Exploration of p-Adic Number Systems and Adelic Number Systems

Ryan Persson

June 9, 2022

Contents

1 Introduction

p-adics are an alternative number system to the Reals. The most important difference between the p-adics and reals, is that in the p-adics, distance is defined in terms of how many times the prime factor p occurs. Each prime p defines a different p-adic number systems. So there are p-adic number systems for each prime p, i.e. the 2-adics, 3-adics, 5-adics, 7-adics, etc... The p-adics at first seem like a strange and unnatural number system, however we are given a hint as to their importance by Ostrowski's theorem, which states that every non-trivial absolute value on the rational numbers is equivalent to either the usual, real absolute value, or one of the infinitely many p-adic absolute values.

From a high level, the p-adics can be divided into several different number systems categorized similarly to the standard $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$. At the lowest level is the ring of p-adic integers, $\mathbb{Z}_p$. The natural numbers and integers are embedded in the set of p-adic integers; $\mathbb{N}, \mathbb{Z} \subset \mathbb{Z}_p$. Similarly, the rational numbers, $\mathbb{Q} = \{\frac{x}{y} : x, y \in \mathbb{Z} \times \mathbb{Z} \setminus \{0\}\}$ have a p-adic analog $\mathbb{Q}_p = \{\frac{x}{y} : x, y \in \mathbb{Z}_p \times \mathbb{Z}_p \setminus \{0\}\}$. Finally, the p-adic absolute value shows that $\mathbb{Q}_p$ is complete, and is analogous to $\mathbb{R}$ in the standard decimal number system.

In this paper we will examine the various types of p-adic numbers, their properties and applications. For the sake of clarity, when talking about various sets of numbers, we will refer to $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$ as the "standard" number systems and $\mathbb{Z}_p, \mathbb{Q}_p$, as the p-adic integers and the field of p-adic numbers or p-adic rationals.

2 Representation of p-Adic Integers:

In this paper, p-adic integers are expressed in several equivalent notations. The first is as an infinite string of digits: $\ldots d_3 d_2 d_1 d_{0_p}$, where each p-adic digit d_i is a natural number less than p, i.e. $d_i \in \{0, \ldots, p-1\}$. Similarly to base 10, such a p-adic integer is the sum of each digit d_i times the base p to the ith power, p^i, i.e.:

$$\sum_{i=0}^{\infty} d_i \times p^i = d_0 p^0 + d_1 p^1 + d_2 p^2 + d_3 p^3 + \ldots = \ldots d_3 d_2 d_1 d_{0_p}.$$

For all natural numbers $\mathbb{N} \in \mathbb{Z}_p$, the sequence (d_i) contains only finitely many non-zero elements. For example, 11_{10} maps to the *3*-adic integer $\ldots 000102_3$ since $11 = 2 + 9 = 2 \times 3^0 + 0 \times 3^1 + 1 \times 3^3$. The inclusion of infinitely many zeros to the left seems strange for natural numbers, as they could be more succinctly expressed using finitely many right-hand digits., (i.e. $11_{10} = 102_3$). But this notation makes more sense when we examine p-adic integers outside of the natural numbers, [6] as will be done later. It is also common for p-adic integers to be expressed in the notation $(d_0, d_1, d_2, ...)$ (or $(d_0, d_1, d_2, \ldots, d_i, 0, 0, 0, \ldots)$ when $(d_i) \in \mathbb{N}$) to denote that all but finitely many digits are zero[6]. In summary, the various equivalent ways that p-adic integers are written are:

- As a power series: $\sum_{i=0}^{\infty} d_i \times p^i$
- As a sequence of digits: $(d_i) = (d_0, d_1, d_2, \ldots)$

- As a truncated string of digits in base p: $\ldots d_2 d_1 d_{0_p}$.

When showing the same number in both base 10 and base p, we will denote the base using subscripts at the end of strings representing numbers. i.e. $11_{10} = ...000102_3$ denotes 11 in base 10 and as a *3*-adic sequence.

3 Addition and Subtraction on the *p*-Adics:

Addition and subtraction on the p-adics is defined digit-wise base p. Given two p-adics, $a = \ldots a_3 a_2 a_1 a_0$ and $b = \ldots b_3 b_2 b_1 b_0$, addition is defined digit-wise such that $c = \ldots c_3 c_2 c_1 c_0 = \ldots a_3 a_2 a_1 a_0 + \ldots b_3 b_2 b_1 b_0$.
The sum c is calculated digit-wise as:
$c_0 \equiv a_0 + b_0 \pmod{p}$
$c_i \equiv a_i + b_i + \epsilon_{i-1} \pmod{p}$
where $\epsilon_{i-1} \in \{0, 1\}$ is the carry digit, and is calculated as the quotient of the sum of the two previous digits of a and b, i.e. $a_{i-1} + b_{i-1} = c_{i-1} + \epsilon_{i-1} p$.
In this number system, $0_{10} = \ldots 0000_p$ is the additive identity , and $1_{10} = \ldots 0001_p$ is the multiplicative identity.

Given a p-adic number, we can calculate its additive inverse, using the additive identity $\ldots 0000_p$. So for example, the additive inverse of $1_{10} = \ldots 0001_3$ is $\ldots 2222_3$, since $\ldots 0001_3 + \ldots 2222_3 = \ldots 0000_3$. This works, because as 1 is added to the first digit $d_0 = 2$ of $\ldots 2222_3$, it changes to $3 \equiv 0 \pmod{p}$ and the carry digit moves up to d_1. This process continues through the infinitely many digits of $\ldots 2222_3$ leaving $\ldots 000_3 = 1_{10}$, the additive identity. This leads to the unusual notation that the additive inverse of 1, in the 3-adics, is $-1_{10} = \ldots 2222_3$ [6].

