Theory of p-adic Numbers and Solving p-adic Equations

by
Ankan Kar [1]
Bachelor of Mathematics(Honours)
Indian Statistical Institute, Bangalore

Course: Writing of Mathematics
Instrcutor: Prof. B. Sury

[1] Homepage: https://ankankar-zargon.github.io

December 2020

Introduction to p-adic Numbers

In mathematics, the p-adic number system for any prime number p extends the ordinary arithmetic of the rational numbers in a different way from the extension of the rational number system to the real and complex number systems. The extension is achieved by an alternative interpretation of the concept of “closeness” or absolute value. In particular, two p-adic numbers are considered to be close when their difference is divisible by a high power of p: the higher the power, the closer they are. This property enables p-adic numbers to encode congruence information in a way that turns out to have powerful applications in number theory – including, for example, in the famous proof of Fermat’s Last Theorem by Andrew Wiles.

These numbers were first described by Kurt Hensel in 1897 though, with hindsight, some of Ernst Kummer’s earlier work can be interpreted as implicitly using p-adic numbers. The p-adic numbers were motivated primarily by an attempt to bring the ideas and techniques of power series methods into number theory. Their influence now extends far beyond this. For example, the field of p-adic analysis essentially provides an alternative form of calculus.

More formally, for a given prime p, the field $\mathbb{Q}_p$ of p-adic numbers is a completion of the rational numbers. The field $\mathbb{Q}_p$ is also given a topology derived from a metric, which is itself derived from the p-adic order, an alternative valuation on the rational numbers. This metric space is complete in the sense that every Cauchy sequence converges to a point in $\mathbb{Q}_p$. This is what allows the development of calculus on $\mathbb{Q}_p$, and it is the interaction of this analytic and algebraic structure that gives the p-adic number systems their power and utility.

The p in “p-adic” is a variable and may be replaced with a prime (yielding, for instance, “the 2-adic numbers”) or another *placeholder variable* (for expressions such as “the ℓ-adic numbers”). The “adic” of “p-adic” comes from the ending found in words such as dyadic or triadic. Here we will talk about p-adic integers in most cases.

p-adic Numbers as Power Series

The most concrete way to think of p-adic integers is as formal power series with base p. This idea is motivated by the unique decomposition of positive integers as sums of powers of p. For example, if we take $p = 3$, we can write 10 as $1+0\times3+1\times3^2$. Taking $p = 2$, we have $10 = 0+1\times2+0\times2^2+1\times2^3$. We can do this for any nonnegative integer and any prime, and this type of construction gives us an explicit definition of the p-adic integers as formal power series. We can also come up with a formal power series to represent any negative integer, but these have infinitely many terms, so they are harder to describe.

Definition

The p-adic integers are the set of formal power series

$$a_0 + a_1 p + a_2 p^2 + \ldots + a_n p^n + \ldots$$

where p is prime and a_i are integers from $\{0, 1, 2, \ldots, p-1\}$.
This set of power series is actually a ring; as a set, it is bijective with $\mathbb{Z}/p\mathbb{Z}[x]$, but the ring structure is different. The disadvantage of this definition of the p-adic integers is that defining addition and multiplication explicitly is difficult. It is possible to do so, but because we must deal with "carrying" when a digit is greater than $p-1$, it involves more complicated constructions than, say, those for $\mathbb{Z}/p\mathbb{Z}[x]$.
For example, if $\alpha = a_0 + a_1 p + a_2 p^2 + \ldots$ and $\beta = b_0 + b_1 p + b_2 p^2 + \ldots$, and $\alpha + \beta = \gamma = c_0 + c_1 p + c_2 p^2 + \ldots$, then $c_0 = a_0 + b_0 \mod p$. To find c_1, we have to solve $c_0 + c_1 p = a_0 + b_0 + a_1 p + b_1 p \mod p^2$. Since we are going from $\mod p$ to $\mod p^2$, there is not an easy way to express c_1 without a_0 and b_0. To find each subsequent term, we similarly have to consider all previous a_i and b_i, as well as c_i. Multiplication has a similar flavor; if $\alpha\beta = \mu = v_0 + v_1 p + v_2 p^2 + \ldots$, then $v_0 = a_0 b_0 \mod p$. To find subsequent terms, we have to consider previous terms. For example, to find v_1, we must solve $v_0 + v_1 p = (a_0 + a_1 p)(b_0 + b_1 p) \mod p^2$.

