P-ADIC NUMBERS AND SOLVING P-ADIC EQUATIONS

AXEL G. R. TURNQUIST

Abstract. This paper provides a review of C. C. MacDuffee's article titled *The p-adic Numbers of Hensel* from 1938 and H. S. Thurston's article titled *The Solution of p-adic Equations*from 1943 published in the American Mathematical Monthly. The first section gives all the necessary background material for understanding the mathematics in both articles as well as a cursory introduction to p-adic numbers.

Contents

1. Background Material

1.1. **Norms.** We begin our introduction to p-adic numbers by a discussion of norms on **fields**. Mathematical fields are **Commutative Rings** that have multiplicative inverses for all elements. Commutative Rings are sets with endowed with two operations, addition and multiplication, defined to be commutative, associative, and closed. In addition, there exist additive and multiplicative identities [4]. Two main examples of fields that will be used in this paper are $\mathbb{Q}$ and $\mathbb{R}$. These both have multiplicative and additive inverses for each element. The multiplicative and additive identities are 1 and 0 respectively. It can be shown that the other properties of fields are also satisfied by $\mathbb{Q}$ and $\mathbb{R}$. Note that $\mathbb{Z}$ is not a field. We denote a generic field F. There are three conditions that have to be satisfied for a norm defined by $|\ |: F \to \mathbb{R}$ from a metric space F to the non-negative real numbers. The three conditions are as follows [5]:

(1)	$\lvert x\rvert = 0$	if and only if x = 0
(2)	$\lvert x+y\rvert \leq \lvert x\rvert + \lvert y\rvert$	(triangle inequality)
(3)	$\lvert xy\rvert = \lvert x\rvert\lvert y\rvert$	

We can begin to build up many norms in this way, one of them being the trivial norm:

$$|x| := \begin{cases} 0, & \text{if } x = 0; \\ 1, & \text{if } x \neq 0. \end{cases}$$

This satisfies the conditions of being a norm. Condition (1) is automatically satisfied. Condition (2) works for all three cases: $|x + 0| \leq |x| + |0|$ because $1 = 1, |x + x| \leq |x| + |x|$ because $1 < 2, |0 + 0| \leq |0| + |0|$ because $0 = 0$. To prevent too much confusion from abstraction, it serves to be instructive to cook up a specific example. Define deg(a) to be the degree of a polynomial. If we examine the constant polynomials we define,

$$deg(a) = -\infty \text{ if } a = 0; \quad deg(a) = 0 \text{ otherwise,}$$

If we multiply a polynomial by 0, then it becomes 0. Likewise, adding $-\infty$ to 0 yields $-\infty$. We can construct a norm that agrees with our notions of the degree of polynomials:

$$|a| := \rho^d(a) \text{ where } \rho \leq 1.$$

It can be checked that this is equivalent to the trivial norm, since $\rho^{-\infty} = 0$ and $\rho^0 = 1$. A norm *induces* a topology on a field F by a metric $(x, y) \to |x - y|$ [5]. We are already aware of another norm, the absolute value, which induces a distance metric on $\mathbb{Q}$ and $\mathbb{R}$. Are there any others?

1.2. **The p-adic Norm.** The common way in which we write number is by their decimal expansion in a series of base ten. These are written in shorthand by a sequence of integers $\ldots a_m a_{m-1} \ldots a_1 a_0.$, where the a_j terminate to the left, i.e. $\exists N$ such that $a_j = 0\ \forall j > N$ and $0 \leq a_j < 10$. If we lift the restriction that all the a_j are 0 beyond a certain point, we denote these as $\mathbb{Z}_{10}$. This is a Commutative Ring

[7]. Multiplication of elements is defined as the multiplication of series representing those elements. Let $a = \sum_{i=0}^{\infty} c_i 10^i$ and $b = \sum_{i=0}^{\infty} b_i 10^i$. Then,

$$a \cdot b = \sum_{i=0}^{\infty} c_i 10^i \cdot \sum_{i=0}^{\infty} b_i 10^i$$

Addition is defined by adding term by term and if $a_i \geq 10$ then the digit is carried over to a higher term. In other words, addition and multiplication are the same as the way that is taught in elementary school. More specifically, $\mathbb{Z}_{10}$ is not an **integral domain** since it has a **zero divisor**, a nonzero element that can be multiplied by another element to yield zero [4], since, for example, the product [7],

$$\begin{array}{r} (\ldots 10112) \\ \times (\ldots 03125) \\ \hline (\ldots 00000) \end{array}$$

is identically zero and defined as the zero element. An integral domain is a ring which does not have any two elements that multiply to produce the zero element, i.e. there are no zero divisors. For example, if $\mathbb{Z}_p$ where p is a prime number, then $\mathbb{Z}_p$ is an integral domain. Suppose we denote $x_1 = \sum_{i=0}^{\infty} a_{j_1} p^j$, $x_2 = \sum_{i=0}^{\infty} a_{j_2} p^j$, and in general $x_i = \sum_{i=0}^{\infty} a_{j_i} p^j$. The infinite sum