Based on this alternate formulation for numbers in p-adic systems, infinite series which diverge in the reals, often converge in the p-adics. As this would mean $\sum_{i=0}^{\infty} 2 \times 3^i = -1$ in the 3-adic number system. This is one case where the need for infinitely many digits to the left arises in p-adic notation, when describing p-adics outside of the natural numbers.

In general, negative integers in the p-adics are expressed by an infinite sequence of digits, where all but finitely many digits are $p - 1$. From this we can see that the standard integers are a subset of the p-adic integers, $\mathbb{Z} \subset \mathbb{Z}_p$, and can be expressed as:

$$x \in \mathbb{Z},$$

$$x = \begin{cases} ...0...d_3 d_2 d_1 d_{0_p} & \text{if } x \geq 0 \\ ...(p-1)...d_3 d_2 d_1 d_{0_p} & \text{if } x < 0. \end{cases}$$

4 Multiplication and Division on *p*-Adics:

This section is brief, as multiplication and division are defined similarly on the p-adics to how they are defined on the integers and rational numbers, with a few important distinctions.

A p-adic integer n is a unit, i.e. it has an inverse $n^{-1} \in \mathbb{Z}_p$ if and only if, $gcd(n,p) = 1$, equivalently its first digit d_0 is non-zero and its p-adic absolute value, $|n|_p = 1$. [7]. This means that the majority of p-adic integers do not have an inverse in $\mathbb{Z}_p$ and thus it is not a field.

Division on the p-adic integers consists of multiplying by the divisor's inverse. Since not all p-adic integers have an inverse in $\mathbb{Z}_p$, it is necessary to introduce the rationals on the p-adics, $\mathbb{Q}_p = \{\frac{\alpha}{\beta} : \alpha, \beta \in \mathbb{Z}_p \times \mathbb{Z}_p \setminus \{0\}\}$.

Adding the rationals extends the p-adics to include numbers which include negative powers of prime p as factors. P-adic rationals are denoted somewhat similarly to rationals in base-10. A decimal point is added on the right and digits are added to the right to indicate multiples of negative powers of p.

Actually calculating the digits of a multiple of two p-adics is not as trivial as addition and subtraction. Given $a, b \in \mathbb{Z}_p$ we can find the nth digit by representing a, b in their power series form and using the Cauchy product rule for infinite series, and carrying digits in excess of p while summing the previous terms as follows:

$$a = \sum_{n=0}^{\infty} a_n p^n, b = \sum_{n=0}^{\infty} b_n p^n$$

$$ab = (\sum_{n=0}^{\infty} a_n p^n)(\sum_{n=0}^{\infty} b_n p^n) = c$$

$$c = \sum_{n=0}^{\infty} c_n p^n,$$

where

$$c_k = \sum_{n=0}^{k} a_n b_{k-n} + (a_{n-1} b_{k-n-1}(\mod p^{n-1}))$$

is the kth digit of c.

Extending the p-adic integers $\mathbb{Z}_p$ to the p-adic rational numbers gives what is commonly referred to as the field of p-adic numbers $\mathbb{Q}_p$. Properties of numbers in this field will be the subject of much of the rest of this text. We will examine their representation and how it differs from p-adic integers in the section on p-adic absolute value.

5 Connection with Two's complement:

There is an interesting connection between p-adic arithmetic and the way arithmetic and storage of binary numbers is efficiently done in computers [3]. Binary arithmetic for base 2 numbers is made fast and efficient by storing binary numbers in a format called Two's Complement. Two's Complement expression of integers is as follows. Given an integer a stored in an n bit datatype as $(d_n d_{n-1} ... d_2 d_1 d_0)$, $d_i \in \{0, 1\}$. If $0 \leq a < 2^{n-1} - 1$, then a is stored as normal base 2, i.e.

$$a = \sum_{i=0}^{n-1} d_i 2^i = d_0 2^0 + d_1 2^1 + ... + d_{n-1} 2^{n-1} = d_{n-1} \dots d_2 d_1 d_0.$$

The nth bit of the datatype is reserved to store the sign of the integer, if $d_n = 0$, the integer is positive. However, if $d_n = 1$, that denotes that a is a negative integer, $-2^{n-1} < a < 0$. In this case, the value of the integer is calculated differently. First, take the binary array, $a = (d_n...d_1d_0)$ and subtract 1 from it. Take the new binary array $(d_n...d_1d_0) - (0...01)$ and calculate the logical not of it. So all zeroes are flipped to 1s, and 1s are changed to zeros. Given this new array $(d'_n d'_{n-1}...d'_1 d'_0) =!((d_n...d_1d_0) - (0...01))$. The value of a is then calculated as:

$$a = -\sum_{i=0}^{n-1} d'_i 2^i = -d'_0 2^0 - d'_1 2^1 - ... - d'_{n-1} 2^{n-1}.$$

The reason why 2's complement is the most commonly used representation for negative integers in binary, is that it allows addition, subtraction and multiplication to be performed exactly the same way with positive or negative integers[3]. Most real integer data types use 16 or 32-bits. But for brevity of explanation, we will look at how 2-s complement works in an 8-bit integer array.

