P-ADICS, HENSEL'S LEMMA AND STRASSMAN'S THEOREM

YUCHEN CHEN

Abstract. This is an expository paper on an introduction to p-adic numbers. We will start by constructing $\mathbb{Q}_p$ by completing the rational numbers with respect to the p-adic norm. Following construction, we will prove Hensel's Lemma, construct a base p power series representation of $\mathbb{Q}_p$, and discuss the connection between the two. We will also discuss formal power series in $\mathbb{Q}_p$, including p-adic logarithms/ exponentials and Strassman's Theorem.

Contents

1. Construction of p-adics

The field of p-adic numbers, $\mathbb{Q}_p$, is a completion of the rational numbers with respect to the p-adic norm, much like how the real numbers are the completion of the rational numbers with respect to the canonical absolute value. We will begin constructing $\mathbb{Q}_p$ by defining the p-adic norm and completing the rational numbers using Cauchy sequences. Let us first define the p-adic valuation.

Definition 1.1. Let x be a non-zero integer and p be a prime number. The p-adic valuation of x, denoted $ord_p(x)$, is defined to be the largest positive integer r such that p^r divides x. If $x = 0$, define $ord_p(x) = \infty$.

Definition 1.2. Suppose x is a rational number. We can write $x = \frac{s}{t}$, where s, t are integers and t is non-zero. The p-adic valuation of x is then defined as

$$ord_p(x) = ord_p(s) - ord_p(t).$$

This is well-defined since a different fractional representation of x yields the same p-adic valuation.

Example 1.3. The following are a few examples of the 3-adic valuation.

Date: August 14, 2018.

(1) $ord_3(19) = 0$
(2) $ord_3(18) = 2$
(3) $ord_3(\frac{19}{18}) = ord_3(19) - ord_3(18) = -2$.

We will now define a few properties of the p-adic valuation.

Proposition 1.4. *Let x, y be rational numbers. Then*

(1) $ord_p(x) = \infty$ if and only if $x = 0$.
(2) $ord_p(xy) = ord_p(x) + ord_p(y)$.
(3) $ord_p(x + y) \geq \min\{ord_p(x), ord_p(y)\}$.

Proof. (1) This follows from Definition 1.1.

(2) First suppose that both x, y are non-zero integers. By the definition of the p-adic valuation, we see that $x = p^{ord_p(x)}a$ and $y = p^{ord_p(y)}b$, where a, b are integers not divisible by p. Then

$$xy = p^{ord_p(x)}ap^{ord_p(y)}b = p^{ord_p(x)+ord_p(y)}ab,$$

and notice that ab is not divisible by p. This shows that $ord_p(xy) = ord_p(x) + ord_p(y)$.

Now suppose that both $x, y \neq 0$ and $x, y \in \mathbb{Q}$. Then we can write $x = \frac{a}{b}$ and $y = \frac{c}{d}$. We can then apply the integer case. The case where x and y are 0 is clear.

(3) We again start with the case where x and y are non-zero integers. We see that $x = p^{ord_p(x)}a$ and $y = p^{ord_p(y)}b$, where a, b are integers not divisible by p. Then

$$x + y = p^{ord_p(x)}a + p^{ord_p(y)}b.$$

We have multiple cases in the computation of $ord_p(x+y)$. In the first case, consider $ord_p(x) = ord_p(y)$. Then

$$x + y = p^{ord_p(x)}(a + b),$$

so $ord_p(x + y) \geq ord_p(x) = \min\{ord_p(x), ord_p(y)\}$. For the other case, without loss of generality, assume that $ord_p(x) > ord_p(y)$. Then

$$x + y = p^{ord_p(y)}(p^{ord_p(x)-ord_p(y)}a + b).$$

It follows that $ord_p(x+y) = ord_p(y) = \min\{ord_p(x), ord_p(y)\}$. This proves the integer case.

Similar to part 2, the rational case follows from the integer case and the case where x and y are 0 is clear.

□

We will now introduce the concept of a norm and then define the p-adic norm.

Definition 1.5. Let R be a ring. A function $N : R \to [0, \infty)$ is a norm if it satisfies the following properties. For any $x, y \in R$,

(1) $N(x) = 0$ if and only if $x = 0$.
(2) $N(xy) = N(x)N(y)$.
(3) $N(x + y) \leq N(x) + N(y)$.

Definition 1.6. The p-adic norm is a function $N : \mathbb{Q} \to [0, \infty)$ defined by

$$N(x) = p^{-ord_p(x)},$$

where $p^{-\infty} = 0$. From now on we will denote $N(x)$ as $|x|_p$.

Example 1.7. Here are some examples of the 3-adic norm which will follow from Example 1.3.

(1) $|19|_3 = 3^{-0} = 1$.
(2) $|18|_3 = 3^{-2} = \frac{1}{9}$.
(3) $|\frac{19}{18}|_3 = 3^2 = 9$.

We will now prove a few properties of the p-adic norm.

Theorem 1.8. *Let x, y be rational numbers. The following properties hold.*

(1) $|x|_p = 0$ *if and only if* $x = 0$.
(2) $|xy|_p = |x|_p|y|_p$.
(3) $|x + y|_p \leq \max\{|x|_p, |y|_p\}$.

Proof. (1) This follows clearly from Proposition 1.4(a).

(2) By definition, $|xy|_p = p^{-ord_p(xy)}$ which is equal to $p^{-(ord_p(x)+ord_p(y))}$ by Proposition 1.4(b). Then

$$p^{-(ord_p(x)+ord_p(y)} = p^{-ord_p(x)}p^{-ord_p(y)} = |x|_p|y|_p.$$

(3) By definition,

$$|x + y|_p = p^{-ord_p(x+y)} \leq p^{-\min\{ord_p(x),ord_p(y)\}}$$

by Proposition 1.4(c). It follows that $|x + y|_p \leq \max\{|x|_p, |y|_p\}$.