$$\sum_{i=1}^{\infty} x_i$$

converges to a single value when for each j there exists an N_j such that $a_{j_i} = 0 \ \forall \ i > N_i$. This amounts to having only a finite number of terms for each power of p in the summation. For example, the series

$$\sum_{i=0}^{\infty} p^i$$

converges to $\ldots p^m \ p^{m-1} \ldots p^2 \ p \ 1$.
What kind of convergence is this? This clearly not convergence in the absolute norm. To let us understand that, we introduce $ord_p(x)$, which equals the highest power of p that divides $x \in \mathbb{Q}$. For example, $ord_2(96) = 5$, because 2^5 divides 96. In line with our notation of $\mathbb{Z}_p$ that we developed earlier, we can also define $ord_p(x)$ in a convenient way [7]:

$$ord_p(x) := \begin{cases} \infty, & \text{if } a_i = 0 \ \forall i; \\ min(s : a_s \neq 0), & \text{otherwise.} \end{cases}$$

And we define a new norm, denoted $|\ |_p$ by [5],

$$|\ |_p := \begin{cases} 0, & \text{if } a_i = 0 \ \forall i; \\ p^{-ord_p(x)}, & \text{otherwise.} \end{cases}$$

Note, this has convergence in the sense described earlier; this will be elaborated on later. First, $|0|_p = 0$, so Condition (1) of the definition of a norm is satisfied. Moreover, Condition (3), which implies $|a \cdot b|_p = |a|_p |b|_p$ is satisfied trivially when either a or b is zero, but if they are not zero, then $|a \cdot b|_p = p^{-ord_p(ab)} =$

$p^{-(ord_p(a)+ord_p(b))} = p^{-ord_p(a)}p^{-ord_p(b)} = |a|_p|b|_p$. Another consequence of this norm is the **strong triangle inequality** [5]:

$$|x+y|_p \leq max(|x|_p, |y|_p).$$

Note that triangle inequality is automatically satisfied, since $max(|x|_p, |y|_p) \leq |x|_p + y_p$. Returning back to the example with degrees of polynomials, this time lifting the restriction that they be constant, we find a familiar example that satisfies the strong triangle inequality [7]:

$$deg(f+g) \leq max(deg(f), deg(g)).$$

The strong triangle inequality has various intuitively surprising and interesting consequences with regards to the metric that it induces. Let $|y| > |x|$. We use the strong triangle inequality to prove that $|x-y| = |y|$ [5]. First,

$$|x-y| \leq max(|x|, |y|)|x-y| \leq |y|.$$

We can establish the converse inequality in the following way:

$$|y| = |x-x+y| \leq max(|x|, |x-y|) \leq |x-y|.$$

Hence,

$$|x-y| = |y|.$$

Thus, we are confronted with what Neal Koblitz refers to as the **isosceles triangle principle**, meaning that the longest two sides are always equivalent in the metric induced by a norm that satisfies the strong triangle inequality. Another interesting consequence of the strong triangle inequality is found by the following argument. Define a "disk" D by [5]:

$$D(a,r) = \{x \in F : |x-a|_p < r\},$$

Then

$$|x-b| = |(x-a)+(a-b)| \leq max((x-a),(a-b)) < r$$

Hence, the wild conclusion is that every point is at the center of the disk!

1.3. **Non-Archimedean Norms.** It turns out that norms on a field F that are **non-Archimedean** satisfy the strong triangle inequality. Three equivalent definitions of non-Archimedean norms are as follows. A norm is non-Archimedean if it satisfies [5] [6] [7]:

(1) the strong triangle inequality

(2) $|n|$ is bounded

(3) $|n| \leq 1$ for every integer n

The last condition is straightforward to prove by induction [6]. We begin with the base case:

$$|1| = 1 \leq 1$$

The equality follows from the definition (3) of the norms and since norms map to the nonzero reals.

$$|1| = |1^2| = |\pm 1||\pm 1| \ \Rightarrow |\pm 1| = 1.$$

Next, suppose that $|k| \leq 1 \ \forall \ k \in \{1, \ldots, n-1\}$. Then,

$$|n| = |(n-1)+1| \leq max(|n-1|, 1) = 1.$$

This can be used to show the strong triangle inequality via the binomial expansion [6]:

$$|(x+y)^n| = |\sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k}| \leq \sum_{k=0}^{n} |x|^k |y|^{n-k} \leq (n+1)\ max(|x|, |y|)^n$$

$$|x+y| \leq \lim_{n\to\infty} \sqrt[n]{n+1}\ max(|x|, |y|) = max(|x|, |y|).$$

This means that the absolute value is an Archimedean norm, while the trivial norm and the p-adic norm are non-Archimedean.

1.4. **Completion.** The Completion Theorem describes the way in which a metric space can be **completed** and what completion means.

