}_p$ is simply the set of formal fractions of $\mathbb{Z}_p$, but using valuations, we can prove the following proposition:

Proposition 2.10. *Any $x \in \mathbb{Q}_p$ can be represented as a series of the form*

$$\sum_{i=m}^{\infty} d_i p^i = d_m p^m + d_{m+1} p^{m+1} + \ldots + d_0 + d_1 p + \ldots$$

where m is an integer and each $0 \leq d_i < p$ is an integer.

Proof. Recall that $\mathbb{Q}_p = \mathrm{Frac}(\mathbb{Z}_p)$. We want to show that

$$\left\{ \sum_{i=m}^{\infty} d_i p^i : m \in \mathbb{Z}, d_i \in \mathbb{Z}, 0 \leq d_i < p \right\} = \mathrm{Frac}(\mathbb{Z}_p).$$

For $m \geq 0$, the series is just a p-adic integer, and since $\mathbb{Z}_p \subset \mathbb{Q}_p$, we have nothing to prove there. Suppose $m < 0$. Then the series is written as

$$\begin{aligned}
\sum_{i=m}^{\infty} d_i p^i &= d_m \frac{1}{p^{-m}} + d_{m+1} \frac{1}{p^{-(m+1)}} + \ldots + d_0 + d_1 p + \ldots \\
&= d_m \frac{1}{p^{-m}} + d_{m+1} \frac{1}{p^{-(m+1)}} + \ldots + \sum_{i=0}^{\infty} d_i p^i
\end{aligned}$$

Since $m < 0$, it follows that each $p^{-m} \in \mathbb{Z}_p$. Furthermore, since each $d_i \in \mathbb{Z}_p$, each term that is not part of the infinite series has the form α/β where $\alpha, \beta \in \mathbb{Z}_p$, i.e. they belong to $\mathrm{Frac}(\mathbb{Z}_p)$. The infinite series is a p-adic integer, which corresponds to $\alpha/1$ in $\mathbb{Q}_p$ where $\alpha \in \mathbb{Z}_p$. Hence, we have a sum of elements in $\mathbb{Q}_p$, which proves that

$$\left\{ \sum_{i=m}^{\infty} d_i p^i : m \in \mathbb{Z}, d_i \in \mathbb{Z}, 0 \leq d_i < p \right\} \subseteq \mathrm{Frac}(\mathbb{Z}_p).$$

In the other direction, suppose $\alpha/\beta \in \mathbb{Q}_p$ is a p-adic number, where $\alpha, \beta \in \mathbb{Z}_p$. Suppose that $v_p(\alpha) = n$ and $v_p(\beta) = k$. Recall that we already defined valuations on $\mathbb{Z}_p$ in Definition 2.3. Then, α and β are written as

$$\alpha = p^n \sum_{i=n}^{\infty} a_i p^{i-n}$$

$$\beta = p^k \sum_{j=k}^{\infty} b_j p^{j-k}$$

By Lemma 1.3, the summation factors of α and β are invertible p-adic integers since they both have nonzero constant terms a_n and b_k. Hence, we can write α/β as

$$\frac{\alpha}{\beta} = \frac{p^n \sum\limits_{i=n}^{\infty} a_i p^{i-n}}{p^k \sum\limits_{j=k}^{\infty} b_j p^{j-k}} = p^{n-k} \left(\sum_{i=n}^{\infty} a_i p^{i-n} \right) \left(p^k \sum_{j=k}^{\infty} b_j p^{j-k} \right)^{-1} = p^{n-k} u$$

where u is the product of the two invertible p-adic integers. Observe that u is an invertible p-adic integer, i.e. it has a non-zero constant term, i.e. $v_p(u) = 0$. If $n \geq k$, then p^{n-k} is also a p-adic integer, i.e. α/β is p-adic integer with the expansion as desired. Similarly, if $n < k$, then we shift the powers in the expansion of u down by $k - n$ so that we have negative indices with negative powers of p, as desired. Thus,

$$\left\{ \sum_{i=m}^{\infty} d_i p^i : m \in \mathbb{Z}, d_i \in \mathbb{Z}, 0 \leq d_i < p \right\} \supseteq \operatorname{Frac}(\mathbb{Z}_p).$$

□

So far, we have only defined them over $\mathbb{Q}$ and $\mathbb{Z}_p$. Using this proposition, it is a trivial matter to extend the p-adic valuation and absolute value to $\mathbb{Q}_p$.