□

Remark 1.9. Theorem 1.8 shows us that the p-adic norm satisfies the definition of a norm given in Definition 1.5. Moreover, the third property of Theorem 1.8, $|x + y|_p \leq \max\{|x|_p, |y|_p\}$, is a stronger property than the triangle inequality given in Definition 1.5(c). The property given in Theorem 1.8(c) is called the ultrametric inequality property. Norms with this property are called non-Archimedian norms. It then follows that the p-adic norm is a non-Archimedian norm. This is an important difference from norms such as the canonical absolute value on the real numbers, which does not satisfy the ultrametric inequality property.

The field $\mathbb{Q}_p$ will now be defined as the completion of $\mathbb{Q}$ with respect to the p-adic norm. A canonical representation of elements in the completion is via Cauchy sequences which we will now describe.

Definition 1.10. A sequence $\{a_n\}_{n=1}^{\infty}$ is Cauchy with respect to $|\cdot|_p$ if for every $\epsilon > 0$, there exists a positive integer N, such that for all positive integers $m, n \geq N, |a_m - a_n|_p < \epsilon$.

Definition 1.11. Let $\{a_n\}_{n=1}^{\infty}$ and $\{b_n\}_{n=1}^{\infty}$ be two Cauchy sequences in the rational numbers. Then define $\{a_n\}_{n=1}^{\infty} \approx_p \{b_n\}_{n=1}^{\infty}$ if $\lim_{n\to\infty} |a_n - b_n|_p = 0$.

Proposition 1.12. *The relation $\approx_p$ defined in Definition 1.12 is an equivalence relation.*

Proof. The reflexive and symmetric properties are easy to verify. We will show the transitive property. Suppose $\{a_n\}_{n=1}^{\infty} \approx_p \{b_n\}_{n=1}^{\infty}$ and $\{b_n\}_{n=1}^{\infty} \approx_p \{c_n\}_{n=1}^{\infty}$. Let $\epsilon > 0$. There exists N' such that if $n \geq N'$ then $|a_n - b_n|_p < \frac{\epsilon}{4}$. There also exists N'' such that if $n \geq N''$ then $|b_n - c_n|_p < \frac{\epsilon}{4}$. Let $N = \max\{N', N''\}$. Then if $n \geq N$, we have that $|a_n - c_n|_p \leq |a_n - b_n| + |b_n - c_n|_p < \epsilon$. Thus, we get that $\{a_n\}_{n=1}^{\infty} \approx_p \{c_n\}_{n=1}^{\infty}$. □

Definition 1.13. We define $\mathbb{Q}_p$ to be the set of equivalence classes of Cauchy sequences of rational numbers given by the equivalence relation $\approx_p$.

Definition 1.14. Define $N_{\mathbb{Q}_p} : \mathbb{Q}_p \to [0, \infty)$ by $N_{\mathbb{Q}_p}(X) = \lim_{n\to\infty} |x_n|_p$, where $\{x_n\}_{n=1}^{\infty}$ is a Cauchy sequence representation of X. From now on, we denote $N_{\mathbb{Q}_p}$, the extension of $|\cdot|_p$ to $\mathbb{Q}_p$, by $|\cdot|_p$ as well.

Proposition 1.15. *The norm $|\cdot|_p$ is well-defined.*

Proof. We need to show that the limit exists and is independent of which representation that we choose. Let $X \in \mathbb{Q}_p$ and $\{x_n\}_{n=1}^{\infty}$ be a representation of X. To show that the limit exists, let $\epsilon > 0$. There exists N' such that if $n, m \geq N$ then $|x_m - x_n|_p < \epsilon$. Then for any $m, n \geq N$, we have that

$$|x_n|_p - |x_m|_p \leq |x_n - x_m|_p$$

and

$$|x_m|_p - |x_n|_p \leq |x_n - x_m|_p.$$

It follows that

$$||x_n|_p - |x_m|_p| \leq |x_n - x_m|_p < \epsilon.$$

Thus, $|X|_p$ is a Cauchy sequence in the real numbers so the limit exists.

Now to show that $|\cdot|_p$ is independent of the choice of representatives, assume that $\{y_n\}_{n=1}^{\infty}$ is a different representation of the same equivalence class. Then

$$\lim_{n\to\infty} |y_n|_p \leq \lim_{n\to\infty} |y_n - x_n|_p + \lim_{n\to\infty} |x_n|_p = \lim_{n\to\infty} |x_n|_p.$$

Similarly,

$$\lim_{n\to\infty} |x_n|_p \leq \lim_{n\to\infty} |x_n - y_n|_p + \lim_{n\to\infty} |y_n|_p = \lim_{n\to\infty} |y_n|_p.$$

Thus, $\lim_{n\to\infty} |x_n|_p = \lim_{n\to\infty} |y_n|_p$. □

Remark 1.16. Given x, y in $\mathbb{Q}_p$, let $\{x_n\}_{n=1}^{\infty}$ and $\{y_n\}_{n=1}^{\infty}$ be representations of x, y respectively. Then $x + y$ is the equivalence class represented by the sequence, $\{x_n + y_n\}_{n=1}^{\infty}$ and xy is the equivalence class given by sequence $\{x_n y_n\}_{n=1}^{\infty}$. With these operations, it can be checked that $|\cdot|_p$ extended to $\mathbb{Q}_p$ satisfies the definition of a norm given in Definition 1.5.

Definition 1.17. A space X is complete with respect to norm N if every Cauchy sequence in X converges to an element of X with respect to norm N.