To give a concrete example of how two's complement works and why it works for addition specifically, let us use $19_{10} = 16 + 2 + 1 = 10011_2 = (00010011)$. The first bit is set to zero to show that the integer is positive. Using the process for finding 2's complement, $-19 =!((00010011) - (00000001)) =!(00010010) = (11101101)$. To show how Two's complement enables fast boolean addition, calculate $19_{10} + -19_{10} = (00010011)_2 + (11101101)_2 = (00000000)_2 = 0_{10}$. This same ease of boolean arithmetic allows Two's Complement notation to allow subtraction and multiplication of negative integers on the same logic gates that handle positive integers.

However, this ease of boolean computation is not the reason I am introducing Two's Complement integers in this paper. There is a deep and interesting comparison between Two's complement integers, and 2-adic integers. n-bit integers in Two's complement representation, act exactly like 2-adic integers, truncated to n-bits. For example, in the 2-adics, the integer $-1_{10} = ...1111_2$ with infinitely many 1s to the left. This is because -1 is the additive inverse of 1. So the representation of -1 must be such that $1 + -1 = 0$. This indeed works, since $...0001_2 + ...1111_2 = ...0000_2$ as addition carries the excess 1 to the left and zeros out every digit. Similarly, in 8-bit Two's Complement representation, $-1 = (11111111)_2, 1 = (00000001)_2, 1 + -1 = (00000001)_2 + (11111111)_2$. The carry digit is added and iterates through every digit, till it reaches the sign digit d_8 and sets it to zero, leaving the additive identity $(00000000)_2 = 0_{10}$.

6 *p*-Adic Valuation and *p*-Adic Absolute Value:

In this section, we'll introduce the p-adic valuation function $\nu_p(n)$. Given $n \in \mathbb{Z}$ (or $\mathbb{Z}_p$), $n = p_1^{e_1} p_2^{e_2} ... p_k^{e_k}$, $\{p_1, ..., p_k\}$ are the prime factors of n and $\{e_1, e_2, \ldots, e_k\}$ are the multiplicities of each prime factor p_i. The function $\nu_{p_i}(n) = e_i$, describes the number of times that the prime factor p_i occurs in n [7]. If p_i is not a prime factor of n, then $\nu_{p_i}(n) = 0$. So n can be expressed as:

$$n = \prod_{p \in \text{prime}} p_i^{\nu_{p_i}(n)}$$

n can be recovered as the product of all primes, each prime p_i to the power of $\nu_{p_i}(n)$, since $p_i^{\nu_{p_i}(n)} = p_i^0 = 1$ for each prime that is not a prime factor of n.

The ***p*-Adic Norm** or ***p*-Adic Absolute Value** is a Non-Archimedean absolute value over $\mathbb{Z}_p$ and $\mathbb{Q}_p$, the p-adic integers and rationals. The p-adic norm is defined in terms of the p-adic valuation function:

$$\forall x \in \mathbb{Q}_p, |x|_p = p^{-\nu_p(x)}.$$

The p-adic norm$|\cdot|_p$ is an absolute value function since it follows the 3 necessary properties of absolute value functions[7]:

(i) $|x| = 0$ iff $x = 0$
(ii) $\forall x, y \in \mathbb{Q}_p, |xy| = |x||y|$
(iii) $\forall x, y \in \mathbb{Q}_p, |x + y| \leq |x| + |y|$ (Triangle Inequality)

From this point on, we will denote the real absolute value function as $|*|$ and a p-adic absolute value for prime p as $|*|_p$.

Given a p-adic integer $n \in \mathbb{Z}_p$, s.t. the smallest power of p in n is $k > 0$. Then $n = ...d_{k+2}d_{k+1}d_k0...0$, so d_k is the first non-zero of n.
We can write n as:

$$n = \sum_{i=k}^{\infty} d_i p^i = d_k p^k + d_{k+1}p^{k+1} + \cdots = p^k(d_k + d_{k+1}p + d_{k+1}p^2 + \dots) = p^k b,$$

$b \in \mathbb{Z}$ and $gcd(b, p) = 1$.
Then $\forall n \in \mathbb{Z}_p, n = p^k b$, the p-adic absolute value of n is: $|n|_p = p^{-k} = p^{-\nu_p(n)}$.

This leads to a few interesting properties of p-adic integers. $\forall n \in \mathbb{Z}_p$, if $gcd(n, p) = 1$ then $|n|_p = p^{-0} = 1$, since p is not a prime factor of n.
If $\nu_p(n) = k > 0$, then $|n|_p = p^{-k} = \frac{1}{p^k} < 1$. This means that, for any p-adic integer n, the p-adic absolute value of n is less than or equal to 1, i.e. $\forall n \in \mathbb{Z}_p, |n|_p \geq 1$. This implies that the p-adic value of all integers lies on or in the unit ball.