Definition 2.11. The p-adic valuation extended to $\mathbb{Q}_p$ is defined as follows: if $x = \sum_{i=m}^{\infty} d_i p^i$ where m is the smallest integer with non-zero coefficient, then

$$v_p(x) = m.$$

Definition 2.12. The p-adic absolute value extended to $\mathbb{Q}_p$ is defined as follows: if $x = \sum_{i=m}^{\infty} d_i p^i$ where m is the smallest integer with non-zero coefficient, then

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

We also have representation of p-adic numbers as strings of numbers in the right-to-left convention.

Definition 2.13. The p-adic representation of the p-adic number $x \in \mathbb{Q}_p$ where

$$x = \sum_{i=m}^{\infty} d_i p^i = d_m p^m + \ldots + d_{-1} p^{-1} + d_0 + d_1 p + d_2 p^2 + \ldots$$

and the integer $m < 0$ is given by

$$x = \cdots d_2 d_1 d_0 \, . \, d_{-1} \cdots d_m$$

Example 2.14. Suppose we want the 5-adic representation of $\frac{7}{15}$. In $\mathbb{Z}_p$, using the summation notation of p-adic integers, we have

$$7 = \sum_{i=0}^{\infty} a_i \cdot 5^i \quad \text{where} \quad (a_i) = (2, 1, 0, 0, \ldots)$$

$$15 = \sum_{i=0}^{\infty} b_j \cdot 5^j \quad \text{where} \quad (b_j) = (0, 3, 0, 0, \ldots).$$

So in $\mathbb{Q}_p$, 7/11 corresponds to the fraction of p-adic integers

$$\frac{\alpha}{\beta} = \frac{\sum\limits_{i=0}^{\infty} a_i \cdot 5^i}{\sum\limits_{j=0}^{\infty} b_j \cdot 5^j}$$

where $\alpha = \sum_{i=0}^{\infty} a_i \cdot 5^i$ and $\beta = \sum_{i=0}^{\infty} b_j \cdot 5^j$. The previous theorem guarantees we have a nice summation representation. To obtain it, we use the same technique as the proof. We first observe that $v_5(\alpha) = 0$ and $v_5(\beta) = 1$. By Lemma 1.3, α is invertible in $\mathbb{Z}^p$ since it has a nonzero constant term, but β is not. Using the fact that $v(\beta) = 1$, we can write

$$\begin{aligned} \beta &= 5 \sum_{j=1}^{\infty} b_j \cdot 5^{j-1} \\ &= 5(3 + 0 \cdot 5 + 0 \cdot 5^2 + \ldots) \end{aligned}$$

where the sum of the RHS is invertible in $\mathbb{Z}_p$. Thus,

$$\frac{\alpha}{\beta} = \frac{\sum\limits_{i=0}^{\infty} a_i \cdot 5^i}{5 \sum\limits_{j=1}^{\infty} b_j \cdot 5^{j-1}} = 5^{-1} \left(\sum_{i=0}^{\infty} a_i \cdot 5^i \right) \left(\sum_{j=1}^{\infty} b_j \cdot 5^{j-1} \right)^{-1}.$$

It remains to find the inverse of $\sum_{j=1}^{\infty} b_j \cdot 5^{j-1} = 3 + 0 \cdot 5 + 0 \cdot 5^2 + \ldots$. To do this, we appeal to its p- adic representation as $\cdots 003_5$, that is 3 in the 'ones' position and 0 in all other positions ad infinitum. We need a p-adic integer that, when multiplied by $\cdots 003_5$, gives the identity $\cdots 001_5$. Since we are working modulo 5, it is simple to do this digit by digit. We first find a digit that when mutliplied by 3 gives 1 modulo 5. Then the remaining digits must multiply in a such a way that produces 0. In practice, we apply grade school multiplication while keeping modulo 5 in mind.

$$\begin{array}{ccccccc}
 & \ldots & 0 & 0 & 0 & 0 & 3 \\
\times & \ldots & 1 & 3 & 1 & 3 & 2 \\
\hline
 & \ldots & 0 & 0 & 0 & 1 & 1 \\
 & \ldots & 0 & 0 & 1 & 4 & \\
 & \ldots & 0 & 0 & 3 & & \\
 & \ldots & 1 & 4 & & & \\
 & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\
\hline
 & \ldots & 0 & 0 & 0 & 0 & 1
\end{array}$$