Theorem 1.18. *The space $\mathbb{Q}_p$ is complete.*

Proof. Let $\{a_n\}_{n=1}^{\infty}$ be a Cauchy sequence in $\mathbb{Q}_p$. We know that each term a_n can be identified by a Cauchy sequence $\{b_{nm}\}_{m=1}^{\infty}$ in $\mathbb{Q}$ by construction. For each positive integer k we can find a positive integer N_k such that for any $m, n \geq N_k$,

we have $|b_{km} - b_{kn}|_p < \frac{1}{k}$. Let $k_1, k_2, k_3, ...$ be positive integers with the property that $k_1 < k_2 < k_3 < ...$, and $k_i \geq N_i$ for all i. Define sequence $\{c_n\}_{n=1}^{\infty}$ by

$$c_n = b_{nk_n}.$$

We first show that $\{c_n\}_{n=1}^{\infty}$ is a Cauchy sequence. Let $\epsilon > 0$. Since $\{a_n\}_{n=1}^{\infty}$ is a Cauchy sequence, there exists N such that if $m_1, m_2 \geq N$ then $|a_{m_1} - a_{m_2}|_p < \epsilon$. Thus, by definition, $\lim_{n\to\infty} |b_{m_1 n} - b_{m_2 n}|_p < \epsilon$. Therefore there exists N' such that if $n \geq N'$ then $|b_{m_1 n} - b_{m_2 n}| < \epsilon$. Now let $m, n \geq \max\{N, N'\}$. We see that

$$|c_m - c_n|_p = |b_{mk_m} - b_{nk_n}|_p < \epsilon.$$

Thus, $\{c_n\}_{n=1}^{\infty}$ is a Cauchy sequence in $\mathbb{Q}$ with respect to $|\cdot|_p$. Let C denote the element of $\mathbb{Q}_p$ represented by the Cauchy sequence $\{c_n\}_{n=1}^{\infty}$.
Finally, we have to show that $\lim_{n\to\infty} a_n = C$. Let $\epsilon > 0$. We have that

$$|C - a_n|_p \leq |C - B|_p + |B - a_n|_p = \lim_{m\to\infty} |b_{mk_m} - b_{nk_n}|_p + \lim_{m\to\infty} |b_{nk_n} - b_{nk_m}|_p.$$

where B is the element of $\mathbb{Q}_p$ represented by the sequence where every term is b_{nk_n}. There exists positive integer N' such that $\frac{1}{N'} < \frac{\epsilon}{2}$ and N'' such that for any $m, n \geq N''$, $|a_m, a_n|_p < \frac{\epsilon}{2}$. Therefore, $\lim_{k\to\infty} |b_{mk} - b_{nk}|_p < \frac{\epsilon}{2}$.

Now let $N = \max\{N', N''\}$. Then for any $n \geq N$, for large enough m, we have $|b_{mk_m} - b_{nk_n}|_p < \frac{\epsilon}{2}$ and $|b_{nk_n} - b_{nk_m}|_p < \frac{\epsilon}{2}$. Thus,

$$|C - a_n|_p \leq \lim_{m\to\infty} |b_{mk_m} - b_{nk_n}|_p + \lim_{m\to\infty} |b_{nk_n} - b_{nk_m}|_p < \epsilon.$$

This shows that $\lim_{n\to\infty} a_n = C$. Thus, $\mathbb{Q}_p$ is complete. □

Definition 1.19. Let X be a space. Suppose that $Y \subset X$. Then Y is dense in X with respect to norm N if every element of X is the limit of a sequence in Y.

Theorem 1.20. *The set of rational numbers is dense in $\mathbb{Q}_p$.*

Proof. We can embed $\mathbb{Q}$ in $\mathbb{Q}_p$, since for every $x \in \mathbb{Q}$, we can map it to the equivalence class represented by the Cauchy sequence $(x, x, ...)$. Let $y \in \mathbb{Q}_p$. Then y can be written as a Cauchy sequence of rational numbers. This sequence converges to y. □

Theorem 1.21. *The space $\mathbb{Q}_p$ is a field.*

Proof. This can be checked and is left to the reader. □

This completes our construction.

2. Representation as Power Series

In the construction of the p-adic field, the elements of $\mathbb{Q}_p$ are represented by Cauchy sequences. While this is important for the construction of $\mathbb{Q}_p$, it is difficult to work with $\mathbb{Q}_p$ as Cauchy sequences. As an example, since the real numbers are also a completion of the rational numbers, we can also represent real numbers by Cauchy sequences, but we rarely think about them in that way. One way to represent elements of $\mathbb{Q}_p$ is by using power series expansions of base p. This is analogous to the decimal expansion of real numbers.

Definition 2.1. We define $\mathbb{Z}_p$, the set of p-adic integers, to be the set of elements of $\mathbb{Q}_p$ with norm less than or equal to 1. In other words,

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

It is not hard to see that $\mathbb{Z}_p$ is a subring of $\mathbb{Q}_p$.

We will start by representing elements of $\mathbb{Z}_p$ as a power series.

Lemma 2.2. *Let α be a p-adic integer. Then there exists Cauchy sequence $\{a_n\}_{n=1}^{\infty}$ in the integers which converges to α such that*

$$0 \leq a_i \leq p^i - 1 \text{ and } a_{i+1} \equiv a_i \mod p^i$$

for all positive integer i.

Proof. Let n be a positive integer. We know that the rationals are dense in $\mathbb{Q}_p$ so there exists rational q such that $|\alpha - q|_p < p^{-n}$. We can write $q = \frac{s}{t}$ where s, t are both integers and coprime. Since $|\alpha|_p \leq 1$, $|q|_p \leq 1$. We then know that p does not divide t. Then t is a unit in $\mathbb{Z} \setminus p\mathbb{Z}$. Thus, there exists integer x such that $tx \equiv s \mod p^n$. Let $x \equiv a_n \mod p^n$. Then $0 \leq a_n \leq p^n - 1$. We also see that $\alpha \equiv q \mod p^n$, and $a_n \equiv q \mod p^n$, so $a_n \equiv \alpha \mod p^n$. This shows that $\{a_n\}_{n=1}^{\infty}$ converges to α. It also follows from this that $a_{i+1} \equiv a_i \mod p^i$ for all positive integer i. □

Proposition 2.3. *Let α be a p-adic integer, then*

$$\alpha = \alpha_0 + \alpha_1 p + \alpha_2 p^2 + ...,$$

where $0 \leq \alpha_i \leq p - 1$.

