Contents

Abstract

Throughout human civilisation, mathematicians have sought to expand the natural numbers into new, unexplored territories. From the introduction of 0 to the discovery of irrationals, we have today a number system $\mathbb{C}$ which can not only express continuous quantities, but also guarantees once unimaginable solutions to vast arrays of equations. But is there another way to get here? Can we rebuild such a versatile yet robust number system from completely different foundations? In this report, we introduce the p-adic number system. From humble beginnings in the p-adic integers, we draw upon techniques in analysis, number theory and field theory to create increasingly powerful and interesting systems. At first glance, things may seem unintuitive. Incrementing numbers does not make them larger. Infinity is closer to zero than infinite strings of digits. So what can we learn from this world of unusual yet truly fascinating properties which seem to have no place in our universe? To find out, let us embark on a great adventure to construct something truly magical, something which inspires awe and wonder in adventurers all over the world, something of which mathematicians once could have only dreamed : $\mathbb{C}_p$.

1 Introduction

We begin with a purely algebraic definition of the p-adic integers $\mathbb{Z}_p$ as integer sequences, and identify p-adic analogues to elements of $\mathbb{Z}$. Then we introduce the p-adic norm. An advantage of this algebraic perspective is that the ring $\mathbb{Z}_p$ is initially independent of the p-adic valuation. After this, we shift to a more analytic perspective by directly defining $\mathbb{Q}_p$ as a completion of $\mathbb{Q}$ under the p-adic norm. We do this to highlight the analagous nature of $\mathbb{R}$, the completion of $\mathbb{Q}$ under the euclidean norm, to $\mathbb{Q}_p$. In fact, we find that $\mathbb{Q}_p$ is a subfield of $\mathbb{R}$ - we take advantage of this by introducing a more convenient and familiar notation for the p-adic numbers by writing each p-adic element as its analogous number in $\mathbb{R}$.

Here, we take a break in constructing fields by introducing perhaps the most important and fundamental result regarding the p-adics - Hensel's lemma. This lemma allows us to prove the existence of solutions in $\mathbb{Q}_p$ by finding solutions in $\mathbb{Z}$ mod p. Using this powerful tool, we create a way to easily visualise how p-adic numbers interact, explicitly constructing the sequences we will have discussed throughout the report. This gives a comfortable transition into finite field extensions of $\mathbb{Q}_p$, which heavily takes advantage of results derived from Hensel's lemma. Here, our primary goal will be to extend the p-adic norm to arbitrary field extensions, hopefully allowing us to create a strong foundation for the algebraic closure of $\mathbb{Q}_p$, that is $\overline{\mathbb{Q}_p}$. From here, we can once again take the completion of $\overline{\mathbb{Q}_p}$ to construct $\mathbb{C}_p$, which is the primary focus of the report. Indeed, the p-adic norm extends to $\mathbb{C}_p$ in the usual way we know from analysis.

The remainder of the report will focus on exploring familiar functions in $\mathbb{C}_p$ by viewing them as series expansions. We will discover some of the unconventional properties regarding convergence, and in particular, explore how log and exp behave differently in the complex p-adics.

2 P-adic Completion of Integers - $\mathbb{Z}_p$

First, we introduce the p-adic integers from the algebraic perspective. Though it is worthwhile to keep this foundation in mind, we will be using a more analytic definition from section 3 onwards as it is more intuitive to work with.

Definition 2.1. *The positive p-adic integers $\mathbb{Z}_p$ are sequences*

$$\{(x_i)_{i\in\mathbb{N}} : x_i \in \mathbb{Z}/p^i\mathbb{Z}\}$$

equipped with the set of projective maps, $\pi_n^m : \mathbb{Z}/p^m\mathbb{Z} \to \mathbb{Z}/p^n\mathbb{Z}$ for $m \geq n$ (defined by sending $x \in \mathbb{Z}/p^m\mathbb{Z}$ to x modulo n). Let $\pi_n^m(x_m) = x_n$ for each $m \geq n$.

We can see that the positive p-adic integers are a subset of $\{(x_i)_{i\in\mathbb{N}} : x_i \in \mathbb{Z}/p^i\mathbb{Z}\}$. In fact, if we define addition and multiplication pointwise, they form a subring. At first glance, it may seem that this construction of $\mathbb{Z}_p$ has very little to do with $\mathbb{Z}$. But upon some investigation, it is easy to see that

Theorem 2.1. *$\mathbb{Z}$ is isomorphic to the set of stable sequences in $\mathbb{Z}_p$.*

Proof. Consider $x \in \mathbb{Z}$. Since the representation of x in base p is unique, we can uniquely write

$$x = x_1 + x_2p + x_3p^2 + x_4p^3 + ... + x_{n+1}p^n$$

with $0 \leq x_i < p^{i-1}$. Then in $\mathbb{Z}_p$, x is equivalent to a sequence (y_i) with $y_{n+1} = x_{n+1}$. So from the definition of the projective maps, it follows that

$$(y_i) = x_1(1,1,1,...)+x_2(0,1,1,...)+x_3(0,0,1,...)+...+x_{n+1}(0,0...,0,1,1,...)$$

which is constant after the n^{th} coordinate. So each element in $\mathbb{Z}$ corresponds to one and only one stable sequence in $\mathbb{Z}_p$. □

By convention, we can represent stable elements of $\mathbb{Z}_p$ by their corresponding element in $\mathbb{Z}$. Divergent elements of $\mathbb{Z}_p$ can be represented by infinite strings of digits in base p. For example, in $\mathbb{Z}_5$ we can write $(4, 24, 124, 624, ...)$ as 4444.... or ....4444. It will soon be apparent that the latter representation is much more useful for our purposes.

Definition 2.2. *Define the valuation $\nu(x_i)_{i\in\mathbb{N}} = k$, where k is the largest integer such that $x_k = 0$, or 0 if no such integer exists. Then the p-adic norm $|x|_p = 1/p^{\nu(x)}$ and set $|(0,0,...)|_p = 0$.*

Theorem 2.2. *$|.|_p$ is non-archimedean, that is, $|x+y|_p \leq \max(|x|_p, |y|_p)$.*

Proof. If $|x|_p \neq |y|_p$, then let $\nu(x) = b$ and $\nu(y) = a$ with $b > a$. Then $\nu(x+y) = a$ since the addition of x to y does not affect the first $a+1$ coordinates of y. Hence $|x+y|_p = |y|_p \leq \max(|x|_p, |y|_p)$.

If $|x|_p = |y|_p$, then let $\nu(x) = \nu(y) = a$. Then $\nu(x+y) \geq a$ since the first a coordinates of $x+y$ will still be 0. Hence $|x+y|_p \leq \max(|x|_p, |y|_p)$. □

Theorem 2.3. *$\mathbb{Z}$ under the p-adic norm is not complete for all prime p.*

Proof. For instance, take the p-adic sequence $x = (1, 1+p, 1+p+p^2, ...)$. Now, since $(p, p^2, p^3, ...)$ converges to 0, we have

$$\begin{aligned}\lim_{n\to\infty}(p-1)\sum_{i=0}^{n} p^i &= \lim_{n\to\infty} p^n - 1 \\ &= \lim_{n\to\infty} -1 \\ &= -1\end{aligned}$$

And it follows that we actually have $x = 1/(1-p) \notin \mathbb{Z}$ but $1/(1-p) \in \mathbb{Z}_p$. □

The p-adic number system reveals a different way to think about magnitude. Though it is outside the scope of this report, one can prove that there are only 3 possible ways to define the size of integers such that the norm axioms are satisfied: the trivial norm which sets the size of all non-zero integers to a constant, the euclidean norm which we all know and love, and the p-adic norm.