The Completion Theorem [6]
Every metric space M, and in our context fields F, can be completed, i.e. there exists a metric space defined as $(\hat{M}, D)$ such that,

(1) $\hat{M}$ is complete with respect to the metric D,

(2) $\hat{M}$ contains a subset $\hat{M}_0$ isometric to M,

(3) $\hat{M}_0$ is dense in $\hat{M}$.

What is the completion for $\mathbb{Q}$ with respect to the absolute value? The answer is $\mathbb{R}$. One of the standard way of building up the reals is to examine the Cauchy sequences of rational numbers [5]. Recall that a sequence is Cauchy if,

$$\text{fix } \epsilon > 0.\ \exists N \text{ s. t. } \forall\ n, m > N,$$

$$|a_m - a_n| < \epsilon$$

All rationals are periodic in $\mathbb{R}$ in decimal expansion. This can be proven by expanding in a geometric sequence. For that same reason, any rational numbers in their expansion in a base are periodic, including the p-adic expansions. We can therefore construct irrational numbers by producing sequences that are aperiodic in its decimal form. For example the sequences [6],

$$0.101, 0.101101, 0.1011011101, \ldots$$

is Cauchy convergent to an irrational number, since the digits are aperiodic. Of course, π is also irrational, because it is aperiodic. Hence, we define the reals as the set of all equivalence classes of Cauchy sequences of rational numbers. This "fills in the holes" because rationals converge to every irrational. Can we do the same thing for $\mathbb{Q}$ using the p-adic norm?

1.5. **Algebraic Definition of Completion.** Probably the cleanest way of defining the p-adic numbers, $\mathbb{Q}_p$ that result from this completion is using commutative ring theory. Define the Cauchy sequences as a Commutative Ring R in the sense that they can be added, subtracted, multiplied, and divided term by term. It follows that if $\{a_n\}$ and $\{b_n\}$ are Cauchy sequences, then $\{a_n + b_n\}$ and $\{a_n \cdot b_n\}$ are also Cauchy. Note then that the additive and multiplicative identities can be defined in the following way:

$$\hat{0} = \{0, 0, 0, \dots\};\ \hat{1} = \{1, 1, 1, \dots\};$$

In the context of commutative ring theory then, there are zero divisors, since any two Cauchy sequences with mutually exclusive zero entries have a product which is equal to $\hat{0}$. Also note that sequences defined by [6],

$$\hat{a} = \{a, a, a, \dots\};$$

have a direct correspondence with their values in $\mathbb{Q}$. This suggests that there is a **subring** of R that is isomorphic to the rational numbers, meaning, briefly, a smaller ring which exhibits the characteristics of a ring and consists only of elements from the larger ring [4].

Another subset of this ring which is of interest is the set N of **null sequences**, those Cauchy sequences which have a zero limit [6]. Or, equivalently, those that satisfy the following: fix $\epsilon > 0$. $\exists\ N \geq 0\ s.t.\ \forall\ n \geq N, |a_n| < \epsilon$. It follows that this set is a ring **ideal**, which in this context means that if $a \in N$ and $b \in R$, then $ab \in N$. If we define a ring homomorphism $f : R \to \hat{R}$ defined by $f := \{a_n\} \to \lim_{n\to\infty} a_n$, then we have a result from the **First Ring Isomorphism Theorem** which states that the new ring $\hat{R}$ is isomorphic to the **Quotient Ring** R/N if the **kernel** of f, the values that f takes to 0, is equivalent to the set N [4]. Since the elements in N are in bijective correspondence with the set $\{\{a_n\} : f(a_n) = 0\}$ by construction, the First Isomorphism Theorem thus follows. What is the resulting ring R/N? It is the ring of equivalence classes of Cauchy sequences because it is isomorphic to R'.

We prove now that it is a field [6]. Let $\{a_n\} \in R/N$, i.e. it is an equivalence class of an element in R. Hence, $\exists\ N \in \mathbb{N}, c$ positive real number such that $|a_n| > c\ \forall\ n > N$, because $\{a_n\}$ is *not* a null sequence. Define another sequence $\{a_n^*\}$ by,

$$\{a_n^*\} := \begin{cases} 0 & 1 \leq n \leq N-1 \\ \frac{1}{a_n} & n \geq N. \end{cases}$$

Therefore, since

$$\hat{1} - \{a_n a_n^*\} = \{1, 1, 1, \dots\} - \{0, \dots, 0, 1, 1, 1, \dots\} = \{-1, \dots, -1, 0, 0, 0, \dots\},$$

Then the product $\{a_n a_n^*\} \equiv \hat{1}$ and thus every Cauchy sequence in R/N has an inverse and consequently R/N is a field. With the p-adic metric, we have produced a field from the completion of the rationals!