The Analytical Definition of p-adic Integers

The p-adic integers can also be seen as the completion of the integers with respect to a p-adic metric. Let us introduce a p-adic valuation on the integers, which we will extend to $\mathbb{Z}_p$.

p-adic Absolute Value

For any integer a, we can write $a = p^n r$ where p and r are relatively prime. The p-adic absolute value is

$$|a|_p = p^{-n}$$

It is natural to wonder how the p-adic norm behaves with addition and multiplication. Let us discuss some properties.

Properties

For all integers a, b:

1. $|a + b|_p \leq \max\{|a|_p, |b|_p\}$

2. $|ab|_p = |a|_p |b|_p$

Proof

Let $a = p^n r$ and $b = p^m s$. Then, $|a|_p = p^{-n}$ and $|b|_p = p^{-m}$.

1. Without loss of generality, say $n \leq m$. Then,

   $$a + b = p^n r + p^m s = p^n (r + p^{m-n} s)$$

   Since $a + b$ is at least divisible by p^n (it is divisible by higher powers of p if $r + p^{m-n}s$ is divisible by p), the absolute value cannot be larger than p^{-n}. Thus,

   $$|a + b|_p \leq \max\{|a|_p, |b|_p\}$$

   as desired.

2. We have

   $$ab = p^{n+m}(rs)$$

   Since r and s are relatively prime with p, rs cannot be divisible by p, and

   $$|ab|_p = |a|_p |b|_p$$

   as desired.

Some more ways to look at it

We can also look at analysis in the p-adics; unlike in standard calculus, a series $\sum a_n$ in the p-adic metric converges if and only if $\lim_{n\to\infty} |a_n|_p = 0$. This condition is obviously necessary, just as in standard calculus. It is sufficient because $|x + y|_p \leq \max(|x|_p, |y|_p)$; adding numbers with smaller valuations does not have any affect on the overall valuation.

Another concept that makes sense is that of a p-adic order. The p-adic order, denoted ord_p, of the integer $a = p^n r$ would be n. Many computations, like some we will see later, are easier when working with orders instead of absolute values.

Recall that a Cauchy sequence is a sequence (a_n) such that for any $\epsilon > 0$, there exists some $N \in \mathbb{N}$ such that for all $n, m > N$, $|a_n - a_m|_p < \epsilon$. Let us consider Cauchy sequences in $\mathbb{Z}$ with respect to the p-adic norm. These are sequences (a_n) such that above some N, $|a_n - a_m|_p < \epsilon$, so the difference between terms can be divided by higher powers of p.

Definition

The ring $\mathbb{Z}_p$ is the completion of $\mathbb{Z}$ with respect to the p-adic norm. That is, $\mathbb{Z}_p$ is the set of all equivalence classes of Cauchy sequences (a_n) where (a_n) and (b_n) are equivalent if $\lim_{n\to\infty} |a_n - b_n|_p = 0$.