Under this new notion of magnitude, the "size" of integers converges towards 0 as powers of p in their prime factorisations increase. One immediate consequence of this is that infinite strings of digits are no longer arbitrarily large (nor small for that matter). For example, in $\mathbb{Z}_2$, $|...01010|_p = 1/2$ and $|...11001100|_p = 1/4$. It is now also apparent that the leading digits of numbers are no longer the most significant. In $\mathbb{Z}_3$, a number with last digit 2, for example 122110202, will always have size 1 regardless of the digits preceding 2. There is also no clear way to increment numbers such that they gradually increase in magnitude. Every value of the p-adic norm has infinite numbers. We will be discovering many more interesting properties which arise from this redefinition of magnitude.

3 Field of Fractions - $\mathbb{Q}_p$

From here, we could define $\mathbb{Q}_p$ by taking the field of fractions of $\mathbb{Z}_p$. However, it is not clear that $\mathbb{Q}_p$ should actually be complete. We will proceed with a more intuitive construction of the p-adic rationals by taking a completion of $\mathbb{Q}$ directly. But before this, we should extend the definition of the p-adic valuation to $\mathbb{Q}$, so that we can clarify the definition of the p-adic norm in this new perspective.

Definition 3.1. *For prime p, let $q = p^k \frac{a}{b} \in \mathbb{Q}$, with $k, a, b \in \mathbb{Z}$ and a, b, p coprime. Then define $\nu_p(q) = k$.*

We know from elementary number theory that the representation of q as $p^k \frac{a}{b}$ is unique. Indeed, from this definition we can extend the p-adic norm by setting $|q|_p = 1/p^{-k}$. We know that ν_p and ν from Definition 2.2 are identical over the integers, so our reformulation of the p-adic norm is consistent with our existing definition. This fact is obvious if we represent stable sequences in $\mathbb{Z}_p$ as their corresponding integer.

Now we can demonstrate the incompleteness of $\mathbb{Q}$ under the p-adic norm. But first, let us introduce an important result which will be explored and applied in greater detail in chapter 4.

Lemma 3.1. *Let $P(x)$ be a polynomial with coefficients in $\mathbb{Q}$. If $P(\alpha_n) \equiv 0 \mod p^n$ for some $n \in \mathbb{Z}$ and $P'(\alpha_n) \not\equiv 0 \mod p$, then there exists $\alpha_{n+1} \in \mathbb{Q}$ such that $\alpha_n \equiv \alpha_{n+1} \mod p^n$ and $P(\alpha_{n+1}) = 0 \mod p^{n+1}$.*

Proof. Suppose $P(\alpha_n) \equiv 0 \mod p$ with $P'(\alpha_n) \not\equiv 0 \mod p$. Then if $P(\alpha_n) \equiv 0 \mod p^n$, we want to find k such that

$$P(\alpha_{n+1}) := P(\alpha_n + kp^n) \equiv 0 \mod p^{n+1}$$

So representing $P(\alpha_n + kp^n)$ as a power series in terms of kp^n,

$$\begin{aligned} \sum_{i=0}^{\infty} \frac{P^{(i)}(\alpha_n)}{i!}(kp^n)^k &\equiv 0 \mod p^{n+1} \\ P(\alpha_n) + P'(\alpha_n)kp^n &\equiv 0 \mod p^{n+1} \\ q + P'(\alpha_n)k &\equiv 0 \mod p^n \\ k &\equiv \frac{-q}{P'(\alpha_n)} \mod p^n \end{aligned}$$

Indeed, with this choice of k, α_{n+1} satisfies $P(\alpha_{n+1}) \equiv 0 \mod p^{n+1}$ and $\alpha_{n+1} \equiv \alpha_n \mod p^n$. □

This is Hensel's lemma, which, for our purposes in this chapter, is useful in constructing p-adic sequences in $\mathbb{Q}$ which "get increasingly close" to polynomial solutions (this is why we used seemingly arbitrary indicies on our variables!). Indeed, by considering polynomials with no solution in $\mathbb{Q}$, we can construct non-convergent Cauchy sequences. This gives us the following result.

Theorem 3.2. *$\mathbb{Q}$ is not complete under the p-adic norm for all prime p.*

Proof. We will first consider the case where $p \neq 2$. Let

$$a = \begin{cases} 1+p \text{ if } 1+p \text{ is non-square} \\ 1+2p \text{ if } 1+p \text{ is square} \end{cases}$$

Then a is a non-square quadratic residue mod p. Now, let x_1 be a solution to $x^2 - a \equiv 0 \mod p$. By Hensel's lemma, $x^2 - a \equiv 0 \mod p^2$ must also have a solution x_2 where $x_2 \equiv x_1 \mod p$. In general, given a solution x_n to $x^2 - a \equiv 0 \mod p^n$, we can find a solution x_{n+1} to $x^2 - a \equiv 0 \mod p^{n+1}$ with $x_n \equiv x_{n+1} \mod p^n$.

So we can inductively define a sequence $(x_n)_{n\in\mathbb{N}}$ such that $x_n \equiv a \mod p^n$ and $x_{n+1} \equiv x_n \mod p^n$ (so $x_{n+1} - x_n$ is a multiple of p^n). Indeed, this is Cauchy since for $m \geq n \geq N$, we have

$$|x_m - x_n| \leq \max(|x_m - x_{m-1}|, ..., |x_{n+1} - x_n|) = |x_{k+1} - x_k| \leq p^{-k} \leq p^{-N} \to 0$$

for some $n \leq k \leq m$. But by Hensel's lemma, the limit of this sequence must be a solution to $x^2 - a = 0$, which is a contradiction since no such number exists in $\mathbb{Q}$.

For the case $p = 2$, we have that $x_1 := 1$ is a solution to $x^3 - 3 \mod 2$. By a similar construction to above, we can create a Cauchy sequence $(x_n)_{n\in\mathbb{N}}$ where $x_n \equiv x_{n+1} \mod 2^n$, which, if convergent, must have a limit which is a solution in $\mathbb{Q}$ to $x^3 - 3$ (the first few numbers in this sequence are $(1, 3, 3, 11, 27, ...)$). This similarly yields a contradiction to the statement that $\mathbb{Q}$ is complete since no such solution exists in $\mathbb{Q}$. □

We remark that the proof for $p \neq 2$ does not work in the case $p = 2$ because given the initial quadratic solution $x_1 = 1$, we have $\frac{d}{dx}(x^2 - x_1) \equiv 0 \mod 2$, which violates a condition of Hensel's lemma.

As a concrete example, in $\mathbb{Q}_3$, $(1, 4, 13, 13, 175, ...)$ is such a sequence which

satisfies the above construction. The fact that $\mathbb{Q}$ is incomplete under the p-adic norm should come as no surprise - the construction given above is analagous to constructing a Cauchy sequence in $\mathbb{Q}$ under the euclidean norm which approaches an irrational number. Here, we invoke the power of Hensel's lemma to let us construct increasingly close approximations.

Definition 3.2. *Define $\mathbb{Q}_p$ to be C/N, where C is the set of Cauchy sequences in $\mathbb{Q}$ under the p-adic norm, and N is the set of null sequences.*

To identify an element of $\mathbb{Q}$ in $\mathbb{Q}_p$, we can apply the map $x \mapsto \overline{(x, x, x, ...)}$. Indeed, this is injective since for $x \neq y$, we have $\overline{(x, x, x, ...)} - \overline{(y, y, y, ...)} = \overline{(x - y, x - y, x - y, ...)} \notin N$. Since the values of the p-adic norm are discrete, any non-null sequence $(x_n) \in C$ must be eventually stationary. And for $\overline{(x_n)} \in \mathbb{Q}_p$,

$$\lim_{n\to\infty} |x_n| \to p^k$$

for some $k \in \mathbb{Z}$.