The p-adic absolute value can be extended to the p-adic rationals $\mathbb{Q}_p$ using ν_p . Given $x \in \mathbb{Q}_p$ we can write x as $x = \frac{a}{b}$, where $a, b \in \mathbb{Z}_p$ and $k = \nu_p(a), r = \nu_p(b)$ are the indices of the smallest non-zero digits of a and b.
Then

$$a = ...a_{k+2}a_{k+1}a_k0...0 = \sum_{i=k}^{\infty} a_i p^i = a_k p^k + a_{k+1}p^{k+1} + a_{k+2}p^{k+2} + \cdots = p^k \times (a_k p^0 + a_{k+1}p^1 + a_{k+2}p^2 + \dots) =$$

$$p^k \sum_{i=k}^{\infty} a_i p^{i-k} = p^k \times c,\ c \in \mathbb{Z}_p$$

$$b = ...b_{r+2}b_{r+1}b_r0...0 = \sum_{i=r}^{\infty} b_i p^i = b_r p^r + b_{r+1}p^{r+1} + b_{r+2}p^{r+2} + \cdots = p^r \times (b_r p^0 + b_{r+1}p^1 + b_{r+2}p^2 + \dots) =$$

$$p^r \sum_{i=r}^{\infty} b_i p^{i-r} = p^r \times d,\ d \in \mathbb{Z}_p.$$

We can then write x as:

$$x = \frac{a}{b} = \frac{...a_{k+2}a_{k+1}a_k0...0}{...b_{r+2}b_{r+1}b_r0...0} = \frac{\sum_{i=k}^{\infty} a_i p^i}{\sum_{i=r}^{\infty} b_i p^i} = \frac{p^k \times (a_k p^0 + a_{k+1}p^1 + a_{k+2}p^2 + \dots)}{p^r \times (b_r p^0 + b_{r+1}p^1 + b_{r+2}p^2 + \dots)} = \frac{p^k \times c}{p^r \times d} = p^{k-r}\frac{c}{d}.$$

Since we have factored $b = p^r \times d$ and $a = p^k \times c$ where p^r and p^k are the largest powers of p in b and a, the first digits of d and c, b_r and a_k are guaranteed to be non-zero. This means that both c and d are invertible, i.e. $\exists c^{-1}, d^{-1} \in \mathbb{Z}_p$ s.t. $cc^{-1} = ...0001_p$, and $dd^{-1} = ...0001_p$.
Then we can write $x = p^{k-r}\frac{c}{d} = p^{k-r}cd^{-1}$. Where cd^{-1} is a p-adic integer of absolute value one, i.e. $\nu_p(cd^{-1}) = 0$. Let $m = k - r$. If $m \geq 0$ then $x = p^m cd^{-1}$ is a p-adic integer. However, if $m < 0$, then x is a p-adic rational number, i.e. $x \in \mathbb{Q}_p$, x can be expressed as:

$$x = \sum_{i=m}^{\infty} x_i p^i = ...x_3x_2x_1x_0.x_{-1}x_{-2}\dots x_m = x_m p^m + x_{m+1}p^{m+1} + ... + x_{-1}p^{-1} + x_0p^0 + x_1p^1 + ...$$

If $m < 0$, then we continue the digits of x past a decimal point before terminating on the right at x_m. If m ¿= 0, x has m-1 zero valued digits on the right. Either way, x_m is the rightmost non-zero digit. It's position in relation to the decimal point is m to the left. Multiplying the invertible p-adic integer cd^{-1} by p^m simply shifts all digits leftwards by m (If m is negative they're shifted in the negative left direction, i.e. right of the decimal).

The p-adic valuation and absolute value are defined on $\mathbb{Q}$ similarly to on $\mathbb{Z}_p$:

$$\nu_p(x) = \nu_p(a/b) = \nu_p(a) - \nu_p(b) = k - r = m,$$

$$|x|_p = p^{-\nu_p(n)} = p^{-m}.$$

The primary difference being that m can be negative, therefore $|x|_p = \frac{1}{p^m}$ can be larger than 1.

7 Convergence On p-Adics:

One of the interesting properties of p-adics which follows from the p-adic absolute value $|*|_p$, is that many series which diverge on the reals, converge on the p-adics. For example, take the 2-adic representation of -1 in the previous section. $-1_{10} = \dots 1111_2$. Given this 2-adic representation, we can calculate that

$$-1 = \sum_{i=0}^{\infty} 1 \times 2^i = 1 \times 2^0 + 1 \times 2^1 + 1 \times 2^2 + \dots$$

Since $-1 \in \mathbb{Z}_2 = \dots 111_2$, its p-adic absolute value is $|-1|_2 = 2^{-\nu_p(-1)} = 2^{-(1)} = \frac{1}{2}$. This is a series which diverges on $\mathbb{Z}$ and $\mathbb{R}$ under the standard absolute value, but converges on $\mathbb{Z}_2$ under $|*|_2$.

8 Cardinality of $\mathbb{Z}_p$ and $\mathbb{Q}_p$:

The set of p-adic integers, $\mathbb{Z}_p$, can be thought of as the set of all countably infinite sequences of p-adic digits. Unlike $\mathbb{R}$, p-adic integers are uniquely defined. There are no cases like $1 = .999\ldots$ in the p-adic integers. Therefore, the function $f : \mathbb{Z}_p \longrightarrow (\mathbb{Z}/p\mathbb{Z})^{\mathbb{N}}$ is a bijection:

$$\sum_{k=0}^{\infty} b_k p^k \mapsto (b_0, b_1, b_2, \ldots).$$

Each digit is drawn from the digits between 0 and p-1, i.e. $b_i \in \{0, 1, ..., p-1\}$, so the number of possible choices of sequences $(b_0, b_1, b_2, ...)$ of length $\mathbb{N}$ is $p^{\mathbb{N}}$. Therefore, since $\mathbb{Z}_p$ contains sequences of digits that are countably infinite in length, the p-adic integers, have cardinality $|\mathbb{Z}_p| = p^{|\mathbb{N}|} = 2^{|\mathbb{N}|}$, the cardinality of the continuum, via Cantor's diagonalization argument [4], $2^{|\mathbb{N}|} > |\mathbb{N}|$. Hence, $|\mathbb{R}| = |\mathbb{Z}_p|$. This cardinality makes intuitive sense, as the p-adic integers contain all possible infinite sequences of digits to the left, whereas the reals contain all possible infinite sequences of digits to the right. We can extend this to prove that $|\mathbb{Q}_p| = |\mathbb{Z}_p|$, since $\mathbb{Q}_p = \{\alpha/\beta \mid \alpha, \beta \in \mathbb{Z}_p, \beta \neq 0\}$ i.e. $\mathbb{Q}_p \subset \mathbb{Z}_p \times \mathbb{Z}_p$.