1.6. **The p-adic Numbers.** The p-adic numbers are then, in the base-p expansion we used before, expressed in the following way,

$$\dots a_m a_{m-1} \dots a_1 a_0 . a_{-1} a_{-2} \dots$$

Where $a_{-n} = 0$ for large n [7]. If $a_{-n} = 0 \ \forall \ n > 0$, then these are the p-adic integers $\mathbb{Z}_p$ that we defined previously. Note, that since the the terms terminate to the right, then the values of the p-adic norm are:

$$\{0\} \cup \{p^n : n \in \mathbb{Z}\}$$

The p-adic numbers written in this way can be shown to be Cauchy [6]. Suppose that the lowest nonzero term is a_{-m}. Then,

$$|\sum_{-m}^{k} d_i p^i - \sum_{-m}^{n} d_i p^i|_p = |\sum_{n+1}^{k} d_i p^i|_p$$

$$\leq max(\{|d_i p^i|_p\}) \leq p^{-N}$$

Since $0 \leq d_i \leq p$ so $|d_i| \leq 1$. The following theorem requires considerable proof, which is omitted. It basically asserts that the way we have been writing p-adic numbers up to this point is valid.

Uniqueness Theorem [6]
Each p-adic number can be uniquely written as the sum of a convergent series of the form

$$\sum_{-\infty}^{\infty} a_n p^n \qquad \text{where } a_{-n} = 0 \text{ for large } n \text{ and } 0 \leq a_n \leq p$$

Note, that this uniqueness does not work for decimal expansions. For example,

$$1.\bar{0} = 0.\bar{9}$$

These are two unique ways of writing the number congruent to 1. Rational numbers can be written in the p-adic expansion, and are periodic eventually to the left (instead of the right for the standard decimal expansion). For example [6]:

$$\frac{1}{2} = \ldots(\frac{p-1}{2})(\frac{p-1}{2})(\frac{p+1}{2}).000\ldots$$

This can be seen to be true by multiplying out by all terms by 2. Negative values also have an infinite p-adic expansion. For example [6],

$$-1 = \ldots(p-1)(p-1)(p-1).000\ldots$$

To see this, add 1,

$$0 = \ldots(p{-}1)(p{-}1)(p).000\cdots = \ldots(p{-}1)(p)0.000\cdots = \ldots(p)00.000\cdots = \ldots 000.000\ldots$$

Because p is prime, it also follows that no p-adic integers solve the equation $x^2 = p$. To solve this equation, we would have to find a p-adic number x that would square to equal $\ldots 0010.000\ldots$. Let $x = \ldots a_2 a_1 a_0.000\ldots$. To solve the equation, a necessary condition is $a_0^2 \equiv (mod\ p)$. However, this has no solution because a prime is not a square number. The question remains whether or not p-adic numbers are the whole story as far as norms go.

1.7. **Ostrowski's Theorem.** The following theorem establishes the classifications of norms on the rationals. It has profound consequences.

Ostrowski's Theorem [7]
Each non-trivial norm on the field of the rational numbers is equivalent either to the absolute value function or to some p-adic norm.

Lemma [7]

Two norms on a field F are *equivalent* if they induce the same topology on F. More concretely, if $|\ |_1$ and $|\ |_2$ are equivalent norms, then there exists a positive real number c such that $|\ |_1 = |\ |_2^c$.

Proof of Ostrowski's Theorem We first that the absolute value is equivalent to all nontrivial Archimedean norms [5], then we will prove that the p-adic norm is equivalent to all nontrivial non-Archimedean norms [7]. Suppose there exists a positive integer n such that $|n| > 1$. Then this is an Archimedean norm, since it is the converse of a non-Archimedean norm, where $|n| < 1$. Let n_0 be the least such n. Hence, $|n_0| = n_0^\alpha$ for some positive real number α since $|n_0| > 1$. We expand n in the base n_0:

$$n = a_0 + a_1 n_0 + \cdots + a_s n_0^s \qquad 0 \leq a_i < n_0, a_s \neq 0.$$

Therefore,

$$\begin{aligned}
|n| &\leq |a_0| + |a_1 n_0| + \cdots + |a_s n_0^s| \\
&= |a_0| + |a_1| n_0^\alpha + \cdots + |a_s| n_0^{s\alpha} \\
&\leq 1 + n_0^\alpha + \cdots + n_0^{s\alpha} && \text{since } |a_i| < 1 \\
&= n_0^{s\alpha}(1 + n_0^{-\alpha} + \cdots + n_0^{-s\alpha}) \\
&\leq n^\alpha (\sum_{i=0}^{\infty} (\frac{1}{n_0^\alpha})^i) && \text{since } n_0^{s\alpha} \leq n^\alpha \leq n_0^{(s+1)\alpha} \\
&= Cn^\alpha
\end{aligned}$$

Replace n with n^N for any large N and repeat the argument,

$$|n^N| \leq Cn^{N\alpha}$$

Taking the Nth root and then passing the limit as $N \to \infty$ yields:

$$|n| \leq n^\alpha.$$

To prove the inequality in the other direction, we proceed as follows:

$$\begin{aligned}
&|n_0^{s+1}| \leq |n + n_0^{s+1} - n| \leq |n| + |n_0^{s+1} - 1| \\
&\Rightarrow |n| \geq n_0^{(s+1)\alpha} - (n_0^{s+1} - n)^{alpha} \\
&\qquad \geq n_0^{(s+1)\alpha} - (n_0^{s+1} - n_0^s)^\alpha \\
&\qquad = n_0^{(s+1)\alpha}(1 - (1 - \frac{1}{n_0})^\alpha) \\
&\qquad \geq C' n^\alpha.
\end{aligned}$$