Definition 3.3. *For $\overline{(x_n)} \in \mathbb{Q}_p$, let $|\overline{(x_n)}| = \lim_{n\to\infty} |x_n|$.*

Note that eventually, for non-zero sequences, $|x_n| = \lim_{n\to\infty} |x_n|$. Also, this norm is well defined since any sequences in the equivalence class of (x_n) differ by a sequence which is eventually null, so they either will eventually be stationary at the same point, or are both null sequences.

As an example, consider the sequence $\overline{(x_n)} = \overline{(1, 4, 13, 13, 175, ...)}$. Clearly, since by construction $x_i \neq 0 \mod p$ for all $i \in \mathbb{N}$, we have that $\overline{(x_n)} = 1$.

Theorem 3.3. *$\{\overline{(x)} : x \in \mathbb{Q}\}$ is dense in $\mathbb{Q}_p$. In other words, $\mathbb{Q}$ is dense in $\mathbb{Q}_p$.*

Proof. Let $\varepsilon > 0$. For any non-null $\overline{(x_n)} \in \mathbb{Q}_p$, there exists some K after which
$(x_n - x_K)_{n\in\mathbb{N}}$ is stationary and terms in $(x_n)_{n\in\mathbb{N}}$ differ by no more than ε. Then for all $n \geq K$,

$$|x_n - x_K| := r < \varepsilon$$

So $|\overline{(x_n - x_K)_{n\in\mathbb{N}}}| = \lim_{n\to\infty} |x_n - x_K| = r < \varepsilon$ by definition of the p-adic norm. Thus for any arbitrary neighbourhood of $\overline{(x_n)}$, there exists a K such that $(x_K) \in \mathbb{Q}$ can be found in it. For null $\overline{(x_n)} \in \mathbb{Q}_p$, we can find (0) in any neighbourhood around $\overline{(x_n)}$. □

This proof is more concise than the one given in Goueva's textbook, as it uses the property that non-null Cauchy sequences are eventually stationary under the p-adic norm.

Theorem 3.4. *$\mathbb{Q}_p$ is a field.*

Proof. We will show that non-zero elements have multiplicative inverses. For $\overline{(x_n)} \notin N$, we can define (y_n) such that

$$y_i = \begin{cases} x_i \text{ if } x_i \neq 0 \\ 1 \text{ if } x_i = 0 \end{cases}$$

. Then $(1/y_n)$ is well defined. Since (x_n) is not null, we must have $x_i = y_i$ (so $x_i - y_i = 0$) for all $i > k$ for some k. So since $(x_n - y_n) = (x_n) - (y_n) \in N$, we have $(x_n) \in \overline{(y_n)}$. Then $(x_n)(1/y_n) \in \overline{(1)}$. □

This result enables us to talk about field extensions of $\mathbb{Q}_p$ by adjoining solutions to polynomials. Since a primary goal of this report is to construct a field with the property of algebraic closure, the fact that $\mathbb{Q}_p$ is already a field is particularly important (and convenient) since we can directly take the algebraic closure of $\mathbb{Q}_p$ and work from there.

4 Hensel's Lemma and Applications

In this section, we will take a break from field construction and exhibit the potential of Hensel's Lemma, introducing a way to compute p-adic sequences and find concrete solutions to p-adic polynomials. This will hopefully enhance the reader's intuition in exploring this unfamiliar number system.

4.1 Hensel's Lemma

We have used Hensel's lemma as a tool to approximate solutions to polynomials using rational sequences. This allowed us to demonstrate the incompleteness of $\mathbb{Q}$. However, a much more powerful consequence of Hensel's lemma is that it enables us to immediately extrapolate solutions to polynomials in $\mathbb{Q}_p$ from solutions in $\mathbb{Q}$ mod p. This gives us a famous theorem derived from Hensel's lemma, which is arguably more significant in the study of p-adics than Hensel's lemma itself.

Lemma 4.1. *Let $P(x)$ be a polynomial with coefficients in $\mathbb{Q}_p$. If $P(\alpha_1) \equiv 0 \mod p$ and $P'(\alpha_1) \not\equiv 0 \mod p$, then there exists $\alpha \in \mathbb{Q}_p$ such that $\alpha \equiv \alpha_1 \mod p$ and $P(\alpha) = 0$.*

Proof. Suppose $P(\alpha_1) \equiv 0 \mod p$ with $P'(\alpha_1) \not\equiv 0 \mod p$. Then if $P(\alpha_n) \equiv 0 \mod p^n$, from Hensel's lemma we can find α_{n+1} satisfying $P(\alpha_{n+1}) \equiv 0 \mod p^{n+1}$ and $\alpha_{n+1} \equiv \alpha_n \mod p^n$. Then by induction, we can choose a sequence $\alpha_1, \alpha_2, ...$ satisfying the above relations. This sequence is Cauchy (by a similar proof to the one used for Theorem 3.2), so it has some limit α such that $P(\alpha) = 0$ (by continuity) and $P(\alpha) \equiv \alpha_1 \mod p$. □

For example, we directly observe that since $x^2 - 7 \equiv 0 \mod 3$, we must have $\sqrt{7} \in \mathbb{Q}_3$. In fact, if a is a quadratic residue mod p, then by Hensel's lemma $x^2 - a = 0$ must have a solution in $\mathbb{Q}_p$. However, as powerful as Hensel's lemma is, polynomial solutions in $\mathbb{Q}_p$ are still predicated on finding solutions in $\mathbb{Q}$ mod p. As a consequence, many polynomials with solutions in $\mathbb{R}$ do not have solutions in $\mathbb{Q}_p$. For example, we can say that since $x^3 - 1/4$ has no solutions mod 7, the cube root of $1/4$ does not exist in $\mathbb{Q}_7$.

Theorem 4.2. *For any prime p and positive integer m such that $p \nmid m$, there exists a primitive m-th root of unity in $\mathbb{Q}_p$ iff $m|p-1$.*

Proof. By Fermat's little theorem, we have that for any $a \in \mathbb{Z}_p$, $a^{p-1} \equiv 1 \mod p$. If m divides $p-1$, then $(a^{(p-1)/m})^m \equiv 1 \mod p$, so there exists a solution to the polynomial $x^m - 1 \equiv 0 \mod p$. Then by Hensel's lemma, $\sqrt[m]{x} \in \mathbb{Z}_p \subset \mathbb{Q}_p$.

Conversely, if there exists $a \in \mathbb{Q}_p$ such that a is a primitive root of unity, then $a^m \equiv 1 \mod p$. But if $m \nmid p-1$, then there exists a solution to $rm + s(p-1) = gcd(m, p-1) < m$. But this implies that $a^{gcd(m,p-1)} \equiv 1 \mod p$, which is a contradiction since then $a^{gcd(m,p-1)} = 1$ has a solution in $\mathbb{Q}_p$ with $gcd(m, p-1) < m$, thus a is not a primitive $m-th$ root of unity. □

For instance, consider $p = 7$ and $m = 3$. Theorem 2.2 states that there must exist a primitive cube root of unity. Indeed, $2^3 \equiv 1 \mod 7$, so using Hensel's lemma we find that the sequence $(2, 30, 324, 1353, ...)$ converges to the primitive cube root of 3 in $\mathbb{Q}_7$.

Theorem 4.3. *The $p-1$-th roots of unity in $\mathbb{Q}_p$ form a cyclic group.*

Proof. For each $a \in \mathbb{Z}_p/p\mathbb{Z}_p$ with $a \not\equiv 0 \mod p$, we have that $a^{p-1} \equiv 1 \mod p$. This gives us $p-1$ distinct $p-1$-th roots of unity in $\mathbb{Q}_p$ by Hensel's lemma. We verify that

$$1 = 1^{p-1} \in \mathbb{Q}_p$$

$$a^{p-1} = 1 \Rightarrow a^{1-p} = 1$$

$$a^{p-1} = 1 \text{ and } b^{p-1} = 1 \Rightarrow (ab)^{p-1} = 1$$

So the $p-1$-th roots of unity in $\mathbb{Q}_p$ form a cyclic subgroup of the multiplicative group $\mathbb{Q}_p$. □

We will conclude this subsection by leaving the reader with the intuition that just as $\mathbb{R}$ can be viewed as a "union" of all the $\mathbb{Q}_p$, so too can $\mathbb{Q}$ be viewed as an "intersection" of all the $\mathbb{Q}_p$. This general idea is called the local-global principle, and has various applications in algebraic number theory. Although this insight is important for developing intuition, its applications are not a focus of this report, so we will only discuss it superficially.