9 Ostrowski's Theorem:

Ostrowski's Theorem is an important theorem about the possible norms that can be defined on the rationals. The theorem states that, every non-trivial norm on the field $\mathbb{Q}$ is equivalent to either the real absolute value function:

$$|x| = \begin{cases} x, & \text{if } x \geq 0 \\ -x, & \text{if } x < 0 \end{cases}$$

or one of the infinitely many p-adic absolute values, $|x|_p = p^{-\nu_p(x)}$. A norm defined on a field is defined to be equivalent to another if they induce the same topology, i.e. they are equivalent up to some power. The important implication of Ostrowski's Theorem, is that since the non-trivial norms on $\mathbb{Q}$ reduce to either the absolute value norm or the p-adic norm, all completions of the rationals are equivalent to either $\mathbb{R}$ or $\mathbb{Q}_p$ for some prime p.

10 Completion of $\mathbb{Q}_p$ Under the p-adic Valuation:

Thus far, we have examined the p-adic integers $\mathbb{Z}_p$ as well as the rationals $\mathbb{Q}_p$ embedded in the p-adics. We have seen via Ostrowski's theorem that every non trivial absolute value on the rationals reduces to either the standard absolute value, or a p-adic absolute value.

The next step is to examine how p-adic absolute value leads to a completion of the rationals with respect to the topology arising from the p-adic valuation. On the standard number system $\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R}$, $\mathbb{R}$ is constructed as the set of limits of all Cauchy sequences of rational numbers $q \in \mathbb{Q}$, which converge under the standard

absolute value $|*|$. This same process of finding the sets of all limits of Cauchy sequences can be done on the p-adic rational numbers using the p-adic absolute value $|*|_p$.

An important distinction between the p-adics and the reals, is that when finding the completion of all convergent Cauchy sequences on $\mathbb{Q}$ under $|*|$, a new field, $\mathbb{R}$ is constructed. But when performing this completion on the p-adic rationals $\mathbb{Q}_p$, $\mathbb{Q}_p$ is found to already be complete under $|*|_p$, i.e. $\mathbb{Q}_p$ is it's own completion under the topology induced by $|*|_p$.

To prepare for this proof, let's briefly examine some definitions [4].
Given a field $\mathbb{F}$ and an absolute value function $|*|$ on $\mathbb{F}$,

i A sequence of elements $(a_i) \in \mathbb{F}$ is called *Cauchy* if $\forall \epsilon > 0, \exists M \in \mathbb{N}, s.t., \forall n, m \geq M$, $|a_n - a_m| < \epsilon$.

ii A field $\mathbb{F}$ is *complete* with respect to $|*|$ if every Cauchy sequence $(a_i) \in \mathbb{F}$ has a limit in $\mathbb{F}$.

iii A subset $S \subset \mathbb{F}$ is *dense* in $\mathbb{F}$ if every open ball around every $a \in \mathbb{F}$ contains an element of S.

The general outline of this proof follows Herwig's text on p-adic completion[4]. To define $\mathbb{Q}_p$, first let $C_p(\mathbb{Q})$ be the set of Cauchy sequences in $\mathbb{Q}$ with respect to the p-adic absolute value $|*|_p$.

$C_p(\mathbb{Q})$ is a ring since $\forall a, b \in C_p(\mathbb{Q}), a = (a_i), b = (b_i),$,

i $(a_i) + (b_i) = (a_i + b_i)$ is also a Cauchy sequence

ii $(a_i) * (b_i) = (a_i * b_i)$ is a Cauchy sequence

therefore $C_p(\mathbb{Q})$ is closed under $(*, +)$.
Additionally, $\mathbb{Q} \subset C_p(\mathbb{Q})$ via the trivial Cauchy sequence $x \in \mathbb{Q}, (x_i) = x, \forall i$.

We then define the maximal ideal

$$\mathbb{I} \subset C_p(\mathbb{Q}), \mathbb{I} = \{(a_n) : a_n \to 0\} = \{(a_n) : \lim_{n\to\infty} |a_n|_p = 0\}$$

of Cauchy sequences that approach zero W.R.T. $|*|_p$.

The field of p-adic numbers is then defined as the quotient of the ring $C_p(\mathbb{Q})$ by its maximal ideal $\mathbb{I}$.

$$\mathbb{Q}_p = C_p(\mathbb{Q})/\mathbb{I}.$$

The purpose of this step in the proof is to specify that Cauchy sequences which converge to the same limit in $\mathbb{Q}_p$ are equivalent.

At this point, we have shown that $\mathbb{Q}_p$ is complete under $|*|_p$. It can additionally be shown that $\mathbb{Q}_p$ follows all of the field axioms. Any number in $\mathbb{Q}_p$ can be expressed in the notation described in the section on p-adic valuation, as a string of digits with a ".", or as a Laurent series sum.