The argument proceeds by following the same procedure as above by replacing n by n^N and performing the same trick to yield $|n| \geq n^\alpha$. Hence, we reach the conclusion, $|n| = n^\alpha$. The argument can be generalized to rational numbers instead of integers, leading to the conclusion

$$|x| = |x|^\alpha \text{ for some } \alpha$$

Since the norm goes to the positive reals. We can see therefore, that any Archimedean norm is equivalent to the absolute value. Suppose now that the norm is non-Archimedean. We look at the set

$$\{n \in \mathbb{N} : |n| < 1\}.$$

This set is nonempty. Let p be the minimal element. We will show that p is prime. If $p = ab$ for some integers a, b, then $|a|, |b| = 1$ since a and b are less than p. If there is an integer q such that $q = ap + r$, where $a \in 0, 1, 2, \ldots$, and $1 \leq r < p$, then $|r| = 1$ and $|ap| = |a||p| \leq |p| < 1$. Hence,

$$1 = |r| \leq max(|ap + r|, |-ap|) = max(|q|, |ap|) = |q|, \qquad \text{since —ap— ¡ } 1$$

And therefore $|q| \geq 1$, so $|q| = 1$ since q is an integer, and the non-Archimedean norm of all integers are less than 1. Hence, all n in the set above are divided by p. More concretely,

$$\begin{aligned} |n| &= |p^{ord_p(n)}| = |p|^{ord_p(n)} \\ &= \frac{1}{p^{ord_p(n)}}^{-\log_p |p|} \\ &= |n|_p^c \end{aligned}$$

Hence, these norms are equivalent. Ostrowski's Theorem coupled with the Completion Theorem gives a list of all the possible completions of $\mathbb{Q}$. The absolute value and its equivalent Archimedean norms produce $\mathbb{R}$, and can be extended, via i, to produce $\mathbb{C}$, which is algebraically complete. The trivial norm produces a discrete topology. The p-adic norm takes $\mathbb{Q}$ to $\mathbb{Q}_ı$, the p-adic numbers. These represent the complete classification of completions of $\mathbb{Q}$. However, as we noted before, there exists no square root of p in $\mathbb{Q}_ı$. So what do we do? In the same way as we extended $\mathbb{R}$ to $\mathbb{C}$, we can extend $\mathbb{Q}$to a field called $\bar{\mathbb{Q}}_ı$. It turns out that even though this is algebraically closed, it is not complete, however, and after completing $\bar{\mathbb{Q}}_ı$ we get Ω [5]. How to obtain Ω will not be elaborated upon here.

2. Introduction to Solving p-adic Equations

2.1. **Existence of a Root.** We revisit the question of solving algebraic equations in the field of p-adic numbers. There are some strange results that we have seen that conflict with our intuition of series expansions. For example, revisiting the p-adic expansion from earlier of -1, we see:

$$-1 = \ldots(p-1)(p-1)(p-1).000\ldots$$

which appears even stranger when written as a series expansion (which it is implicitly in the above condensed form). For concreteness, let us choose $p = 7$. The non-intuitive result is:

$$-1 = 6 + 6 \cdot 7 + 6 \cdot 7^2 + 6 \cdot 7^3 + \ldots$$

As MacDuffee comically puts it, in his 1938 article titled *The p-adic Numbers of Hensel*, "One cannot blame a respectable mathematician for looking twice at [such an] equation." [1] Now we develop some tools using **modular arithmetic** in order to be able to solve for equations p-adic integers, something which we noted was impossible for $x^2 = p$. In general, since we have expanded our p-adic number in terms of base-p, we can say that an element α of $\mathbb{Q}_l$ is congruent to its series expansion $a_0 + a_1p + \cdots + a_{i-1}p^{i-1}(mod\ p^i)$ [1].

From now on, the prime p is fixed. Given a polynomial with rational coefficients $f(x)$, is it possible to find a p-adic number α such that $f(\alpha) = 0$? This amounts to showing that $f \equiv 0\ (mod\ p^i)\ \forall\ i \in \mathbb{N}$. If we already have a solution $f(a_0) \equiv 0\ (mod\ p)$, then we use an iterative method to derive the results in general [1]. We assume a solution to the next iteration: $a_0 + a_1p$. Hence, defining the polynomial function $f = \sum_{i=0}^{\infty} c_i$, we get

$$\begin{aligned}
f(a_0 + a_1p) &= \sum_{i=0}^{\infty} c_i(a_0 + a_1p)^i \\
&= \sum_{i=0}^{\infty}(\binom{i}{0}c_i a_0^i + \binom{i}{1}c_i a_0^{i-1}a_1p + \text{higher order terms}) \\
&= \sum_{i=0}^{\infty}(c_i a_0^i + ic_i a_0^{i-1}a_1p)(mod\ p^2) \\
&= f(a_0) + f'(a_0)a_1p(mod\ p^2) \\
&= h_0p + f'(a_0)a_1p(mod\ p^2) \\
&= h_0 + f'(a_0)a_1(mod\ p).
\end{aligned}$$