Theorem 4.4. *$x \in \mathbb{Q}$ is a nonnegative square iff it is a square in $\mathbb{Q}_p$ for every prime p.*

Proof. Since $\mathbb{Q} \subseteq \mathbb{Q}_p$, it is clear that if $x = a^2 \in \mathbb{Q}$ is a square, then $x = a^2 \in \mathbb{Q}_p$ is also a square. Conversely, if x is a square in $\mathbb{Q}_p$ for every p, then $x = a^2$ for some $a \in \mathbb{Q}_p$. Hence $\nu_p(x) = 2\nu_p(a)$, so $\nu_p(x)$ is even for all primes p. Hence we can write $x = \prod_i^{\infty}(p_i)^{2n}$ with $n \in \mathbb{Z}$, so x is a square in $\mathbb{Q}$. □

Corollary 4.4.1. *For $n \geq 1$, $x = (a_1)^2 + ... + (a_n)^2 \in \mathbb{Q}$ iff $x = (a_1)^2 + ... + (a_n)^2 \in \mathbb{Q}_p$ for any p.*

Proof. Suppose x is the sum of squares in $\mathbb{Q}_p$ for all p. So let $x = x_1 + ... + x_n$, where x_i is square in $\mathbb{Q}_p$ for all i and all p. Then x_i is also square in $\mathbb{Q}$ for all i, so x is also the sum of squares in $\mathbb{Q}$. The converse is the similar. □

4.2 Constructing the Sequences

So far, we have developed an abstract intuition of what it means to complete $\mathbb{Q}$ under the p-adic norm. But what do these "new" numbers look like? As an example, let us construct the primitive 4^{th} root of unity ζ_4 in $\mathbb{Q}_5$ using Hensel's lemma.

We will construct the sequence $(x_1, x_2, ...) \in \mathbb{Q}_5$ corresponding to ζ_4. First, we note that $2^4 \equiv 1 \mod 5$. Hensel's lemma guarantees the existence of x_2, where $x_2 \equiv x_1 \mod 5$ and $(x_2)^4 - 1 \equiv 0 \mod 25$. There are 5 numbers mod 25 which satisfy the first condition, namely $2, 7, 12, 17$ and 22. We check that $2^4 \not\equiv 1 \mod 25$, but $7^4 \equiv 1 \mod 25$, so $x_2 = 7$. Again, there are 5 numbers which satisfy $x_3 \equiv x_2 \mod 25$, namely $7, 32, 57, 82$ and 107. We can similarly confirm that $x_3 = 57$ since $57^4 \equiv 1 \mod 125$.

This algorithm is clearly tedious and rather unenlightening. As mathematicians, we can automate this process using a simple Python script (given in the appendix).

By calling `lift(2,5,lambda x:x**4-1,10)`, we obtain as the following sequence as output:

$$(2, 7, 57, 182, 2057, 14557, 45807, 280182, 280182, 6139557, 25670807, ...)$$

In base 5, this is

$$(2, 12, 212, 1212, 31212, 431212, 2431212, 32431212, 32431212, 3032431212, ...)$$

We note that a number $a_1...a_n$ represented in base k is essentially of the form $k^0a_n + k^1a_{n-1} + k^2a_{n-1} + ...$, which is a more convenient form to interpret p-adic numbers.

Using this, we can directly compute $\zeta_2 = (\zeta_4)^2 = -1$ as a sequence in $\mathbb{Q}_5$. By squaring each number in the sequence representing ζ_4, we obtain that

$$-1 = (4, 144, 100444, 2024444, 2040344444, 413221444444, 13244124444444, ...).$$

In other words, $-1 = \lim_{n\to\infty} 5^n - 1$. Indeed, we verify that $|\lim_{n\to\infty} 5^n| = \lim_{n\to\infty} \frac{1}{p^n} = 0$.

Let us try a less trivial example. Theorem 3.2 guarantees the existence of ζ_7 in $\mathbb{Q}_{29}$. Using our algorithm, we obtain in base 29 (with A,B,C,... representing $10, 11, 12, ...$), by lifting the solution $7^7 - 1 \equiv 0 \mod 29$,

$$\zeta_7 = (7, M7, 5M7, 35M7, 335M7, A335M7, LA335M7, 7LA335M7, ...)$$

Another 7th root ζ_7' can be obtained by lifting $20^7 - 1 \equiv 0 \mod 29$:

$$\zeta_7' = (K, JK, DJK, KDJK, 5KDJK, J5KDJK, J5KDJK, 70J5KDJK, ...)$$

By theorem 3.2, we can generate all the $7th$ roots with ζ_7. Indeed, we observe that $(\zeta_7)^2 = \zeta_7'$.

5 Finite Field Extensions - $\mathbb{Q}_p[\alpha]$

Now, we have the tools to begin exploring finite extensions of $\mathbb{Q}_p$. Instead of delving into general field theoretic results, this section will be devoted to analysing some of the interesting properties which are unique to finite extensions of $\mathbb{Q}_p$. Then we will focus on extending the p-adic norm to extensions of $\mathbb{Q}_p$. Beyond this, much of our knowledge about the structure of $\mathbb{Q}_p[\alpha]$ comes from field theory and Galois theory, which, while very important, will not be the main focus of this report.

5.1 Extending $\mathbb{Q}_p$

First, let us begin by exploring the finite field extensions of $\mathbb{Q}_p$.

Theorem 5.1. *For all $n \in \mathbb{N}$ with $n > 1$, $\sqrt[n]{p} \notin \mathbb{Q}_p$.*

Proof. If there exists $x \in \mathbb{Q}_p$ such that $x^n = p$, then $x^n \equiv p \equiv 0 \mod p$. But using Hensel's lemma, this clearly lifts to a solution $x = 0$, which is a contradiction since $p \neq 0$. □

Now, recalling the Lengdre symbol $\left(\frac{a}{p}\right) = \begin{cases} 0 \text{ if } a = 0 \\ 1 \text{ if } a \neq 0 \text{ is a square residue mod } p \\ -1 \text{ otherwise} \end{cases}$:

Corollary 5.1.1. *For $a \in \mathbb{Q}$, we have $\sqrt{a} \in \mathbb{Q}_p$ iff $\left(\frac{a}{p}\right) = 1$.*

Proof. We already know that $\sqrt{a} \notin \mathbb{Q}_p$ if $\left(\frac{a}{p}\right) = -1$ and $\sqrt{a} \in \mathbb{Q}_p$ if $\left(\frac{a}{p}\right) = 1$. From the above theorem, we have that $\sqrt{a} \notin \mathbb{Q}_p$ if $\left(\frac{a}{p}\right) = 0$. □

To start with a simple example, consider the roots of $x^2 - x - 1$ in $\mathbb{Q}_3$ and $\mathbb{Q}_5$. We have that $\sqrt{5} \in \mathbb{Q}_3$ since $\left(\frac{3}{5}\right) = 1$, but $\sqrt{5} \notin \mathbb{Q}_5$. The roots of $x^2 - x - 1$ are $\frac{1 \pm \sqrt{5}}{2}$, so it has 2 roots in $\mathbb{Q}_3$ and no roots in $\mathbb{Q}_5$, however we can construct a minimal quadratic extension $\mathbb{Q}_5[\sqrt{5}]$ to incorporate the roots of $x^2 - x - 1$. So this raises the question: since there are infinitely many non-solutions to $x^2 \equiv a \mod 5$, does this mean there are infinitely many quadratic extensions of $\mathbb{Q}_5$? This assumption turns out to be incorrect:

Theorem 5.2. *For $p \geq 3$, there are exactly 3 quadratic extensions of $\mathbb{Q}_p$.*

Proof. I claim that $\mathbb{Q}_p[\sqrt{a}], \mathbb{Q}_p[\sqrt{p}]$ and $\mathbb{Q}_p[\sqrt{ap}]$, where a is a non-residue mod p (existence of a guaranteed by $p \geq 2$), are precisely the 3 quadratic extensions. First, recall that $\sqrt{a}, \sqrt{p} \notin \mathbb{Q}_p$, so they form a non-trivial field extension.