Proof. By Lemma 2.2, we have a sequence $\{a_n\}_{n=1}^{\infty}$ which converges to α such that

$$0 \leq a_i \leq p^i - 1 \text{ and } a_{i+1} \equiv a_i \mod p^i.$$

From these conditions, we see that we can rewrite $\{a_n\}_{n=1}^{\infty}$ as

$$a_1 = \alpha_0,$$

$$a_2 = \alpha_0 + \alpha_1 p,$$

$$a_3 = \alpha_0 + \alpha_1 p + \alpha_2 p^2, ...$$

We have then defined the coefficients for the power series representation of α. It is clear that this power series converges to α, since $\{a_n\}_{n=1}^{\infty}$ is the sequence of partial sums and we know that it converges to α. □

Theorem 2.4. *The power series representation in Proposition 2.3 is unique.*

Proof. Let $\alpha = \alpha_0' + \alpha_1' p + ...$ be another power series representation of α. Let n be the first positive integer where, $\alpha_n \neq \alpha_n'$. Without loss of generality, we assume that $\alpha_n < \alpha_n'$. Define β_n as

$$\beta_n = a_0 + a_1 p + ... + a_n p^n,$$

and define β_n' similarly with a_i' as the notation for the coefficients. We see that $\beta_n' - \beta_n = (a_n' - a_n)p^n$. Thus, $|\beta_n' - \beta_n|_p = \frac{1}{p^n}$. However, by the ultrametric inequality property, we also have that $|\beta_n' - \beta_n|_p = |(\beta_n' - \alpha) + (\alpha - \beta_n)|_p < \frac{1}{p^n}$. We then have a contradiction so the power series representation is unique. □

Remark 2.5. This is not true for decimal expansion since $0.9999... = 1.00000....$

Theorem 2.6. *Let α be a p-adic rational number, then*

$$\alpha = \alpha_{-m}p^{-m} + \alpha_{-m+1}p^{-m+1} + ... + \alpha_{-1}p^{-1} + \alpha_0 + \alpha_1 p + \alpha_2 p^2 + ...,$$

where $0 \leq \alpha_i \leq p-1$.

Proof. If α is a p-adic integer, then we are done. If not, then we know that $|\alpha|_p > 1$, so by definition of p-adic norm, $|\alpha|_p = p^m$, for some positive integer m. We then notice that $|p^m\alpha|_p = 1$, so there exists power series expansion $p^m\alpha = \alpha_0 + \alpha_1 p + \alpha_2 p^2 + ...$ We can then write

$$\alpha = \alpha_0 p^{-m} + \alpha_1 p^{-m+1} + ... + \alpha_{m-1}p^{-1} + \alpha_m + \alpha_{m+1}p + ...$$

□

Example 2.7. Suppose we wish to find the base 5 expansion of 7. We can see that $7 = 2 + 1(5)$. In general, the p-adic expansions for integers are finite.

Theorem 2.8. *Suppose x is a p-adic integer with $|x|_p < 1$, then $\sum_{k=0}^{\infty} x^k$ converges to $\frac{1}{1-x}$.*

Proof. This proof is the same as in $\mathbb{R}$. □

Example 2.9. We will find $-1 \in \mathbb{Q}_5$. From Theorem 2.8, we see that $\sum_{k=0}^{\infty} 5^k = \frac{1}{-4}$

Thus, $-1 = 4\sum_{k=0}^{\infty} 5^k = \sum_{k=0}^{\infty} 4 \cdot 5^k$.

We will now define addition and multiplication with p-adic power series expansions. These are analogous to addition and multiplication in the decimal system.

Addition. Let $\sum a_k p^k$ and $\sum b_k p^k$ be elements in $\mathbb{Q}_p$. To add, we start in the p^0 place and add $a_0 + b_0$. We define c_0 by $c_0 \equiv (a_0 + b_0) \bmod p$. If $(a_0 + b_0) \geq p$, we "carry" the multiple of p to the p^1 place. We repeat the process and the sum is $\sum c_k p^k$. This is analogous to the vertical addition algorithm in the decimal system.

Example 2.10. We know that the p-adic expansion for $1 \in \mathbb{Q}_5$ is $1+0\cdot5+0\cdot25+...$, and we have shown that $-1 = \sum_{k=0}^{\infty} 4 \cdot 5^k$ in $\mathbb{Q}_5$. We will now verify that $-1 + 1 = 0$ in $\mathbb{Q}_5$.

$$\begin{array}{cccccc} & & 1 & 1 & & \\ & ... & 4 & 4 & 4 & \\ + & & & & 1 & \\ \hline & ... & 0 & 0 & 0 & . \end{array}$$

Multiplication. Let $\sum a_k p^k$ and $\sum b_k p^k$ be elements in $\mathbb{Q}_p$. To multiply we need to "match" up powers of p. For example, to find the c_2 term, we need to find all terms that multiply to have a p^2 term. Thus, we have $c_2 = a_0b_2 + a_2b_0 + a_1b_1$, where we carry accordingly when adding. Similar to addition, an easier way to visualize multiplication is with the vertical method we are familiar with for integers.

Example 2.11. Later on in Example 3.4, we will show that $\sqrt{-1}$ exists in $\mathbb{Q}_5$. Suppose we wish to find a p-adic expansion of $\sqrt{-1}$. We note that $\sqrt{-1}\cdot\sqrt{-1} = -1$.

$$\begin{array}{cccccc} & \ldots & a_2 & a_1 & a_0 & \\ \times & \ldots & a_2 & a_1 & a_0 & \\ \hline & \ldots & a_0a_2 & a_0a_1 & a_0^2 & \\ & \ldots & a_1a_2 & a_1^2 & & \\ & \ldots & a_2^2 & & & \\ \hline & \ldots & 4 & 4 & 4 & . \end{array}$$

From this, we see that we want $a_0^2 \equiv 4 \bmod 5$. One option is that $a_0 = 3$. We need to carry a 1. We then see that we want $3a_1 + a_1^2 + 1 \equiv 4 \bmod 5$. We see that $a_1 = 3$ works. We need to carry a 3 over. For a_2, we see that we want $2a_2 + 4a_2 + a_2^2 + 3 \equiv 4 \bmod 5$. Notice that $a_2 = 2$ works here. Continuing like this we can get more coefficients. Note that if we chose $a_0 = 2$, we would get a different power series representation.