11 Complex *P*-adic Integers:

As shown earlier, positive and negative integers both are naturally included in the p-adic integers. Positive integers in the form $...000d_n....d_1d_0$, i.e. all but finitely many p-adic digits are zero, and negative integers in the form: $...(p-1)(p-1)(p-1)d_n...d_1d_0$, i.e. all but finitely many p-adic digits are $p-1$. The additive inverse of 1 specifically, -1, is $...(p-1)(p-1)(p-1)$ in each p-adic number system. My question is, is there any prime base p in which the imaginary unit, $\sqrt{-1} = i$ can be calculated as the square root of p-adic -1? Such a p-adic integer (Or possibly $i \in \mathbb{Q}_p$?) would have to be of a form such that the polynomial form of -1_p

$$-1 = \sum_{n=0}^{\infty}(p-1)p^n$$

could be decomposed into two equal Taylor Series of the form

$$i = \sum_{n=0}^{\infty} a_n p^n,$$

$$i^2 = (\sum_{n=0}^{\infty} a_n p^n)(\sum_{n=0}^{\infty} a_n p^n) = \sum_{n=0}^{\infty}(p-1)p^n = -1.$$

If we take the above equation $i^2 = -1$ and rearrange it as $i^2 + 1 = 0$. Then we can see that i is the solution to the polynomial equation $x^2 + 1 = 0$ and the question of whether $i \in \mathbb{Z}_p$ can be re-framed as checking for which values of p do $\mathbb{Z}_p$ or $\mathbb{Q}_p$ contain a solution to $x^2 + 1 = 0$.
To answer this question we will need a few different tools [8].

First, since $\forall \alpha, \beta \in \mathbb{Q}_p$, $|\alpha\beta|_p = |\alpha|_p|\beta|_p$ and since $|(-1)(-1)|_p = |1|_p = 1$, then $|-1|_p = |i^2|_p = 1 \rightarrow |i|_p = 1$.

Therefore a solution i to $x^2 + 1 = 0$ is a p-adic integer. Let us denote this p-adic integer as $i = \ldots a_3a_2a_1a_{0_p}$.

Since in any p-adic base, $-1_{10} = ...(p-1)(p-1)(p-1)_p$ we can see that the first p-adic digit of i, a_0 must equal $p-1$ when squared, i.e. $a_0^2 = p-1$. Since a p-adic digit $a_0 \in \{0, 1, ..., (p-1)\} = \mathbb{Z}/p\mathbb{Z}^*$ (the set of possible p-adic digits for $\mathbb{Z}_p$, we can see that this is only possible if $p-1$ is a square, i.e. $p = 1 + b^2$ for some $b \in \mathbb{N}$.

The order of an element $a_0 \in \mathbb{Z}/p\mathbb{Z}^*$ is the smallest n such that $a_0^n \equiv 1(\mod p)$. Since $a_0^2 \equiv -1(\mod p)$ this implies that $a_0^4 \equiv 1(\mod p)$, i.e. a_0 has order 4 in $\mathbb{Z}/p\mathbb{Z}^*$.

Then by Lagrange's theorem, if the subgroup $a_0^n \in \mathbb{Z}/p\mathbb{Z}^*$ has order 4 then 4 must divide $\mathbb{Z}/p\mathbb{Z}^*$ and since $|\mathbb{Z}/p\mathbb{Z}^*| = p-1$, then 4 divides $p-1$.

Finally, $4|(p-1) \implies p \equiv 1(\mod 4)$.

To summarize this proof and its result, a solution to $x^2 + 1 = 0$ must have p-adic

digits $\ldots a_2a_1a_{0_p}$ and $a_0^2 \equiv -1(\mod p)$ necessitates that $p \equiv 1(\mod 4)$.
At his point, we have determined that only primes $p \equiv 1(\mod 4)$ correspond to sets of p-adic integers that could contain a solution to $x^2 + 1 = 0$ and that the first digit of our solution must be $\sqrt{p-1}$. To determine whether a full p-adic solution $i \in \mathbb{Z}_p$ s.t. $i^2 = -1$ exits, we will use a tool called Hensel's Lemma [13]

Hensel's Lemma: Let $f(x) \in \mathbb{Z}_p[x]$ be a polynomial over the p-adic integers and $a_0 \in \mathbb{Z}/p\mathbb{Z}^*$ be a p-adic digit. If $f(a) \equiv 0(\mod p)$ but $f'(a) \not\equiv 0(\mod p)$ then there exists a unique $z \in \mathbb{Z}_p$ such that:

$$f(z) = 0$$
$$z \equiv a_0(\mod p).$$

Now, letting p be a prime such that. $p \equiv 1(\mod 4)$, $f(x) = x^2+1, f'(x) = 2x$ and letting $a_0 = \sqrt{p-1}$. We can see that $(\sqrt{p-1})^2 + 1 = p - 1 + 1 = p \equiv 0(\mod p)$ and $2\sqrt{p-1} \equiv 2(-1)(\mod p) \not\equiv 0(\mod p)$.
Therefore, by Hensel's Lemma, for primes $p \equiv 1(\mod 4)$, there exists a unique solution $i \in \mathbb{Z}_p$ s.t. $i^2 + 1 = 0 \implies i^2 = -1$.