For non-residues a, b, we have that

$$x + y\sqrt{a} \in \mathbb{Q}_p[\sqrt{a}] = x + \frac{y\sqrt{a}}{\sqrt{b}}\sqrt{b}$$

with $x, y \in \mathbb{Q}_p$. Indeed, if $b^{-1} \equiv x^2 \mod p$, then $b \equiv x^{-2} \mod p$, so contrapositively, if b is a non-residue, b^{-1} is also a non-residue. And

$$\left(\frac{ab^{-1}}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b^{-1}}{p}\right) = (-1)^2 = 1,$$

so we have $\frac{y\sqrt{a}}{\sqrt{b}} \in \mathbb{Q}_p$. Hence $\mathbb{Q}_p[\sqrt{a}] \subseteq \mathbb{Q}_p[\sqrt{b}]$, so symmetrically,

$$\mathbb{Q}_p[\sqrt{a}] = \mathbb{Q}_p[\sqrt{b}]$$

thus our choice of a does not matter.

Now, consider arbitrary field extension $K = \mathbb{Q}_p[\sqrt{p^n a}]$. If a is a quadratic residue, then $K = \mathbb{Q}_p[\sqrt{p^n}]$, so n must be odd and we have $K = \mathbb{Q}_p[\sqrt{p}]$. If a is a quadratic non-residue, then if n is even we have $K = \mathbb{Q}_p[\sqrt{a}]$, and if n is odd we have $K = \mathbb{Q}_p[\sqrt{pa}]$. But since we showed that the choice of a does not matter, these are the only 3 quadratic extensions. □

It follows that the only quadratic extensions of $\mathbb{Q}_3$ are $\mathbb{Q}_3[\sqrt{2}]$, $\mathbb{Q}_3[\sqrt{3}]$ and $\mathbb{Q}_3[\sqrt{6}]$. It follows that any root of the polynomial $x^2 + bx + c$ can be written in the form $x + y\sqrt{2}$, $x + y\sqrt{3}$ or $x + y\sqrt{6}$, where $x, y \in \mathbb{Q}_3$.

For example, the roots of $x^2 - 5x + 3$ are

$$\frac{5 \pm \sqrt{13}}{2} = \frac{5}{2} \pm \frac{\sqrt{13}}{2\sqrt{2}}\sqrt{2}$$

with $\frac{\sqrt{13}}{2\sqrt{2}} \in \mathbb{Q}_3$.

As a special case, we can study the cubic extensions of $\mathbb{Q}_3$. Since $1^3 \equiv 1 \mod 3$ and $2^3 \equiv 2 \mod 3$, we have $\sqrt[3]{2}, \sqrt[3]{1} \in \mathbb{Q}_3$. So any non-trivial cubic

extension must be of the form $\mathbb{Q}_3[\sqrt[3]{3^k}]$. And since $\mathbb{Q}_3[\sqrt[3]{3}]$ is equivalent to $\mathbb{Q}_3[\sqrt[3]{9}]$, this gives us the single cubic extension $\mathbb{Q}_3[\sqrt[3]{3}]$.

5.2 Extending $|.|_p$

Whenever we add elements to our p-adic algebraic structure, we must also extend the definition of the p-adic norm so that we can create an appropriate metric on our new set. We did this when we extended the definition of the p-adic norm from $\mathbb{Z}_p$ to $\mathbb{Q}_p$. Here, we have the more complicated task of extending the p-adic norm $|.|_p$ to finite field extensions of $\mathbb{Q}_p$ in the most natural way possible. First, let us investigate a seemingly natural extension of non-archimedean norms to field extensions. The construction given below can be viewed as a counterexample to the misconception that any field norm naturally extends the p-adic valuation.

Definition 5.1. *Let V be a finite dimensional vector space over a field F. A field norm on V is a map $||.||$ satisfying, for $a \in F$ and $x \in V$,*

$$\begin{aligned} ||x|| = 0 \text{ iff } x = 0 \\ ||ax|| = |a| \cdot ||x|| \\ ||x + y|| \leq \max ||x||, ||y|| \end{aligned}$$

Naturally, we can envision field extensions over $\mathbb{Q}_p$ as vector spaces equipped with a norm. For example, we can write elements in

$$\mathbb{Q}_3[\sqrt{2}] = \{x + y\sqrt{2} : x, y \in \mathbb{Q}_3\}$$

as (x, y), and clearly we want any norm on $\mathbb{Q}_3[\sqrt{2}]$ to satisfy $||(x, 0)|| = |x|$, so that our norm "extends" the p-adic valuation. So consider the norm defined by $||(x, y)|| = \sqrt{|x|^2 + 2|y|^2}$. As an example, we would have

$$||(6, 2)|| = \sqrt{|6|^2 + 2|2|^2} = 2\sqrt{11}$$

Lemma 5.3. *The norm on $\mathbb{Q}_p[\alpha] = \{(x, y) := x + y\alpha : x, y \in \mathbb{Q}_p\}$ defined by $||(x, y)|| = \sqrt{|x|^2 + |\alpha y|^2}$ is a field norm.*

Proof. We will prove the condition $||ax|| = |a| \cdot ||x||$. The other conditions follow immediately from the properties of a norm on a vector space.

For $a \in \mathbb{Q}_p$ and $x = (x_1, x_2) \in \mathbb{Q}_p[\alpha]$, we have

$$\begin{aligned} ||ax|| &= ||(ax_1, ax_2)|| \\ &= \sqrt{|ax_1|^2 + |\alpha a x_2|^2} \\ &= |a|\sqrt{|x_1|^2 + |\alpha x_2|^2} \\ &= |a| \cdot ||x|| \end{aligned}$$

□

Although this particular extension of $|.|_p$ satisfies the definitions of a field norm, its properties do not naturally extend the notion of an "absolute value" in a p-adic field. In particular, we want our extended p-adic norm to be well behaved with respect to multiplication. For example, in $\mathbb{Q}_3[\sqrt{2}]$ with the norm described above,

$$||3 + 2\sqrt{2}|| = 2\sqrt{11} \neq 3 = ||1 + \sqrt{2}||^2$$

So in general, $||xy|| \neq ||x|| \cdot ||y||$. We essentially want a way to define $||\alpha||$ in $\mathbb{Q}_p[\alpha]$ such that $||xy|| = ||x|| \cdot ||y||$ for all $x, y \in \mathbb{Q}_p[\alpha]$. This motivates the following definition:

Definition 5.2. *[3] Let $K = F(\alpha)$ be a finite extension of F and suppose α has monic irreducible polynomial $f(x) = x^n + ... + a_0$ for $a_i \in F$. The norm of α from K to F*

$$N_{K/F}(\alpha) = \det(A_\alpha)$$

where A_α is the corresponding matrix for the F-linear map $\sigma : K \to K$ given by $\sigma(x) = \alpha x$.