There is a natural ring structure given by component-wise addition and multiplication. Let (a_n) and (b_n) be representatives in two equivalence classes. Define $(a_n) + (b_n)$ to be $(a_n + b_n)$. This must be a Cauchy sequence. For any ϵ, there exist some N_1 and N_2 such that for all $n, m > N_1$ and $p, q > N_2$, $|a_n - a_m|_p \leq \epsilon$ and $|b_p - b_q|_p \leq \epsilon$. Take N to be the maximum of N_1 and N_2. Then, for any $n, m > N$, we have $|a_n + b_n - a_m - b_m|_p \leq \max\{|a_n - a_m|_p, |b_n - b_m|_p\} \leq \epsilon$. So, $(a_n + b_n)$ is a Cauchy sequence. Addition does not depend on choice of representative. If we have (a'_n) and (b'_n), two other representatives, then we know $\lim_{n\to\infty}(a_n - a'_n) = 0$ and $\lim_{n\to\infty}(b_n - b'_n) = 0$, so $\lim_{n\to\infty}(a_n + b_n - a'_n - b'_n) = 0$.

Let us also define multiplication to be $(a_n)(b_n) = (a_n b_n)$. We know that multiplication is well-defined since

$$|a_n b_n - a_m b_m|_p = |a_n b_n - a_n b_m + a_n b_m - a_m b_m|_p \leq \max\{|a_n|_p |b_n - b_m|_p, |b_m|_p |a_n - a_m|_p\}.$$

Since $|a_n|_p$ and $|b_n|_p$ are both bounded by 1, we know that $(a_n b_n)$ is a Cauchy sequence. The same equation shows that multiplication does not depend on choice of representative. If we take the same equation above and substitute a_m for a'_n and b_m for b'_n and take the limit as $n \to \infty$, we get that the absolute value approaches 0.

This definition yields two facts. Firstly, the integers are contained in the p-adic integers. For any integer n, we can consider the Cauchy sequence (a_m) where each of the $a_m = n$. This sequence is constant, so it must be Cauchy. So, we know $\mathbb{Z} \subseteq \mathbb{Z}_p$. This fact implies that an equation can only have a solution in $\mathbb{Z}$ if it has a solution in $\mathbb{Z}_p$. Secondly, the p-adic norm can be uniquely extended to $\mathbb{Z}_p$. If (a_n) is a sequence in $\mathbb{Z}_p$, then we can define $|(a_n)|_p$ to be $\lim_{n\to\infty} |a_n|_p$. We know that $|a_n|_p$ must have a limit, as (a_n) is a Cauchy sequence with respect to this absolute value.

The Algebraic Definition of p-adic Integers

There is also an algebraic definition of the completion of a group, which can also give us an equivalent definition of the p-adic integers as a completion of $\mathbb{Z}$.

Definition

Let us consider a family of groups $\{G_i\}$ with homomorphisms $\phi_{ji} : G_j \to G_i$ for all $i \leq j$ such that ϕ_{ii} is the identity on G_i and $\phi_{ki} = \phi_{kj} \circ \phi_{ji}$ for all $i \leq j \leq k$. The inverse limit, denoted $\varprojlim G_n$, is

the set of all sequences (a_n) with the property $a_n \in G_n$ and $\phi_{ji}(a_j) = a_i$ for all $i \leq j$.
The inverse limit $\varprojlim G_n$ has a natural group structure given by component-wise addition. Additionally, if the G_n are rings, then $\varprojlim G_n$ inherits a ring structure. For all n, we have a natural projection $p_n : \varprojlim G_n \to G_n$ defined by $(a_n) \mapsto a_n$. This map is a group homomorphism. The completion of a group G with respect to a system of subgroups

$$G = G_0 \supseteq G_1 \supseteq G_2 \supseteq \cdots \supseteq G_n \supseteq \cdots$$