Now that we have proved the existence of $i \in \mathbb{Z}_p$ in some p-adics, let us attempt to actually construct it. Given that a unique solution to $f(x)$ has been proven to exist in $\mathbb{Z}_p$, Hensel's lemma provides a method to determine a Cauchy sequence of p-adic digits to generate it. Given the polynomial $f(x) \in \mathbb{Z}_p[x]$ and the unique solution $(a_n) \in \mathbb{Z}_p$, where $(a_n) = (\ldots a_2a_1a_0)_p = \sum_{n=0}^{\infty} a_n p^n$. The nth p-adic digit of the sequence can be calculated starting with the first digit $a_0 = \sqrt{(p-1)}p^0$ by calculating a Cauchy sequence (β) where $\beta_1 = a_0$ and each additional term $\beta_n = \sum_{i=0}^{n-1} a_i p^i$. The next digit a_n can then be calculating by continuing this Cauchy sequence $\beta_{n+1} = \beta_n + a_n p^n$ and finding the p-adic digit a_n s.t. $f(\beta_{n+1}) = f(\beta_n + a_n p^n) \equiv 0(\mod p^{n+1})$.

We can use this process to calculate $i \in \mathbb{Z}_5$ since 5 is the smallest odd prime that is congruent to 1 mod 4. Let $a_0 = \sqrt{5-1} = 2, \beta_1 = 2$ and note that $f(x) = x^2 + 1$ and $f(\beta_{n+1}) \equiv 0(\mod p^{n+1}) \to (\beta_{n+1})^2 \equiv -1(\mod p^{n+1})$.

We can rewrite the above as as $(\beta_n + a_n p^n)^2 \equiv -1(\mod p^{n+1})$.
Calculating the first few digits of $-1 \in \mathbb{Z}_5$ we get:

$$-1 \equiv (2 \times 5^0)^2(\mod 5)$$
$$-1 \equiv (2 \times 5^0 + 1 \times 5^1)^2(\mod 25)$$
$$-1 \equiv (2 \times 5^0 + 1 \times 5^1 + 2 \times 5^2)^2(\mod 125).$$

I implemented this algorithm as a function in python and calculated the 5-adic value of i to 10 digits as $...3032431212_5$. Calculating the 1st 1000 digits of $i \in \mathbb{Z}_5$ doesn't appear to give any repeating patter of digits, so unfortunately this method of expressing complex numbers isn't computationally useful in the same way that Two's Complement is useful for storing negative integers.

12 Adeles:

Now that the complete field of p-adic numbers is defined, we can use this to begin digging into the ring of Adeles. Learning about the Adeles brought me into some areas of math that are admittedly, pretty far above my head. In this section, I will make note of the aspects I don't fully understand and in what ways I know my understanding to be incomplete. To start, the Adeles are defined as the restricted product of complete local fields. To understand what this means we need to define both Complete Local Fields and the restricted product.

A **Complete Local Field** $\mathbb{K}$ is a field that follows certain properties, depending on whether it is defined W.R.T to a discrete or non-discrete topology[2].

A field $\mathbb{K}$ defined W.R.T a discrete valuation must be both complete with respect to a topology induced by a discrete valuation, and it must have a finite residue field. We have show that the field $\mathbb{Q}_p$ is complete W.R.T to the p-adic valuation $|*|_p$. Additionally, the p-adic valuation is a discrete valuation as it maps each $x \in \mathbb{Q}_p$ to an integer via the p-adic valuation $\nu_p(x) = e, e \in \mathbb{N}$, the number of times the prime factor p occurs in x. The finite residue field condition is somewhat above my head but has one important implication I'll examine shortly in the case of the p-adic adeles.

In the case that $\mathbb{K}$ is defined W.R.T a non-discrete topology, it must be locally compact with respect to the topology that is used to complete it. In the case of the Reals, $\mathbb{R}$ is locally compact W.R.T to the standard absolute value function by the Heine-Borel theorem.

For $\mathbb{K} = \mathbb{Q}$, the adele ring of rational numbers, $\mathbb{A}_\mathbb{Q}$ is the restricted product of every allowed completion of $\mathbb{Q}$; $\mathbb{R}$ as well as the completed p-adic numbers $\mathbb{Q}_p$ for every prime p:

$$\mathbb{A}_\mathbb{Q} = \mathbb{R} \times \prod_{p \in P}{}' \mathbb{Q}_p$$

The restricted product condition comes from the requirement that a complete local field completed W.R.T a discrete topology must have a finite residue field (I think). It implies that any element $a \in \mathbb{A}_\mathbb{Q}$ must have only finitely many non integer entries.

Each element $a \in \mathbb{A}_\mathbb{Q}$ takes the form $a = (a_\infty, a_2, a_3, a_5, ..., a_p, ...)$ where $a_\infty \in \mathbb{R}$ and $a_p \in \mathbb{Q}_p$. i.e. each element of a is drawn from a completion of $\mathbb{Q}$ W.R.T $|*|_p$ or $|*|_\infty$. The notation $|*|_\infty$ denotes the standard absolute value function which completes $\mathbb{Q}$ with $\mathbb{R}$.

13 Adelic Absolute Value:

Now that the Adeles have been defined, we can examine the concept of *Adelic absolute value.* The adelic absolute value or adelic norm, is a function on the ring of Adeles[2]:

Given $\alpha \in \mathbb{A}_\mathbb{Z}, \alpha = (a_\infty, a_2, a_3, ...)$

$$||\alpha|| := |a_\infty|_\infty \prod_p |a_p|_p,$$

where $|*|_\infty$ and $|*|_p$ are the real and p-adic absolute values.