3. Hensel's Lemma

In this section, we will introduce Hensel's Lemma.

Definition 3.1. Let $f(X)$ be a polynomial with integer coefficients, and p be a prime number. Suppose we have a solution $f(x_1) \equiv 0 \bmod p$. Then a solution $f(x_n) \equiv 0 \bmod p^n$ where $x_n \equiv x_1 \bmod p$ is called a lift of x_1 modulo p^n for some given $n > 0$.

Example 3.2. Let $f(X) = X^2 + 1$. We can see that $f(2) \equiv 0 \bmod 5$ and $f(3) \equiv 0 \bmod 5$. Suppose we want to find a lift of 2 and 3 mod 25. We need $x \equiv 2 \bmod 5$, so $x = 5t + 2$ for some integer t. We then want that $(5t + 2)^2 + 1 \equiv 0 \bmod 25$, so $t = 1$. This gives us that $x = 7$. A similar calculation shows us that 18 is a lift of 3 modulo 25.

The idea of lifts is important in regards to Hensel's lemma. More specifically, Hensel's lemma will tell us under what conditions further lifts can be obtained and more importantly will extend the idea of lifts to finding p-adic solutions of a polynomial in $\mathbb{Z}_p$.

Theorem 3.3. *(Hensel's Lemma). If $f(X)$ is a polynomial with coefficients in the p-adic integers and $a \in \mathbb{Z}_p$ satisfies*

$$f(a) \equiv 0 \text{ mod } p \text{ and } f'(a) \not\equiv 0 \text{ mod } p,$$

then there exists a unique $\alpha \in \mathbb{Z}_p$ such that $f(\alpha) = 0$ and $\alpha \equiv a \text{ mod } p$.

Proof. The idea of the proof revolves around finding α by inductively constructing a Cauchy sequence, $\{a_n\}_{n=1}^{\infty}$, such that for any n, $f(a_n) \equiv 0 \bmod p^n$ and $a_n \equiv a \bmod p$. This will be done by subsequently lifting from n to $n + 1$.

The base case is clear. We take a_1 to be a which satisfies the properties stated above.

For the inductive step, suppose there exists an a_n that satisfies the above properties. To find an a_{n+1} with the desired properties, we only need that $a_{n+1} \equiv a_n$

mod p^n and that $f(a_{n+1}) \equiv 0 \bmod p^{n+1}$. Since $a_{n+1} \equiv a_n \bmod p^n$, $a_{n+1} = tp^n + a_n$ for some integer t. By Taylor series expansion centered on a_n,

$$f(tp^n + a_n) = f(a_n) + f'(a_n)tp^n + \frac{f''(a_n)}{2!}t^2p^{2n} + ...,$$

so

$$f(tp^n + a_n) \equiv f(a_n) + f'(a_n)p^n t \bmod p^{n+1}.$$

Then set $f(tp^n + a_n)$ to 0 resulting in,

$$0 \equiv f(a_n) + f'(a_n)p^n t \bmod p^{n+1}.$$

This can be solved for t and we get that

$$t \equiv \frac{-f(a_n)}{f'(a_n)p^n} \bmod p.$$

As a result, we have found the unique a_{n+1} term.

We have now constructed the Cauchy sequence $\{a_n\}_{n=0}^{\infty}$. Denote its limit as α. We must show that $\alpha \equiv a \bmod p$ and also that $f(\alpha) = 0$.

We will first show that for any positive integer $n > 1$, $a_n \equiv a_1 \bmod p$, with induction. The base case is clear from construction of $\{a_n\}_{n=0}^{\infty}$. For the inductive step, suppose that $a_n \equiv a_1 \bmod p$. Since $a_{n+1} \equiv a_n \bmod p^n$, $a_{n+1} \equiv a_1 \bmod p$.

By letting n go to infinity, it follows that $\alpha \equiv a_1 \bmod p$. Thus, $\alpha \equiv a \bmod p$.

To show that $f(\alpha) = 0$, It is sufficient to show that $|f(\alpha)|_p = 0$. By what we found above, $|f(a_n)|_p \leq \frac{1}{p^n}$ for every positive integer n, since $f(a_n) \equiv 0 \bmod p^n$. Taking n to infinity shows us that $|f(\alpha)|_p \leq 0$, so $|f(\alpha)|_p = 0$ must hold since the p-adic norm cannot be negative. This implies that $f(\alpha) = 0$.

□

Example 3.4. We will now show that $\sqrt{-1}$ exists in $\mathbb{Z}_5$. Let $f(X) = X^2 + 1$. We see that $f(2) \equiv 0 \bmod 5$ and $f'(2) \not\equiv 0 \bmod 5$, so by Hensel's Lemma, there exists a root of f in $\mathbb{Z}_5$. Similarly, $f(3) \equiv 0 \bmod 5$, and $f'(3) \not\equiv 0 \bmod 5$. We then have another root of f. This makes sense, since f is a polynomial of degree two, so we would expect f to have two roots, unless one is a double root.

Remark 3.5. The p-adic expansion seems similar to Hensel's Lemma, especially with regards to lifting. The proof of Hensel's Lemma shows us that each lift gives us a closer approximation to the p-adic solution. For example, take $f(X) = X^2 + 1$ again in $\mathbb{Q}_5$. In Example 2.2, we showed that 3 is a lift mod 5, 18 is a lift mod 25 and continuing the process it follows that 68 is a lift mod 125. We can write these lifts as follows

$$3 = 3$$

$$18 = 3 + 3 \cdot 5$$

$$68 = 3 + 3 \cdot 5 + 2 \cdot 25.$$

As we can see, each lift gives us the next term in the partial sum, resulting in a closer and closer approximation of the power series representation.