with maps $\phi_{n+1} : G/G_{n+1} \to G/G_n$ is denoted by $\hat{G}$ and defined as $\varprojlim G/G_n$. The inverse limit $\varprojlim G/G_n$ is the set of all sequences (a_n) with the property $a_n \in G/G_n$ and $\phi_{n+1}(a_{n+1}) = a_n$ for all n.
It is noted that this definition of completion is analogous to the topological definition of completion. The subgroups G_n provide a topology on G, as they define open neighborhoods of the identity on G. By translation, for an element g of G, we have a basis for open neighborhoods given by $g + G_n$. The Cauchy sequences (s_n) in this topology are sequences such that for any G_k, there is some N such that for all $n, m > N$, $s_n - s_m$ is in G_k. Any Cauchy sequence gives an element of the inverse limit. We can define p_k to be the projection $G \to G/G_k$. Then, $p_k(s_n) = p_k(s_m)$ for all $n, m > N$. If $a_k := p_m(s_n)$ for all $n > N$, then (a_k) is an element of $\varprojlim G/G_k$. We can show that the completion is the same as the inverse limit by showing that there is an inverse map, and every element in the inverse limit yields a Cauchy sequence. If we have $(a_k) \in \varprojlim G/G_k$, then we can choose a sequence of representatives $s_n \in G$ in the equivalence classes of $a_n \in G/G_n$. We can show that (s_n) is a Cauchy sequence, which does not vary under choice of representative, and get that the inverse limit and completion are equivalent.
One common special case of completions of groups is the I-adic completion of a ring R for some ideal I. The sequence of subgroups we consider is $G = R$ and $G_n = I^n R$. We can apply this idea, with $R = \mathbb{Z}$ and $I = (p)$, to define the p-adic integers in a different way. The p-adic integers are the (p)-adic completion of $\mathbb{Z}$, that is, $\varprojlim \mathbb{Z}/p^n\mathbb{Z}$. The p-adic integers are a special case as told above.
The inverse limit definition of the p-adics is equivalent to the Cauchy completion of $\mathbb{Z}$ under the p-adic norm. All three definitions of the p-adics are equivalent.

Now let's discuss some other norms and concepts of p-adic numbers with a different approach to understand solving p-adic equations. Mathematical fields are commutative rings that have multiplicative inverses for all elements. Commutative rings are sets endowed with two operations, addition and multiplication, defined to be commutative, associative, and closed. In addition, there exist additive and multiplicative identities. Two main examples of fields that will be used here 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 by F.

There are three conditions that have to be satisfied for a norm defined by $|\cdot| : F \to \mathbb{R}$ from a metric space F to the non-negative real numbers:

1. $|x| = 0$ if and only if $x = 0$
2. $|x + y| \leq |x| + |y|$ (triangle inequality)
3. $|xy| = |x| \cdot |y|$

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. Let's define $\deg(a)$ to be the degree of a polynomial. If we examine the constant polynomials we define:

$$\deg(a) = \begin{cases} -\infty & \text{if } a = 0 \\ 0 & \text{otherwise} \end{cases}$$

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:

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

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 $(x, y) \mapsto |x - y|$. We are already aware of another norm, the absolute value, which induces a distance metric on $\mathbb{Q}$ and $\mathbb{R}$.

The p-adic norm

The common way in which we write numbers is by their decimal expansion in a series of base ten. These are written in shorthand by a sequence of integers $\ldots a_m a_{m-1} \ldots a_1 a_0 \ldots$, where the a_j terminate to the left, i.e., there exists N such that $a_j = 0$ for all $j > N$ 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. Multiplication of elements is defined as the multiplication of series representing those elements. Let $a = \sum_{i=0}^{\infty} a_i 10^i$ and $b = \sum_{i=0}^{\infty} b_i 10^i$. Then,

$$ab = \left(\sum_{i=0}^{\infty} a_i 10^i\right)\left(\sum_{i=0}^{\infty} b_i 10^i\right)$$

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, since, for example, the product

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

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 $x_1 = \sum_{j=0}^{\infty} a_{j1} p^j$, $x_2 = \sum_{j=0}^{\infty} a_{j2} p^j$, and in general $x_i = \sum_{j=0}^{\infty} a_{ji} p^j$. 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 $a_{ji} = 0$ for all $i > N_i$. 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 $\ldots p^m p^{m-1} \ldots p^2 p^1$.