Where h_0 is an integer $0 \leq h_0 < p$ because $f(a_0) \equiv 0(mod\ p)$. Extrapolating this result to higher order terms, we obtain the general result, where α_{n-1} is the p-adic series expansion of α up to its a_{n-1} term [1].

$$a_n f'(\alpha_{n-1}) + h_{n-1} \equiv 0(mod\ p). \tag{4}$$

Where $f(\alpha_{n-1}) \equiv h_{n-1}p^n(mod\ p^{n+1})$. The result being that a solution exists for $h_n \neq 0$ as long as $f'(\alpha_{n-1}) \neq 0$. Otherwise, the uniqueness of h_n would fail. One further simplification can be made [3]. We note that $\alpha_{n-1} = a_0 + pq$, where $q = a_1 + a_2p + \cdots + a_{n-1}p^{n-2}$ is an integer. Thus, proceeding in a process similar to the one above, we obtain the result:

$$f'(\alpha_{n-1}) = f'(a_0) + f''(a_0)pq + \dots$$

$$f'(\alpha_{n-1}) \equiv f'(a_0)(mod\ p)$$

Thus reducing Equation (4) to:

$$a_n f'(a_0) + h_{n-1} \equiv 0 \tag{5}$$

Summarily, we have that the equation $f(x) = 0$ will have a solution in $\mathbb{Q}_p$ if $f(x) \equiv 0(mod\ p)$ has a solution $x = a_0$ such that $f'(a_0) \neq 0(mod\ p)$ [3].

We use an example to illustrate the abstract derivation above [1]. Consider solving for the square root of 7 in its 3-adic expansion. In other words, we solve the equation $f(x) = x^2 - 7$ for a 3-adic number x. The first step is to come up with an $a_0^2 \equiv 7(mod\ 3)$. The solutions are $a_0 = 1, 2$. We choose $a_0 = 1$ and apply Equation (5). $f(a_0) = -6 = 3(mod\ 9) = 3 \cdot h_0(mod\ 9)$, so $h_0 \equiv 1(mod\ 3)$; $f'(a_0) = 2(mod\ 3)$. Equation (4) becomes:

$$2a_1 + 1 \equiv 0(mod\ 3) \Rightarrow a_1 = 1; \alpha_1 = 1 + 1 \cdot 3 = 4.$$

So, for our next iteration, we get from Equation (4), that $f'(a_0) \equiv 2(mod\ 3)$ as before, $f(\alpha_1) \equiv 9(mod\ 27)$ so $9 \cdot h_1(mod\ 27) \equiv 3$ implies that $h_1 \equiv 1(mod\ 3)$. Solving for a_2 gives $a_2 = 1$. Continuing in this way, we can solve uniquely for α_n provided that the derivative is nonzero. Continuing this process yields:

$$\alpha_4 = 1 + 1 \cdot 3 + 1 \cdot 3^2 + 0 \cdot 3^3 + 2 \cdot 3^4 + \dots$$

This shows the existence of at least *one* solution to the roots of the polynomial $f(x)$, but does not make any assertions about the other zeroes. Further questions, based on the questions raised by the MacDuffee article are pursued in H. S. Thurston's 1943 article, *The Solution of p-adic Equations.*

2.2. **Thurston's Method.** H. S. Thurston relies on a technique of successive approximations using a "chain of equations" to analyze some marginal cases that cannot be dealt with with the above technique of only analyzing $f(x)$. Let

$$f(x) = x^n + c_{n-1}x^{n-1} + \dots + c_1 x + c_0$$

The chain of equations are:

$$f(x) = 0, F_1(x) = 0, F_2(x) = 0, \dots, F_i(x) = 0,$$

where the coefficients of the solution α are determined successively by each $F_i(x)$. Given a solution $f(\alpha) = 0$, then if we write $\alpha = a_0 + \alpha_1 p$, where $\alpha_1 = a_1 + a_2 p + a_3 p^2 + \dots$,

$$\begin{aligned} f(a_0 + \alpha_1 p) &= (a_0 + \alpha_1 p)^n + c_{n-1}(a_0 + \alpha_1 p)^{n-1} + \dots + c_1(a_0 + \alpha_1 p) + c_0 \\ &= \sum_{j=1}^{n} c_j (a_0 + \alpha_1 p)^j \\ &= \sum_{j=1}^{n} c_j (a_0^j + j a_0^{j-1} \alpha_1 p + \text{higher order terms}) \\ &= f(a_0) + f'(a_0)\alpha_1 p + \dots + \alpha_1^n p^n = 0. \end{aligned}$$