4. Logarithms and Exponentials

We begin our discussion on logarithms and exponentials by deriving a few more facts about p-adic power series. Many of these rely on the ultrametric inequality property and thus do not hold in $\mathbb{R}$.

Theorem 4.1. *A series $\sum_{n=0}^{\infty} a_n$ in $\mathbb{Q}_p$ converges if and only if the sequence $\{a_n\}_{n=0}^{\infty}$ converges to 0.*

Proof. By definition, the sequence of partial sums $\{S_n\}_{n=0}^{\infty}$ must converge. Then $\{S_n\}_{n=0}^{\infty}$ must be a Cauchy sequence. Let $\epsilon > 0$. There exists positive integer N such that for any $m, n \geq N$, $|S_m - S_n|_p < \epsilon$. Let $M \geq N$. Then $|a_M|_p = |S_{M+1} - S_M|_p < \epsilon$. Thus, $\{a_n\}_{n=1}^{\infty}$ converges to 0.
For the converse, we know that $\{a_n\}_{n=1}^{\infty}$ converges to 0. Let $\epsilon > 0$. There exists positive integer N such that if $n \geq N$ then $|a_n|_p < \epsilon$. Now let $m, n \geq N$. Without loss of generality assume that $m > n$. Then $|S_m - S_n|_p \leq \max\{a_{n+1}, ..., a_m\} < \epsilon$ by the ultrametric inequality property. Thus, $\{S_n\}_{n=0}^{\infty}$ is Cauchy so it converges. □

Remark 4.2. In the real numbers, the second part of Theorem 4.1 does not hold, for example the sum of the harmonic sequence. The backwards direction is a consequence of the ultrametric inequality property which is not satisfied by the absolute value in the real numbers.

Theorem 4.3. *If $\sum_{k=0}^{\infty} a_k$ converges, then any reordering must also converge. Moreover, any reordering must converge to the same sum.*

Proof. This is the result of $\sum_{k=0}^{\infty} a_k$ being absolutely convergent. Let $\sum_{k=0}^{\infty} a'_k$ be a reordering. Let $\epsilon > 0$. We know that $\{a_n\}_{n=0}^{\infty}$ converges to 0, since the sum of $\{a_n\}_{n=0}^{\infty}$ converges, so we can find positive integer N, such that if $n \geq N$ then $|a_n|_p < \epsilon$, $|a'_n|_p < \epsilon$ and $|\sum_{k=0}^{\infty} a_k - S_n|_p < \epsilon$, where S_n is the n-th partial sum of the original series. Let $n \geq N$. Define S as the sum of terms a_i, $i \leq n$, where $|a_i|_p \geq \epsilon$, and S' as the sum of a'_i, $i \leq n$ where $|a'_i|_p \geq \epsilon$. Notice that $S = S'$. By the ultrametric inequality property, we deduce that $|S_n - S|_p < \epsilon$ and $|S'_n - S'|_p < \epsilon$, since we subtracted out the terms in each case that have p-adic norm greater than ϵ. Then using ultrametric inequality property again, we see that $|S_n - S'_n|_p = |S_n - S + S' - S'_n|_p < \epsilon$. Using the ultrametric inequality property again, we get that

$$|\sum_{k=0}^{\infty} a_k - S'_n|_p = |\sum_{k=0}^{\infty} a_k - S_n + S_n - S'_n|_p < \epsilon.$$

□

Definition 4.4. Let $f(X)$ be a formal power series with coefficients in a ring R. Then $r \in \mathbb{R} \cup \{\infty\}$ is the radius of convergence of f if for any x in the disc $D = \{x \in R \mid |x| < r\}$, $f(x)$ converges.

Remark 4.5. Suppose that $f(X) = \sum_{n=0}^{\infty} a_n X^n$ is a power series in $\mathbb{Q}_p[[X]]$. By Theorem 4.1, we know that if $f(x)$ converges then $a_n x^n \to 0$. We then write the

radius of convergence r as

$$r = \sup\{|x|_p \mid a_n x_n \to 0\}.$$

Theorem 4.6. *Let* $f(X) = \sum_{n=0}^{\infty} a_n X^n$ *be a power series in* $\mathbb{Q}_p[[X]]$. *Then the radius of convergence is*

$$r = \frac{1}{\limsup_{n\to\infty} |a_n|_p^{1/n}}.$$

Proof. This proof is the same as the proof in $\mathbb{R}$. □

We will now introduce logarithims and exponentials in $\mathbb{Q}_p$.

Definition 4.7. We define p-adic log and exponential as follows

$$\log_p(X) = \sum_{n=0}^{\infty} (-1)^{n+1} \frac{(X-1)^n}{n}$$

and

$$\exp_p(X) = \sum_{n=0}^{\infty} \frac{X^n}{n!}.$$

Theorem 4.8. *The p-adic logarithm,* log_p, *is defined for all* x *such that* $|x-1|_p < 1$.

Proof. We will compute the radius of convergence. Observe that $|\frac{(-1)^{n+1}}{n}|_p = |\frac{1}{n}|_p = p^{ord_p(n)}$. Thus,

$$\limsup_{n\to\infty} |a_n|_p^{1/n} = \limsup_{n\to\infty} p^{\frac{ord_p(n)}{n}} = 1.$$

By Theorem 4.6, we get that the radius of convergence is 1. □

To compute the domain of exp_p, we will first show a lemma.