Hence $(\cdots 003)^{-1} = \cdots 13132_5$. Finally, we simply multiply the p-adic integers to obtain α/β. Writing $\sum_{i=0}^{\infty} a_i \cdot 5^i$ as $\cdots 0012_5$, we multiply it to $(\cdots 003)^{-1} = \cdots 13132_5$ in the usual way:

$$\begin{array}{ccccccc}
 & \ldots & 1 & 3 & 1 & 3 & 2 \\
\times & \ldots & 0 & 0 & 0 & 1 & 2 \\
\hline
 & \ldots & 3 & 1 & 3 & 1 & 4 \\
 & \ldots & 3 & 1 & 3 & 2 & \\
 & \ldots & 0 & 0 & 0 & & \\
 & \ldots & 0 & 0 & & & \\
 & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\
\hline
 & \ldots & 1 & 3 & 1 & 3 & 4
\end{array}$$

Thus, we arrive at the 5-adic representation of 7/15:

$$\begin{aligned}\frac{\alpha}{\beta} &= 5^{-1}(\cdots 13134)\\ &= 5^{-1}(4\cdot 5^0 + 3\cdot 5^1 + 1\cdot 5^2 + 3\cdot 5^3 + 1\cdot 5^4 + \cdots)\\ &= 4\cdot 5^{-1} + 3\cdot 5^0 + 1\cdot 5^1 + 3\cdot 5^2 + 1\cdot 5^3 + \cdots\end{aligned}$$

i.e.

$$\frac{7}{15} = \cdots 1313.4_5$$

2.4 Algebra of $\mathbb{Q}_p$

Using the p-adic absolute value, we can explore the algebra of $\mathbb{Q}_p$ more deeply. This sections serves to simply state interesting results regarding the algebra of $\mathbb{Q}_p$.

Proposition 2.15. *Let F be a field and $|\cdot|$ be a non-archimedean absolute value. The set*

$$\mathcal{O} = \{x \in F : |x| \leq 1\} \subset F$$

*is a subring of F, and it is called the **valuation ring** of $|\cdot|$. The set*

$$\mathcal{B} = \{x \in F : |x| < 1\} \subset \mathcal{O}$$

*is an ideal of $\mathcal{O}$, and it is called the **valuation ideal** of $|\cdot|$. Furthermore, $\mathcal{B}$ is a maximal ideal in $\mathcal{O}$, and every element of the complement $\mathcal{O} - \mathcal{B}$ is invertible in $\mathcal{O}$.*

Definition 2.16. A ring that contains a unique maximal ideal whose complement consists of invertible elements is called a **local ring**.

It follows from that definition above that a valuation ring is a local ring.

Proposition 2.17. *The ring of p-adic integers is the valuation ring*

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

which implies that $\mathbb{Z}_p$ is a local ring.

This proposition is consistent with every we have seen so far. Any integer with no factor of p has absolute value of 1, and integers with factors of p have absolute value less than 1 and decreases as the number of factors of p increases.

Conversely, fractions, in lowest terms, whose denominators have a factor of p have absolute value greater than 1. An interesting implication of this proposition is that fractions with no factors of p in the numerator and denominator must be p-adic integers, since their valuation is 0 and absolute value is thus 1. We briefly saw this earlier when inverting p-adic integers with nonzero constant terms, e.g. when we inverted $\cdots 0003_5$ to get $1/3 = \cdots 13132_5$ in the previous example.

Since $\mathbb{Z}_p$ is a local ring, it must have a unique maximal ideal by definition. The following proposition describes what this ideal is.

Proposition 2.18. *The maximal ideal of $\mathbb{Z}_p$ is $p\mathbb{Z}_p = \{x = \mathbb{Q}_p : |x|_p < 1\}$.*

We also know that $\mathbb{Z}_p$ is a valuation ring, which we used to deduce it is a local ring. Thus, $\mathbb{Z}_p$ is also its valuation ideal, and it consists of the multiples of p. By Proposition 2.15, it follows that $\mathbb{Z}_p^\times = \mathbb{Z}_p - p\mathbb{Z}_p$. This is consistent with Lemma 1.3, since multiples of p have zero constant term, i.e. they are not invertible. Invertible integers, on the other hand, have a constant term and cannot be divisible by p.

This final corollary should not be a surprise given our understanding of the representation of a p-adic number in $\mathbb{Q}_p$.

Corollary 2.19. *$\mathbb{Q}_p = \mathbb{Z}_p[1/p]$, that is, $\mathbb{Q}_p$ is obtained by adjoining the inverse of p to $\mathbb{Z}_p$. In other words, $\mathbb{Q}_p$ is the kernel of $\mathbb{Z}_p[x] \to \mathbb{Q}_p$ sending $x \mapsto 1/p = p^{-1}$.*

3 Brief Look into p-Adic Analysis

In previous examples, we put an equality between a clearly finite number and a clearly divergent series, e.g. $1/3 = \cdots 13132_5$. Assuming the corresponding sequence of digits is never eventually zero, then our knowledge of real analysis tells us this infinite should hopelessly diverge. But divergence is simply a matter of perspective.