This clearly does not converge in the absolute norm. To understand this, we introduce $\mathrm{ord}_p(x)$, which equals the highest power of p that divides $x \in \mathbb{Q}$. For example, $\mathrm{ord}_2(96) = 5$, because 2^5 divides 96. In line with our notation of $\mathbb{Z}_p$ that we developed earlier, we can also define $\mathrm{ord}_p(x)$ in a convenient way:

$$\mathrm{ord}_p(x) := \begin{cases} \infty & \text{if } a_i = 0 \\ \min(s : a_s \neq 0) & \text{otherwise} \end{cases}$$

And we define a new norm, denoted $|\cdot|_p$ by,

$$|x|_p := \begin{cases} 0 & \text{if } a_i = 0 \text{ for all } i \\ p^{-\mathrm{ord}_p(x)} & \text{otherwise} \end{cases}$$

It can be noted that 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 $|ab|_p = |a|_p|b|_p$, is satisfied trivially when either a or b is zero. But if they are not zero, then $|ab|_p = p^{-\mathrm{ord}_p(ab)} = p^{-(\mathrm{ord}_p(a)+\mathrm{ord}_p(b))} = p^{-\mathrm{ord}_p(a)} p^{-\mathrm{ord}_p(b)} = |a|_p|b|_p$. Another consequence of this norm is the strong triangle inequality:

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

It can be noted that the 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:

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

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 $|x-y| = |y|$. First,

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

We can establish the converse inequality in the following way:

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

Hence we get, $|x-y| = |y|$.
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. Let's define a "disk" D by:

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

Then,

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

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

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:

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. We begin with the base case: $|1| = 1 \leq 1$.
The equality follows from the definition 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 $|k| \leq 1$ for all $k \in \{1, \ldots, n-1\}$. 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:

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

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

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

The Completion Theorem

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 $\hat{M}$.

The completion for $\mathbb{Q}$ with respect to the absolute value is $\mathbb{R}$. One of the standard ways of constructing the reals is by examining the Cauchy sequences of rational numbers. Recall that a sequence is Cauchy if,

$$\forall \epsilon > 0, \exists N \text{ such that } \forall n, m > N, \quad |a_m - a_n| < \epsilon$$

All rationals are periodic in their decimal expansion. This can be proven by expanding in a geometric sequence. For the same reason, any rational number in its expansion in any base is periodic, including the p-adic expansions. Therefore, we can construct irrational numbers by producing sequences that are aperiodic in their decimal form. For example, the sequence

$$0.101, 0101101, 101101101, \ldots$$

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.

The p-adic numbers are expressed in base-p expansion as,

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

where $a_n = 0$ for large n. If $a_n = 0$ for all $n > 0$, these are the p-adic integers $\mathbb{Z}_p$ as defined previously. It can be noted that since the terms terminate to the right, 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. Suppose that the lowest nonzero term is a_{-m}. Then,

$$\left| \sum_{-m}^{k} d_i p^i - \sum_{-m}^{n} d_i p^i \right|_p = \left| \sum_{n+1}^{k} d_i p^i \right|_p \leq \max(|d_i|_p) \leq p^{-N}$$

since $0 \leq d_i \leq p$. 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:

Each p-adic number can be uniquely written as the sum of a convergent series of the form,

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

It is noted 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 eventually periodic to the left (instead of the right for the standard decimal expansion). For example,

$$\frac{1}{2} = \dots \left(\frac{p-1}{2}\right)\left(\frac{p-1}{2}\right)\left(\frac{p+1}{2}\right).0000\dots$$

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

$$-1 = \dots (p-1)(p-1)(p-1).0000\dots$$

To see this, we can add 1:

$$0 = \dots (p-1)(p-1)(p).0000\dots = \dots (p-1)(p)0.000\dots = \dots (p)00.000\dots = \dots 000.000\dots$$

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 $\dots 0010.000\dots$. Let $x = \dots a_2 a_1 a_0.000\dots$. To solve the equation, a necessary condition is $a_0^2 \equiv p \pmod{p}$. However, this has no solution because a prime is not a square number. The question remains whether p-adic numbers are the whole story as far as norms go.