With this definition, let us return to our previous example and evaluate $N_{\mathbb{Q}_3[\sqrt{2}]/\mathbb{Q}_3}(3 + 2\sqrt{2})$. Choose the basis $\{1, \sqrt{2}\}$ for $\mathbb{Q}_3[\sqrt{2}]$ over $\mathbb{Q}_3$. Then the linear map $\sigma : \mathbb{Q}_3[\sqrt{2}] \to \mathbb{Q}_3[\sqrt{2}]$ with $\sigma(x) = x(3 + 2\sqrt{2})$ gives us $\sigma(1) = 3 + 2\sqrt{2}$ and $\sigma(\sqrt{2}) = 4 + 3\sqrt{2}$. So the matrix of σ is

$$\begin{bmatrix} 3 & 4 \\ 2 & 3 \end{bmatrix}$$

So

$$N_{\mathbb{Q}_3[\sqrt{2}]/\mathbb{Q}_3}(3 + 2\sqrt{2}) = \begin{vmatrix} 3 & 4 \\ 2 & 3 \end{vmatrix} = 1$$

Most importantly, we can also check that $N_{\mathbb{Q}_3[\sqrt{2}]/\mathbb{Q}_3}(1+\sqrt{2}) = -1$ since the linear transformation given by $x \mapsto x(1+\sqrt{2})$ has matrix

$$\begin{bmatrix} 1 & 2 \\ 1 & 1 \end{bmatrix}$$

This reveals two important facts. The first is immediately obvious - the norm of elements in the field extensions of $\mathbb{Q}_p$ need not be non-negative. The second requires some investigation - it seems that our new norm satisfies

$$N_{K/F}(x)N_{K/F}(y) = N_{K/F}(xy)$$

which is indeed reassuring. But first, let us present alternative ways to calculate these norms:

Theorem 5.4. *Denote irred(α) as the irreducible polynomial for α over $\mathbb{Q}_p$.*
The definition for $N_{K/F}(\alpha)$ is equivalent to:
1) $N_{K/F}(\alpha) = (-1)^n a_0$ where n is the degree of irred(α) and a_0 is its constant term.
2) $N_{K/F}(\alpha) = \prod_{i=1}^{n} \alpha_i$, where α_i are the conjugates of $\alpha = \alpha_1$ over F.

Proof. We choose a convenient basis for K, an n-dimensional vector space over F, namely the set $\{1, \alpha, ..., \alpha^{n-1}\}$. With this basis, the matrix A_α has the following form, which shows that $\det(A_\alpha) = (-1)^n a_0$

$$\begin{bmatrix} 0 & 0 & 0 & ... & 0 & -a_0 \\ 1 & 0 & 0 & ... & 0 & -a_1 \\ 0 & 1 & 0 & ... & 0 & -a_2 \\ . & . & 1 & ... & . & . \\ . & . & . & ... & . & . \\ . & . & . & ... & 1 & -a_{n-1} \end{bmatrix}$$

By the product of roots formula, we know that

$$\prod_{i=1}^{n} \alpha_i = (-1)^n a_0$$

where α_i are the roots of *irred*(α), which are the conjugates of α over F by definition. □

Corollary 5.4.1. *The norm $N_{K/F}$ satisfies $N_{K/F}(x)N_{K/F}(y) = N_{K/F}(xy)$ for all $x, y \in K/F$.*

Proof. Let $a_0, ..., a_n$ be the coefficients of $irred(x)$ and let $b_0, ..., b_m$ be the coefficients of $irred(y)$. So $irred(xy)$ has constant term $a_0 b_0$ with degree $n + m$. Then

$$\begin{aligned} N_{K/F}(x)N_{K/F}(y) &= (-1)^n a_0 (-1)^m b_0 \\ &= (-1)^{m+n} a_0 b_0 \\ &= N_{K/F}(xy) \end{aligned}$$

□

Finally, we have the tools to extend the p-adic norm $|.|_p$ to finite extensions of $\mathbb{Q}_p$.

Definition 5.3. *Let $K/\mathbb{Q}_p$ be a finite extension of degree n. Then for $x \in K$, define*

$$|x|_K = \sqrt[n]{|N_{K/\mathbb{Q}_p}(x)|_p}$$

as the absolute value of x which extends the p-adic norm on $\mathbb{Q}_p$.

In this definition, we move away from viewing elements of $K/\mathbb{Q}_p$ as vectors over $\mathbb{Q}_p$, since the absolute value is well behaved with respect to multiplication. It easily follows by construction that $|.|$ inherits satisfaction of the norm axioms from the p-adic norm. However, one thing still remains ambiguous. Is this extended absolute value still non-archimedean? We will conclude this section with the following result:

Theorem 5.5. *The extended absolute value $|.|_K$ over $K/\mathbb{Q}_p$ is non-archimedean.*

Proof. This result is highly non-trivial and is not a major focus of this report, so it will be omitted. For a full proof, see page 152 of Goueva's *P-adic Numbers - an Introduction*[2]. □

6 The Algebraic Closure - $\overline{\mathbb{Q}_p}$

In our quest to construct a p-adic number system to rival the utility and robustness of $\mathbb{C}$, we don't just want finite extensions of $\mathbb{Q}_p$. We need something much greater. We need the entire algebraic closure of $\mathbb{Q}_p$, that is $\overline{\mathbb{Q}_p}$, fully equipped with solutions to every polynomial. Firstly, it is apparent that

Lemma 6.1. *$\overline{\mathbb{Q}_p}$ is an infinite extension over $\mathbb{Q}_p$.*

Proof. $\mathbb{Q}_p[\{\zeta_i : i \in \mathbb{N}\}]$ where ζ_i are the primitive roots of unity is already an infinite extension of $\mathbb{Q}_p$, and it a subfield of $\overline{\mathbb{Q}_p}$. Hence $\overline{\mathbb{Q}_p}$ is an infinite extension of $\mathbb{Q}_p$. □

The astute reader would have noticed that in the construction of the absolute value, we did not require the finiteness of K over $\mathbb{Q}_p$, nor did we reference specific elements used to extend $\mathbb{Q}_p$ to K (we simply required the elements to be evaluted to actually be in K), so the absolute value naturally extends to $\overline{\mathbb{Q}_p}$.

However, there is an issue with $\mathbb{Q}_p$ that can be easily overlooked. Although we diligently constructed $\mathbb{Q}_p$ as the completion of $\mathbb{Q}$, it actually turns out that

Theorem 6.2. *$\overline{\mathbb{Q}_p}$ is not complete.*

Proof. [1] In $\overline{\mathbb{Q}_2}$, consider the sequence

$$\left(\sum_{n=1}^{N} 2^{n+1/n}\right)_{N\in\mathbb{N}}$$

We note that $2^{n+1/n}$ is a solution to the polynomial $x^n - 2^{n^2} = 0$, so each term in the sequence is in $\overline{\mathbb{Q}_2}$. Also, for $m, k \geq N$, we have

$$\left|\sum_{n=m+1}^{k} 2^{n+1/n}\right| \leq 2^{m+1/m} = 2^{-m} \leq 2^{-N}$$

so this sequence is cauchy. But we note that the denominator of the exponents in $\left(\sum_{n=1}^{N} 2^{n+1/n}\right)_{N\in\mathbb{N}}$ becomes arbitrarily large, so we would require polynomials of arbitrarily large degree and of arbitrarily many terms for which $\sum_{n=1}^{N} 2^{n+1/n}$ is a solution. Hence $\left(\sum_{n=1}^{N} 2^{n+1/n}\right)_{N\in\mathbb{N}}$ does not converge in $\mathbb{Q}_2$ so $\mathbb{Q}_2$ is not complete. □

7 Complex P-adic Numbers - $\mathbb{C}_p$

We have arrived at the final step of our construction - the complex p-adic numbers. The remainder of this report will explore familiar functions under $\mathbb{C}_p$ and their properties.