Letting $f(a_0) = k_0 p$. Then we define,

$$F_1(x) = k_0 + f'(a_0)x + \dots + x^n p^{p-1} = 0$$

So we can see that α_1, and by construction α_i is a solution to $F_i(x) = 0$, because

$$f(\alpha) = pF_1(\alpha_1) = p^2 F_2(\alpha_2) = \dots = p^k F_k(\alpha_k)$$

There are are two cases that cannot be solved by methods in MacDuffee's paper and are treated in Thurston's paper, the first is where $F_i = F_j$ for all $j > i$. The

second case is where $f(a_0) \equiv f'(a_0) \equiv 0$, and therefore $F_i(a_i) \equiv F_i'(a_i) \equiv 0(mod\ p)$ for all i. We first address the simpler case where $F_1(x) = f(x)$. In this case,

$$F_1(x) = k_0 + f'(a_0)x + \cdots + x^n p^{p-1} = f(x)$$

Then $f(a_0 + px) = p^n F_1(x)$, since $f(x)$ is a *monic* polynomial, meaning that the leading coefficient is 1. Solving for a coefficient of c_{n-k} can be calculated through induction. Here I have produced the induction which gives rise to the results quoted in the Thurston paper. First, we check the base case:

$$\begin{aligned} c_{n-1} &= (\frac{1}{p^n})(c_{n-1}p^{n-1} + na_0p^{n-1}) \\ &= \frac{c_{n-1}}{p} + \frac{na_0}{p} \\ &= \frac{na_0}{p-1} \end{aligned}$$

Solving for c_{n-2}, the base case:

$$\begin{aligned} c_{n-2} &= (\frac{1}{p^n})(c_{n-2}p^{n-2}) + c_{n-1}(n-1)a_0p^{p-2} + \binom{n}{2}a_0^2p^{p-2}) \\ c_{n-2}(p^2-1) &= c_{n-1}(n-1)a_0 + \binom{n}{2}a_0^2 \\ c_{n-2}(p^2-1) &= (c_{n-1})^2\binom{n}{2}\frac{2(n-1)a_0(p-1)}{a_0n^2(n-1)} + (c_{n-1})^2\binom{n}{2}\frac{(p-1)^2a_0^2}{n^2a_0^2} \\ c_{n-2}(p^2-1) &= \binom{n}{2}(\frac{c_{n-1}}{n})^2(2(p-1) + (p-1)^2) \\ c_{n-2} &= \binom{n}{2}(\frac{c_{n-1}}{n})^2(\frac{2p-2+p^2-2p+1}{p^2-1}) \\ c_{n-2} &= \binom{n}{2}(\frac{c_{n-1}}{n})^2 \end{aligned}$$

Now assume:

$$c_n = \binom{n}{k}(\frac{a_0}{p-1})^k$$

We induct on the index k:

$$\begin{aligned}
c_{n-(k+1)} &= \frac{1}{p^n}(c_{n-(k+1)}p^{n-(k+1)} + \binom{n-k}{1}a_0 c_{n-k}p^{n-(k+1)} + \cdots + \\
&\quad \binom{n-1}{k}a_0^k c_{n-1}p^{n-(k+1)} + \binom{n}{k+1}a_0^{k+1}p^{n-(k+1)}) \\
c_{n-(k+1)}(p^{k+1}-1) &= \sum_{j=1}^{k+1} c_{n-(k-j+1)}\binom{n-(k-j+1)}{j}a_0^j \\
&= \sum_{j=1}^{k+1}\binom{n}{k-j+1}(\frac{a_0}{p-1})^{k-j+1}\binom{n-(k-j+1)}{j}a_0^j \\
&= \sum_{j=1}^{k+1}\frac{n!}{(k-j+1)!(n-k-1)!j!}\frac{a_0^{k+1}}{(p-1)^{k-j+1}} \\
&= \binom{n}{k+1}(a_0^{k+1})\sum_{j=1}^{k+1}\frac{(k+1)!}{(k-j+1)!j!(p-1)^{k-j+1}} \\
&= \binom{n}{k+1}(\frac{a_0}{p-1})^{k+1}\sum_{j=1}^{k+1}\binom{k+1}{j}(p-1)^j \\
&= \binom{n}{k+1}(\frac{a_0}{p-1})^{k+1}(((p-1)+1)^{k+1}-1) \\
&= \binom{n}{k+1}(\frac{a_0}{p-1})^{k+1}(p^{k+1}-1)
\end{aligned}$$

because the binomial expansion runs from index 0 to $k+1$, while this ran from 1 to $k+1$, hence the extra -1 term. Thus, we get the result cited in Thurston's paper:

$$c_{n-(k+1)} = \binom{n}{k+1}(\frac{a_0}{p-1})^{k+1}$$

The coefficients are integral, and since $0 \leq a_0 < p$, it follows that $a_0 = 0$, or $p-1$. This means that $f(x) = x^n$ when $a_0 = 0$ or $f(x) = (1+x)^n$ when $a_0 = p-1$. Thus, if $f(x) = F_1(x)$, then we get a fairly simple expression for how to solve the polynomial. This can be generalized to say that if $F_i(x) = F_j(x)$ for every $i > j$, then $F_j = (x+1)^n$ or $F_j(x) = x^n$ [3].