Lemma 4.9. *Let* n *be a positive integer. We know that* n *has a finite p-adic expansion*

$$n = \sum_{i=0}^{m} a_i p^i.$$

We define

$$S_n = \sum_{i=0}^{m} a_i.$$

Then

$$ord_p(n!) = \frac{n - S_n}{p-1}.$$

Proof. For each $1 \le i \le m$, we notice that the number of integers between 1 and n that are divisible by p^i is $\left\lfloor \frac{n}{p^i} \right\rfloor$. We can then see that

$$ord_p(n!) = \sum_{i=1}^{m} \left\lfloor \frac{n}{p^i} \right\rfloor.$$

Observe that

$$\frac{n}{p^i} = \frac{\sum_{k=0}^{m} a_k p^k}{p^i} = \sum_{k=0}^{m} a_k p^{k-i} = \sum_{k=0}^{i-1} a_k p^{k-i} + \sum_{k=i}^{m} a_k p^{k-i}.$$

It is clear that $\sum_{k=i}^{m} a_k p^{k-i}$ is an integer. From our construction of the p-adic expansion, $a_k \leq p-1$ for all k. This shows that

$$\sum_{k=0}^{i-1} a_k p^{k-i} \leq \sum_{k=0}^{i-1} (p-1)p^{k-i} = (p^i - 1)p^{-i} < 1.$$

It follows that

$$\left\lfloor \frac{n}{p^i} \right\rfloor = \sum_{k=i}^{m} a_k p^{k-i}.$$

We now have that

$$ord_p(n!) = \sum_{i=1}^{m} \sum_{k=i}^{m} a_k p^{k-i}$$

$$= \frac{a_1(p-1) + a_2(p^2-1) + ... + a_m(p^m - 1)}{p-1}$$

$$= \frac{(a_1 p + ... + a_m p^m) - (a_1 + ... + a_m)}{p-1}$$

$$= \frac{(a_0 + a_1 p + ... + a_m p^m) - (a_0 + a_1 + ... + a_m)}{p-1} = \frac{n - S_n}{p-1}.$$

□

Theorem 4.10. *The exponential exp_p is defined for all x such that $|x|_p < p^{\frac{-1}{p-1}}$.*

Proof. We again compute the radius of convergence. Using our lemma, we see that

$$|\frac{1}{n!}|_p^{\frac{1}{n}} = p^{\frac{(n-S_n)}{n(p-1)}} = p^{\frac{1-\frac{S_n}{n}}{p-1}}.$$

It follows that

$$\limsup_{n\to\infty} |\frac{1}{n!}|_p^{\frac{1}{n}} = p^{\frac{1}{p-1}}.$$

Thus, the radius of convergence by Theorem 4.6 is $p^{\frac{-1}{p-1}}$.

□

The p-adic logarithm and exponential share properties with the logarithm and exponential in real numbers.

Theorem 4.11. *If x, y are p-adic numbers such that $|x-1|_p < 1$ and $|y-1|_p < 1$, then*

$$\log_p(xy) = \log_p(x) + \log_p(y).$$

Proof. We can evaluate the expression, $\log_p(x) + \log_p(y) - \log_p(xy)$ by rearranging the terms of the sequence by Theorem 4.3. They can be rearranged so that each term is 0. The theorem then follows. □

Theorem 4.12. *If x, y are p-adic numbers such that $|x|_p < p^{\frac{-1}{p-1}}$ and $|y|_p < p^{\frac{-1}{p-1}}$, then*

$$\exp_p(x+y) = \exp_p(x)\exp_p(y).$$

Proof. This proof is similar to the proof of Theorem 4.11. □

Theorem 4.13. *Define $D = \{x \in \mathbb{Q}_p \mid |x|_p < p^{\frac{1}{p-1}}\}$. The exponential $\exp_p : D \to 1+D$ and logarithm $\log_p : 1+D \to D$ are inverses. That is*

$$\log_p(\exp_p(x)) = x \text{ and } \exp_p(\log_p(x)) = x. \tag{4.14}$$

Proof. We must show that these series converge. First we see that

$$|\exp_p(x) - 1|_p = |\sum_{k=1}^{\infty} \frac{x^n}{n!}|_p \leq |x|_p.$$

Similarly,

$$|\log_p(x)|_p = |\sum_{k=1}^{\infty} (-1)^{n+1} \frac{(x-1)^n}{n}|_p \leq |x-1|_p.$$

The expressions in (4.14) follow from the space of formal power series expansions. □

5. Strassman's Theorem

We will continue to discuss p-adic power series. In this section, we will introduce Strassman's Theorem which relates to the zeros of a power series. In particular, Strassman's Theorem will give us the maximum number of zeros of a power series in the p-adic integers under certain conditions. We will then conclude with a few corollaries. This section follows closely from Hutter, Szedlák, Wirth [4].

Theorem 5.1. *(Strassman's Theorem) Let $f : \mathbb{Z}_p \to \mathbb{Q}_p$ be such that $f(X) = \sum_{n=0}^{\infty} a_n X^n$ is a non-zero power series in $\mathbb{Q}_p[[X]]$, and $\lim_{n\to\infty} a_n = 0$. Define N as follows,*

(1) $|a_N|_p = \max_{n\geq 0} |a_n|_p$

(2) $|a_n|_p < |a_N|_p$ for all $n > N$.

Then f has at most N zeros.

Proof. We will prove Strassman's Theorem using induction.
In the base $N = 0$ case, we will use contradiction by assuming that there exists a zero, that is there exists α such that

$$0 = f(\alpha) = \sum_{n=0}^{\infty} a_n \alpha^n.$$

So

$$-a_0 = \sum_{n=1}^{\infty} a_n \alpha^n$$

which gives us that

$$|a_0|_p = |\sum_{n=1}^{\infty} a_n \alpha^n|_p.$$

It follows that

$$|\sum_{n=1}^{\infty} a_n\alpha^n|_p \leq \max_{n\geq 1}|a_n\alpha^n|_p \leq \max_{n\geq 1}|a_n|_p.$$

The second inequality comes from the fact that $|\alpha|_p \leq 1$, since α is a p-adic integer. This contradicts the second condition we set on N, so we see that in the $N = 0$ case, f cannot have a zero.