7.1 Exploring $\mathbb{C}_p$

So far, we have constructed an algebraically closed field $\overline{\mathbb{Q}_p}$ from $\mathbb{Z}_p$, and have extended the p-adic norm to this new field. However, the algebraic closure of the complete field $\mathbb{Q}_p$ is surprisingly no longer complete. There is one more thing we must do to complete our construction of $\mathbb{C}_p$, the p-adic analogue of $\mathbb{C}$.

Definition 7.1. *$\mathbb{C}_p$ is the completion of $\overline{\mathbb{Q}_p}$ under the extended p-adic norm.*

We note that it is not immediately obvious that $\mathbb{C}_p$ is algebraically closed. It is a famous result in field theory that the completion of an algebraically closed field is itself algebraically closed. This property is proven in Lawrence Washington's *Cyclotomic Fields*:

Theorem 7.1. *$\mathbb{C}_p$ is algebraically closed.*

Proof. Proven in page 48-50 of Lawrence Washington's *Cyclotomic Fields*[4]. □

Now, we can define analogues to exponentiation and logarithms in $\mathbb{C}_p$ by their series expansions. But first, let us review an important property of series in the world of the non-archimedean p-adic norm:

Theorem 7.2. *A series $\sum_{n=0}^{\infty} a_n$ converges in $\mathbb{C}_p$ iff $\lim_{n\to\infty} a_n = 0$.*

Proof. If $|a_n| \to 0$, then for any $\varepsilon > 0$ we have $n \geq N \Rightarrow |a_n| < \varepsilon$. So

$$\begin{aligned}\left|\sum_{n=0}^{\infty} a_n\right| &\leq \max(|a_1|, |a_2|, ...) \\ &= \max(|a_1|, |a_2|, ..., |a_{N-1}|, \varepsilon)\end{aligned}$$

Which is a finite value. Conversely, if $\sum_{n=0}^{N} a_n$ converges to L as $N \to \infty$, then $a_N = \sum_{n=1}^{N} a_n - \sum_{n=1}^{N-1} a_n$ converges to $L - L = 0$. □

7.2 The Exponential Function - $\exp(x)$

Definition 7.2. *Define*

$$exp(x) = \sum_{n=0}^{\infty} \frac{x^n}{n!}$$

This is analogous to the power series of e^x in $\mathbb{C}$. An interesting (and somewhat inconvenient) property is that e^x is not well defined for all numbers in its domain. In fact,

Theorem 7.3. *The radius of convergence of $exp(x)$ is no less than $p^{-1/(p-1)}$.*

Proof. If this series converges for some x, then $\lim_{n\to\infty} \frac{x^n}{n!} = 0$. In other words,

$$\lim_{n\to\infty} \nu\left(\frac{x^n}{n!}\right) = \infty$$
$$\lim_{n\to\infty} (n\nu(x) - \nu(n!)) = \infty$$

We see that

$$\nu(n!) = \left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + ... < \frac{n}{p} + \frac{n}{p^2} + ... = \frac{n}{p-1}$$

Indeed, if $\nu(x) > \frac{1}{p-1}$, we have $\nu(x) - \nu(n!)/n > 0$. Let this value be k. Then $\lim_{n\to\infty}(n\nu(x) - \nu(n!)) = \lim_{n\to\infty} kn = \infty$.

So we deduce that the radius of convergence of $\exp(x)$ is no less than $p^{-1/(p-1)}$. □

This fact is convenient as it lies between the discrete norm values p^{-1} and p^0. We can compute that $\exp(a)$ is actually divergent if $|a| = 1$ since $\lim_{n\to\infty} \nu\left(\frac{a}{n!}\right) = \lim_{n\to\infty} \nu\left(\frac{1}{n!}\right) < 0 < \infty$. So for odd p, $\exp(x)$ converges for $|x| \leq p^{-1}$ and diverges for $|x| \geq 1$. In $\mathbb{C}_2$, $\exp(x)$ is indeterminate for $|x| = p^{-1}$ and divergent for $|x| \geq 1$.

It is notable that $\exp(p^k n)$ with $(p, n) = 1$ is defined iff $k \geq 1$ ($k \geq 2$ for $p = 2$). Notably, $\exp(1)$ is undefined and $\exp(0)$ is defined.

7.3 The Logarithmic Function - $\log(x)$

Once again, we borrow power series expansions from calculus to define:

Definition 7.3.

$$\log(1+x) := \sum_{n=1}^{\infty} \frac{(-1)^{n+1}x^n}{n}$$

Theorem 7.4. $\log(1+x)$ *has radius of convergence* 1*, and is divergent if* $|x| = 1$*.*

Proof. We will determine the convergence conditions for $\frac{(-1)^{n+1}x^n}{n}$ as $n \to \infty$, which is equivalent by Theorem 6.2. For (absolute) convergence, we must have (similar to above)

$$\nu(x) - \nu(n)/n > 0$$

as $n \to \infty$. But there exist an infinitude of $n \in \mathbb{Z}_p$ where $\nu(n) = 0$. So we have $\nu(x) > 0$. But the series is clearly divergent for $\nu(x) = 0$ (observe $\sum_{n=1}^{\infty}(-1)^{n+1}$). In other words, $\log(1+x)$ converges iff $|x| < 1$. □

Notably, $\log(1+x)$ is divergent for all $x \in \mathbb{C}_p^{\times}$.

We can extend this function by setting $\log(xy) = \log(x) + \log(y)$ for each $x, y \in \mathbb{C}_p$ and $\log(p) = 0$. It can be proven that $\log(1/n) = -\log(n)$. Indeed, now $\log(1)$ would be defined as $\log(1) = \log(p) + \log(1/p) = 0$.

The following is a weaker version of Lemma 5.5 in Washington's *Cyclotomic Fields*[4], which states that for $|x| < p^{-1/(p-1)}$, then $|\log(1+x)| = |x|$. In particular, if $p = 2$, we have $|x| = p^{-1} \Rightarrow |\log(1+x)| < |x|$.

Theorem 7.5. *In* $\mathbb{C}_p$ *for odd* p*, if* $|x| < p^{-1}$*, then* $|\log(1+x)| = |x|$*.*

Proof. First, observe that for $n \in \mathbb{Z}$, $\nu(n) \leq \log_p(n)$, so $|n|_p \geq p^{-\log_p(n)} = 1/n$. Now, for all $n > 1$, we have

$$\left|\frac{x^n}{n}\right| \leq |x^n|\frac{1}{|n|} < np^{1-n}|x| < 2 \cdot 2^{1-n}|x| = 2^{2-n}|x| \leq 2^0|x| = |x|$$

Hence

$$|\log(1+x)| = \max(|x|, |-x^2/2|, |x^3/3|, ...) = |x|$$

as desired. □

Theorem 7.6. $\log(x) = 0$ *precisely at the values where* $x = p^{a/b}\zeta$*, where* ζ *is a* k^{th} *root of unity and* $a, b \in \mathbb{Z}$ *with* $b \neq 0$*.*

Proof. First, we verify that

$$\log(p^{a/b}\zeta) = \frac{1}{b}\log(p^a) + \log(\zeta) = \frac{1}{k}\log(\zeta^k) = 0$$

Now, suppose $\log(x) = \log(1 + y) = 0$. [We can assume that x is not the multiple of a rational power of p so if follows that $|y| < 1$] (*why?*). Choose sufficiently large N such that $|y^{p^N}| < p^{-1/(p-1)}$. Then

$$x^{p^N} = (1 + y)^{p^N} = \sum_{n=0}^{p^N} \binom{p^N}{n} y^n$$

Then

$$\begin{aligned} |x^{p^N} - 1| &\leq \max\left(|p^N y|, \left|\binom{p^N}{2} y^2\right|, ..., |y^{p^N}|\right) \\ &= \max(p^{-1}, p^{-1}, ..., |y^{p^N}|) \\ &= |y^{p^N}| \\ &< p^{-1/(p-1)} \end{aligned}$$

Hence by the previous lemma, we conclude that $0 = |\log(x^{p^N})| = |x^{p^N} - 1|$. Hence x is a root of unity. □

Using results from calculus, we can show that exp and log are inverses of each other in the domain which they are defined. But recall that we extended log beyond its natural domain. So are these functions still inverses of each other?