In the last couple of sections, we introduce new tools, that is a new absolute value, that we claim fixes our divergent situation. Let's recall the definition of convergent and Cauchy sequences. Suppose we have a sequence (x_n) in a normed space X, i.e. X has an absolute value.

Convergent: The sequence (x_n) converges to $x \in X$ if, for $\epsilon > 0$, there exists $N \in \mathbb{N}$ such that whenever $n > N$, $|x_n - x| < \epsilon$.

Cauchy: The sequence (x_n) is Cauchy if, for $\epsilon > 0$, there exists $N \in \mathbb{N}$ such that whenever $n, m > N$, $|x_n - x_m| < \epsilon$.

In general, all convergent sequences are Cauchy, but not all Cauchy sequences are convergent. In the case of $\mathbb{Q}$, we know from real analysis that $\mathbb{Q}$ is not complete, i.e. not all Cauchy sequences in $\mathbb{Q}$ converge. To fix this, we construct the real numbers $\mathbb{R}$ as a completion of $\mathbb{Q}$, and one way of doing this is defining equivalences classes of Cauchy sequences in $\mathbb{Q}$ as way to plug the "holes". The key part of this construction is that it depends on the absolute value. The choice of absolute value thus dictates what elements of the completion look like. What if we pick a different absolute value?

Proposition 3.1. *$\mathbb{Q}_p$ is a completion of $\mathbb{Q}$ with respect to the p-adic absolute value $|\cdot|_p$.*

This is an amazing fact since our hopelessly divergent sums now have a chance at being Cauchy and converge in a meaningful way. Let's look at an example to illustrate this fact.

Example 3.2. We know from the previous example that $7/15 = \cdots 1313.4_5$. Let's consider the sequence of 5-adic numbers $(0.4_5, 3.4_5, 13.4_5, 313.4_5, 1313.4_5, \ldots)$. We claim this sequence is Cauchy with respect to $|\cdot|_5$ and hence converges. To illustrate this claim concretely, let's compare $|13.4_5 - 3.4_5|_5$ with $|1313.4_5 - 313.4_5|_5$:

$$|13.4_5 - 3.4_5|_5 = |10.0_5|_5 = 5^{-v_5(10.0)} = 5^{-1} = \frac{1}{25}$$
$$|1313.4_5 - 313.4_5|_5 = |1000.0_5|_5 = 5^{-v_5(1000.0)} = 5^{-3} = \frac{1}{125}$$

The distance between terms of the sequences decreases as we move forward. For $\epsilon < 1/5^k$, we just need to choose x_i and x_j in the sequence such that $v_5(x_i - x_j) > k$. This means the first k terms of x_i and x_j are the same, so the subtraction would leave 5^{k+1} as the lowest power of 5. As k increases arbitrarily, the 5-adic absolute value then decreases arbitrarily, i.e. the sequence converges.

Equipped with the fact that all Cauchy sequences in $\mathbb{Q}_p$ are convergent, we can begin building another field of analysis analogous to real analysis. As the section title suggests, this is known as p-adic analysis. It is known that the p-adic absolute value induces a metric on $\mathbb{Q}_p$ so we can talk about the topology of $\mathbb{Q}_p$ and work our way towards the notion of limits, continuity, differentiation, etc.

We call a field equipped with a non-archimedean absolute value an *ultrametric space.* Since the p-adic absolute value is non-archimedean, then $\mathbb{Q}_p$ is an ultrametric space. The topology and analysis on $\mathbb{Q}_p$ is then much more exotic compared to real analysis, where the absolute value is archimedean. For example, all triangles in an ultrametric space are always isosceles. Every point in an open and closed ball is a center of that ball, which is counterintuitive to our geometric picture of ball that has a single center. Every ball, open or closed, is both open and closed. These are just a few of the interesting facts about $\mathbb{Q}_p$, and ultrametric spaces in general, that lead to the strange and exotic world of p-adic analysis.

References

[1] Brian Courthoute, Pablo Guzman, and Antoine Ronk. *The p-adic integers.* `https://math.uni.lu/eml/projects/reports/P-adics.pdf`

[2] Fernando Q Gouvea. *p-adic Numbers: An Introduction.* Berlin, Springer, 1997.

[3] David A Madore. *A first introduction to p-adic number.* 7 December 2000, `http://www.madore.org/ david/math/padics.pdf`

[4] Julian Marhonic *The p-adics, Hensel's Lemma, and Newton Polygons.* `https://math.uchicago.edu/ may/REU2013/REUPapers/Marohnic.pdf`