For the inductive step, we assume this theorem holds for some $N-1$ and we will show that the N case holds. This will be done by factoring out a zero and then using our inductive assumption. If f has no zeros then we are done. Otherwise we denote the zero as α. Notice that

$$f(x) = f(x) - f(\alpha) = \sum_{n=0}^{\infty} a_n(x^n - \alpha^n) = (x-\alpha)\sum_{n=0}^{\infty}\sum_{j=0}^{n+1} a_n x^j \alpha^{n-1-j}.$$

Rearranging, we get that

$$f(x) = (x-\alpha)\sum_{j=0}^{\infty}\sum_{n=j+1}^{\infty} a_n x^j\alpha^{n-1-j} = (x-\alpha)\sum_{j=0}^{\infty}\sum_{k=0}^{\infty} a_{j+1+k}x^j\alpha^k.$$

where $k = n-1-j$. Define $b_j = \sum\limits_{k=0}^{\infty} a_{j+1+k}\alpha^k$ and $g(x) = \sum\limits_{j=0}^{\infty} b_j x^j$. Doing so allows us to write

$$f(x) = (x-\alpha)g(x).$$

We will now show that we can use our inductive assumption on $g(x)$. We will first show that $\lim\limits_{j\to\infty} b_j = 0$. From previous result, we see that

$$|b_j|_p \leq \max_{k\geq 0}|a_{j+1+k}\alpha^k|_p \leq \max_{k\geq 0}|a_{j+1+k}|_p.$$

Since $|a_n|_p \to 0$, it follows that $\max\limits_{k\geq 0}|a_{j+1+k}|_p \to 0$, so $\lim\limits_{j\to\infty} b_j = 0$.

Observe that for any $j \geq 0$, we have that

$$|b_j|_p \leq \max_{k\geq 0}|a_{j+1+k}|_p \leq |a_N|_p.$$

Furthermore,

$$|b_{N-1}|_p = |\sum_{k=0}^{\infty} a_{N+k}\alpha^k|_p = |a_N|_p.$$

This shows that $N-1$ satisfies the first condition. Now let $j > N-1$. Then

$$|b_j|_p \leq \max_{k\geq 0}|a_{j+1+k}|_p < |a_N|_p.$$

Then we see that $g(x)$ satisfies the conditions in our inductive assumption, so $g(x)$ has at most $N-1$ zeros. It follows that $f(x)$ has at most N zeros. □

We will finish by discussing a few corollaries of Strassman's Theorem.

Corollary 5.2. *Let $f(X) = \sum a_n X^n$ be a power series in $\mathbb{Z}_p[[X]]$ such that it converges on $\mathbb{Z}_p$ and it has zeros $\alpha_1, ..., \alpha_m \in \mathbb{Z}_p$. Then there exists $g(X) \in \mathbb{Z}_p[[X]]$ which converges on $\mathbb{Z}_p$ and has no zeros in $\mathbb{Z}_p$ such that*

$$f(X) = (X-\alpha_1)...(X-\alpha_m)g(X).$$

Proof. This corollary follows from the factoring process in the inductive step in the proof of Strassman's Theorem. First, we can factor α_1 and get that

$$f(X) = (X - \alpha_1)g_1(X),$$

where $g_1(X)$ has at most $m-1$ zeros. Continuing this process, we get that

$$f(X) = (X - \alpha_1)...(X - \alpha_m)g_m(X)$$

where $g_m(X)$ has no zeros. Then let $g(X) = g_m(X)$. □

Corollary 5.3. *Let $f(X)$ be a non-zero power series in $\mathbb{Z}_p[[X]]$ converging in $p^m\mathbb{Z}_p$ for some $m \in \mathbb{Z}$. Then $f(X)$ has finitely many zeros in $p^m\mathbb{Z}_p$.*

Proof. Define $g(X) = f(p^m X)$. Since $f(X)$ converges on $p^m\mathbb{Z}_p$, $g(X)$ converges on $\mathbb{Z}_p$. Suppose α is a zero of $f(X)$, then $p^{-m}\alpha$ is a zero of $g(X)$. By applying Strassman's Theorem to $g(X)$, we see that $g(X)$ has finitely many zeros, so $f(X)$ must also have finitely many zeros. □

Corollary 5.4. *Let $f(X), g(X)$ be power series in $\mathbb{Z}_p[[X]]$, such that both are non-zero and converge on $p^m\mathbb{Z}_p$ for some integer m. Suppose there exists infinitely many $\alpha \in p^m\mathbb{Z}_p$ such that $f(\alpha) = g(\alpha)$. Then $f(X) = g(X)$.*

Proof. Define $h(X)$ such that $h(X) = f(X) - g(X)$. Suppose $h(X)$ is nonzero. By Corollary 5.3, $h(X)$ has finitely many zeros. However, for each α, $h(\alpha) = 0$. This is a contradiction, so $h(X) = 0$. □

Corollary 5.5. *Let $f(X)$ be a power series in $\mathbb{Z}_p[[X]]$ such that $f(X)$ is nonzero, converges in $p^m\mathbb{Z}_p$ and is periodic with period $\tau \in p^m\mathbb{Z}_p$. Then $f(X)$ is constant.*

Proof. Since f is periodic, $f(\tau n) = f(0)$ for all integer n. Notice also that $\tau n \in p^m\mathbb{Z}_p$. By corollary 5.4, $f(X) = f(0)$ showing that $f(X)$ is constant. □

Acknowledgments

I would like to thank my mentors Billy Lee and Karl Schaefer. They have helped me discover this topic, suggest helpful readings and helped me with understanding along the way. I would also like to thank Professor Peter May for hosting the REU and providing me the opportunity to explore many interesting topics of mathematics.

References

[1] Andrew Baker. An Introduction to p-adic Numbers and p-adic Analysis. http://www.maths.gla.ac.uk/~ajb/dvi-ps/padicnotes.pdf

[2] Keith Conrad. Hensel's Lemma. http://www.math.uconn.edu/~kconrad/blurbs/gradnumthy/hensel.pdf

[3] Jan-Hendrik Evertse. P-adic Numbers. http://www.math.leidenuniv.nl/~evertse/dio2011-padic.pdf

[4] Hannah Hutter, May Szedlák, Philipp Wirth. Elementary Analysis in $\mathbb{Q}_p$. https://www2.math.ethz.ch/education/bachelor/seminars/hs2011/p-adic/report6.pdf