Surprisingly, we actually have that

Theorem 7.7. *exp and* log *are not inverses of each other.*

Proof. First, since exp was not extended, we naturally have $\log(\exp(x)) = x$ whenever $\log(\exp(x))$ converges. Indeed,

$$|\exp(x) - 1| = \left|\sum_{n=1}^{\infty} \frac{x^n}{n!}\right| < 1$$

since each $|x^n/n!| \leq |x^n| \cdot \frac{1}{|n!|} < \frac{p^{-n/(p-1)}}{p^{-n/(p-1)}} = 1$. Thus $\exp(x) - 1$ falls within the radius of convergence of $\log(1+x)$. Hence $\log(\exp(x)) = x$ for all $|x| < p^{-1/(p-1)}$.

But observe that $\exp(\log(\zeta)) = \exp(0) = 0 \neq \zeta$. As expected, ζ lies outside of log's radius of convergence and violates the hypothesis that $\exp^{-1} = \log$. □

Lemma 7.8. *For any prime p, the $(p-1)^{th}$ roots of unity are distinct mod p.*

Proof. Let ζ be a primitive $(p-1)^{th}$ root of unity, where p is prime. Then ζ generates the cyclic group of the $(p-1)^{th}$ roots of unity (Theorem 4.3), which is isomorphic to $(\mathbb{Z}/p\mathbb{Z})^\times$ with isomorphism $x \mapsto x \mod p$. So $\zeta \mod p$ generates $(\mathbb{Z}/p\mathbb{Z})^\times$, hence for any $n \in (\mathbb{Z}/p\mathbb{Z})^\times$, we have $(\zeta \mod p)^k = \zeta^k \mod p = n$ for some $1 \leq k \leq p-1$. Thus the $(p-1)^{th}$ roots of unity are distinct mod p. □

This lemma allows us to formulate the following definition:

Definition 7.4. *Given $a \in \mathbb{Z}_p$ and prime p with $p \nmid a$, define $\langle a \rangle = \omega(a)^{-1}a$, where, if $p \neq 2$, $\omega(a)$ is the distinct $(p-1)^{th}$ root of unity such that $a \equiv \omega(a) \mod p$. If $p = 2$, $\omega(a)$ is the distinct 2^{nd} root of unity such that $a \equiv \omega(a) \mod 4$.*

This is the notion of taking the "principal part" of $a \in \mathbb{C}_p$. This is useful since we always have that (for $p \neq 2$), $\langle a \rangle \equiv 1 \mod p$. Now,

Lemma 7.9. $\log(a) = \log\langle a \rangle$

Proof.

$$\begin{aligned}
\log\langle a \rangle &= \log(\omega(a)^{-1}a) \\
&= \log(\omega(a)^{-1}) + \log(a) \\
&= -\frac{1}{k}\log(1) + \log(a) \qquad\qquad (k = \begin{cases} 2 \text{ if } p = 2 \\ p-1 \text{ otherwise} \end{cases}) \\
&= \log(a)
\end{aligned}$$

□

Theorem 7.10. *Given $a \in \mathbb{Z}_p$ with $p \nmid a$, we have $\langle a \rangle^x = \exp(x \log(a))$ for $x \in \mathbb{Z}$.*

Proof. First by definition, Since $\langle a\rangle \equiv 1^x \equiv 1 \mod q$, we have that $\nu_q(\langle a\rangle^x - 1) > 0$ so $|\langle a\rangle^x - 1|_p \leq p^{-1}$ if $p \neq 2$ and $|\langle a\rangle^x - 1|_p \leq p^{-2}$ if $p = 2$. Thus

$$|\langle a\rangle^x - 1|_p < p^{-1/(p-1)}$$

Hence by the log and exp identities shown previously,

$$\begin{aligned}\langle a\rangle^x &= \exp\log(\langle a\rangle^x) \\ &= \exp(x\log(\langle a\rangle)) \\ &= \exp(x\log(a)) \qquad \text{(Lemma 7.8)}\end{aligned}$$

□

Definition 7.5. *For all $X, n \in \mathbb{Q}_p$, define*

$$\binom{X}{n} = \frac{X!}{n!(X-n)!}$$

We will state without proof 2 theorems in functional analysis.

Theorem 7.11. *Any continuous function $f : \mathbb{Z}_p \to \mathbb{Q}_p$ can be written uniquely as $\sum_{n=0}^{\infty} a_n \binom{X}{n}$ with $a_n \to 0$.*

Theorem 7.12. *Let $r < p^{-1/(p-1)} < 1$. If $f(x) = \sum_{n=0}^{\infty} a_n \binom{X}{n}$ with $|a_n| \leq Mr^n$ for some $M \in \mathbb{Q}_p$, then $f(x)$ can be expressed as a power series with radius of convergence at least $(rp^{1/(p-1)})^{-1} > 1$.*

Theorem 7.13. *$\langle a\rangle^x$ converges if $|x| < qp^{-1/(p-1)}$.*

Proof. Similar to above, we have that since $\langle a\rangle \equiv 1 \mod q$, $\nu_p(\log\langle a\rangle - 1) > 0$ for $p \neq 2$ and $\nu_p(\log\langle a\rangle - 1) > 1$ for $p = 2$, hence $|\log\langle a\rangle| \leq 1/q$. For $\langle a\rangle^x = \exp(x\log(a))$ to converge, we must have

$$\begin{aligned}|x\log(a)| &< p^{-1/(p-1)} \\ |x| &< qp^{-1/(p-1)}\end{aligned}$$

which completes the proof. □

Corollary 7.13.1. *We observe that if $p \neq 2$, then $\langle a\rangle^x$ converges when $|a| \leq p \cdot p^{-1} = 1$. If $p = 2$, then it converges when $|a| \leq p^2 \cdot p^{-2} = 1$. Hence $\langle a\rangle^x$ always converges if $a \in \mathbb{Z}_p$.*

We will confirm theorem 7.12 with lemma 7.13. We can write

$$\langle a\rangle^s = (1 + \langle a\rangle - 1)^s = \sum_{n=0}^{\infty} \binom{s}{n} (\langle a\rangle - 1)^n.$$

By Theorem 7.13, since $\nu_q(\langle a\rangle - 1) > 0 \Rightarrow (\langle a\rangle - 1)^n \to 0$, this representation is unique. Let $r = q^{-1}$ and $M = 1$. Then $|\langle a\rangle - 1|^n \leq q^{-n} = Mr^n$, so $\langle a\rangle^n$ has radius of convergence at least $(q^{-1}p^{1/(p-1)})^{-1} = qp^{-1/(p-1)}$, so Theorem 7.12 and Lemma 7.13 agree in this case.

8 Appendix

Code for constructing p-adic sequences using Hensel's Lemma used in section 4:

```
def lift(a, p, f, n):
    power = 1
    ar = [a]
    if f(a)%p!=0:
        return []
    while n>0:
        for i in range(p):
            modp = p**power
            new = a+i*(modp)
            if f(new)%(p*modp)==0 and new%(modp)==a%(modp):
               a = new
               break
        power += 1
        ar.append(a)
        n -= 1
    return ar
```

References

[1] GEdgar. Is a completion of an algebraically closed field with respect to a norm also algebraically closed?, March 2011.

[2] Fernando Quadros Goueva. *P-adic Numbers - an Introduction.* Universitext, 1997.

[3] Evan Turner. The p-adic numbers and finite field extensions of q_p, November 2013.

[4] Lawrence C. Washington. *Cyclotomic Fields.* Graduate Texts in Mathematics, 1996.