For there to exist such an $F_j(x)$, then a necessary and sufficient condition for $F_j(x) = x^n$ or $F_j(x) = (1+x)^n$ is that $f(x) = (x-a)^n$ or $f(x) = (x+a)^n$, respectively. The derivation behind this is outlined in Thurston's paper and will not be reproduced here.

The second case, where $f(a_0) \equiv f'(a_0) \equiv 0$, and $F_i(a_i) \equiv F_i'(a_i) \equiv 0(mod\ p)$ proceeds by first assuming that $f(x)$ has no multiple roots. If α were a multiple root of $f(x)$, then Thurston asserts that $f'(x)$ would have a multiple root of order n. This is because $f(x)$ could be written as follows:

$$f(x) = (x-\alpha)^n g(x)$$

And its derivative would be:

$$f'(x) = (x-\alpha)^n g'(x) + n(x-\alpha)^{n-1}g(x)$$

So α would still be a root of $f'(x)$ and thus $F_i(\alpha_i) = F_i'(\alpha_i) = 0$. If we assume that $f(x)$ has no multiple roots, but $f(a_0) \equiv f'(a_0) \equiv 0$, then $f(a_0 + a_1 p) \equiv 0(mod\ p^2)$ since the first two terms in the expansion are $f(a_0) + f'(a_0)a_1 p = 0$. Since the first two terms have no reliance on a_1, we can replace a_1 by x and write that $f(a_0 + xp) \equiv 0(mod\ p^2)$. If we write $f(a_0 + xp) = p^{\beta_1} F_1(x)$, where $\beta_1 = n$ in the first case above, we can see that $\beta_1 \geq 2$, because since $f(a_0 + xp) \equiv 0(mod\ p^2)$ and $f(x)$ is monic, we can factor out at least p^{β_1}, where $\beta_1 \geq 2$. Taking the derivative of $f(a_0 + xp) = p^{\beta_1} F_1(x)$, we get,

$$f'(a_0 + xp) \cdot p = p^{\beta_1} F_1(x)$$

Hence, plugging in a_1 for x, we get,

$$f'(a_0 + a_1 p) = p^{\beta_1 - 1} F_1(a_1).$$

By the assumption above that $F_i(a_i) \equiv F_i'(a_i) \equiv 0(mod\, p)$, then $F'(a_1) \equiv 0(mod\, p)$, so $f'(a_0 + a_1 p) \equiv 0(mod\ p^{\beta_1}$. This means that $a_0 + a_1 p$ is a multiple root of $f(x) \equiv 0(mod\ p^{\beta_1})$. If we define $F_1(x)(a_1 + xp) = p^{\beta_2} F_2(x)$, then an identical process yields [3]:

$$f'(a_0 + a_1 p + a_2 p^2) \equiv 0(mod\ p^{\beta_1 + \beta_2 - 1}).$$

Meaning that $a_0 + a_1 p + a_2 p^2$ is a multiple root of $f(x) \equiv 0(mod\ p^{\beta_1 + \beta_2 - 1})$. By induction, the process yields that $a_0 + a_1 p + a_2 p^2 + \ldots$ is a multiple root of $f(x) = 0$, which is a contradiction to the hypothesis. This final result tells us that either there is no solution, or if multiple roots have been eliminated, then at some finite value m, $F_m(a_m) \equiv 0$, but $F_m'(a_m) \neq 0(mod\ p)$. This results in the striking conclusion that it is possible to solve for all of the possible simple (non multiple) roots in a finite number of steps. The process is as follows if there are no multiple roots: first, find a solution a_0 to $f(x) \equiv 0(mod\, p)$. Then find a solution a_1 to $F_1(x) \equiv 0(mod\, p)$. Proceed in this way finding solutions a_i to $F_i(x) \equiv 0(mod\, p)$ until either there is no solution, or if $F_i'(x) \neq 0(mod\ p)$ then this indicates the existence and uniqueness of a solution.

References

[1] C. C. MacDuffee, University of Wisconsin *The p-adic Numbers of Hensel* American Mathematical Monthly, Vol. 45, No. 8, pp. 500-508, 1938.

[2] Fernando Q. Gouvêa, *p-adic Numbers: An Introduction*, Springer-Verlag, New York, NY, 1993.

[3] H. S. Thurston, University of Alabama *The Solution of p-adic Equations* American Mathematical Monthly, Vol. 50, No. 3, pp. 142-148, 1943.

[4] Michael Artin, *Algebra* Pearson Education, Inc., Boston, MA, 2011.

[5] Neal Koblitz *p-adic Numbers, p-adic Analysis, and Zeta-Functions* Springer-Verlag, New York, NY, 1977.

[6] Svetlana Katok, *p-adic Analysis Compared with Real* American Mathematical Society, 2007.

[7] W. H. Schikhof, *Ultrametric Calculus* Cambridge University Press, Cambridge, UK, 1984.