This has the interesting implication that given an element of the Adeles which takes the form: $\alpha = (a, a, a, a, ...), a \in \mathbb{Q}$, i.e. every part of α is a, then $||\alpha|| = 1$, since by the fundamental theorem of arithmetic, $a \in \mathbb{Q}$ can be factorized as a unique product of some set of primes $a = p_1^{e_1} p_2^{e_2} ... p_k^{e_k}$, i.e.
$|a|_\infty = |p_1^{e_1} p_2^{e_2} ... p_k^{e_k}|_\infty = p_1^{e_1} p_2^{e_2} ... p_k^{e_k}$.
Each $|a|_{p_i} = p_i^{-e_i}$ by the definition of p-adic absolute value. So

$$||\alpha|| := |a|_\infty \prod_p |a|_p = p_1^{e_1} p_2^{e_2} ... p_k^{e_k} \prod_p p_i^{-e_i} = p_1^{e_1} p_2^{e_2} ... p_k^{e_k} \times p_1^{-e_1} p_2^{-e_2} ... p_k^{-e_k} = 1,$$

as each prime factor p_i is canceled out since it occurs e_i in both the numerator and divisor.

14 Adelic Products:

One application of Adeles that has shown some value in both physics and mathematics is the *Adelic Product:* The Adelic product is defined for a function $f(x_1, ..., z_n; a_1, ..., a_m), x_i \in \mathbb{Q}, a_i \in \mathbb{C}$

$$f_\infty(x_1, ..., z_n; a_1, ..., a_m) \prod_p f_p(x_1, ..., z_n; a_1, ..., a_m) = C,$$

C constant. Where f_∞, f_p are real or complex valued functions. The Adelic product connects real valued functions to Adelic functions and has seen a few applications in mathematical physics as well as functional analysis [2].

15 Conclusion:

We have examined and worked with both the p-adic integers $\mathbb{Z}_p$ and the field of p-adic numbers $\mathbb{Q}_p$. We've examined how to represent this numbers in various ways and how to perform computations with them. We've also examined some of the ways they are important in number theory, specifically how the various fields of p-adic numbers $\mathbb{Q}_p$ are the only alternative to $\mathbb{R}$ as a completion of the rational numbers.

The various sets of p-adic numbers are a fascinating and non-intuitive subject. I ended up having to learn a lot more than I expected and making many mistakes, in the process of learning about these number systems. The majority of the interesting applications of the p-adics and Adeles in both mathematical physics and analysis are still far above my head. It was also interesting to see the many unexpected places where they show up in computer science.

16 Bibliography

Footnote: Code associated with this paper. Here https://github.com/RyanPersson/p-adics is a link to a repository containing the code I wrote for this paper. There is

both a Mathematica page which performs various computations and visualizations on p-adics, as well as a short python implementation of Hensel's Lemma which calculates the digits of solutions to polynomials in $\mathbb{Z}_p$, given a polynomial function, an initial first digit and a base p.

References

[1] Bhatnagar, Tejasi. "A Baby's Guide toe the p-adic Number System." https://www.thecosmictreehouse.com/post/a-baby-s-guide-to-the-p-adic-number-system

[2] Dragovich, Branko. "ADELES IN MATHEMATICAL PHYSICS". Institute of Physics https://arxiv.org/pdf/0707.3876.pdf

[3] Finley, Thomas. (4, 2000) "Two's Complement." Cornell University. https://www.cs.cornell.edu/~tomf/notes/cps104/twoscomp.html

[4] Herwid, Theodor Christian. "THE P-ADIC COMPLETION OF Q AND HENSEL'S LEMMA" University of Chicago. https://www.math.uchicago.edu/~may/VIGRE/VIGRE2011/REUPapers/Herwig.pdf

[5] Lamb, Evelyn. (2018) "The Numbers Behind a Fields Medalist's Math" Scientific American https://blogs.scientificamerican.com/roots-of-unity/the-numbers-behind-a-fields-medalists-math/

[6] Madore, David A. (12/7/2000) "A First Introduction to p-adic Numbers." http://www.madore.org/~david/math/padics.pdf

[7] Nguyen, Lam. "The p-Adic Numbers." University of Utah. http://www.logetale.com/static/pdf/student_reviews/p-adics.pdf

[8] Petsche, Clayton. (5/31/2022) "E-mail correspondence on p-Adics". MTH 333 FUND CONCEPTS OF TOPOLOGY, Oregon State University.

[9] Ruiter, Joshua. (10/15/2019) "Ostrowski's Theorem and Completion of Fields." Michigan State University. https://users.math.msu.edu/users/ruiterj2/math/Documents/Notes%20and%20talks/Ostrowski's%20Theorem.pdf

[10] Tao, Terry. (8/27/2008) "Tate's proof of the functional equation." terrytao.wordpress. https://terrytao.wordpress.com/2008/07/27/tates-proof-of-the-functional-equation/

[11] Turnquist, Axel G. R. "P-ADIC NUMBERS AND SOLVING P-ADIC EQUATIONS." University of Washington. https://sites.math.washington.edu/~morrow/336_12/papers/axel.pdf

[12] Weisstein, Eric W. "p-adic Norm." From MathWorld–A Wolfram Web Resource. https://mathworld.wolfram.com/p-adicNorm.html

[13] Zheng, Yiduan. "p-ADIC NUMBERS, $\mathbb{Q}_p$, AND HENSEL'S LEMMA". University of Chicago. http://math.uchicago.edu/~may/REU2020/REUPapers/Zheng,Yiduan.pdf