Ostrowski's Theorem

Ostrowski's Theorem: 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.
This theorem establishes the classifications of norms on the rationals. It has profound consequences.

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

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 conflict with our intuition of series expansions. For example, revisiting the p-adic expansion from earlier of -1, we see:

$$-1 = \dots (p-1)(p-1)(p-1).00000\dots$$

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:

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

Now we develop some tools using modular arithmetic in order to be able to solve for equations in 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 $\mathbb{Q}_p$ is congruent to its series expansion $a_0 + a_1 p + \ldots + a_{i-1} p^{i-1} \mod p^i$.

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 $f \equiv 0 \mod p^i$ for all $i \in \mathbb{N}$. 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. We assume a solution for the next iteration: $a_0 + a_1 p$. Hence, defining the polynomial function $f = \sum_{i=0}^{\infty} c_i$, we get,

$$f(a_0 + a_1 p) = \sum_{i=0}^{\infty} c_i (a_0 + a_1 p)^i$$

$$= \sum_{i=0}^{\infty} \left(\binom{i}{0} c_i a_0^i + \binom{i}{1} c_i a_0^{i-1} a_1 p \right) + \text{higher order terms}$$

$$\equiv \sum_{i=0}^{\infty} (c_i a_0^i + i c_1 a_0^{i-1} a_1 p) \mod p^2$$

$$= (f(a_0) + f'(a_0) a_1 p) \mod p^2$$

$$= (h_0 p + f'(a_0) a_1) \mod p$$

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:

$$\alpha_n f'(\alpha_{n-1}) + h_{n-1} \equiv 0 \mod p$$

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. We note that $\alpha_{n-1} = a_0 + pq$, where $q = a_1 + a_2 p + \ldots + a_{n-1} p^{n-2}$ is an integer. Thus, proceeding in a process similar to the one above, we obtain the result:

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

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

Thus reducing the equation to,

$$\alpha_n f'(a_0) + h_{n-1} \equiv 0 \mod p$$

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 $f'(a_0) \neq 0 \mod p$.

We use an example to illustrate the abstract derivation above. 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 find $a_0^2 \equiv 7 \mod 3$. The solutions are $a_0 = 1, 2$. We choose $a_0 = 1$ and apply the equation above. $f(a_0) = -6 \equiv 3 \mod 9 = 3h_0 \mod 9$, so $h_0 \equiv 1 \mod 3$; $f'(a_0) = 2$ mod 3. The equation becomes:

$$2a_1 + 1 \equiv 0 \mod 3 \Rightarrow a_1 = 1; \quad \alpha_1 = 1 + 1 \times 3 = 4$$

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

$$\alpha_4 = 1 + 1 \times 3 + 1 \times 3^2 + 0 \times 3^3 + 2 \times 3^4 + \ldots$$

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 zeros.

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 using only the analysis of $f(x)$. Let

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

The chain of equations is:

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

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 $\alpha_1 = a_1 + a_2 p + a_3 p^2 + \ldots$,

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

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

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

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

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

There 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,

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

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, the induction which gives rise to the results quoted in the Thurston paper is produced. First, we check the base case:

$$\begin{aligned} c_{n-1} &= \left(\frac{1}{p^n}\right)\left(c_{n-1}p^{n-1} + n a_0 p^{n-1}\right) \\ &= \frac{c_{n-1}}{p} + \frac{n a_0}{p} \\ &= \frac{n a_0}{p-1} \end{aligned}$$

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

$$c_{n-2} = \left(\frac{1}{p^n}\right)\left(c_{n-2}p^{n-2} + c_{n-1}(n-1)a_0 p^{n-2} + \binom{n}{2} a_0^2 p^{n-2}\right)$$

$$c_{n-2}(p^2 - 1) = c_{n-1}(n-1)a_0 + \binom{n}{2} a_0^2$$

$$c_{n-2}(p^2-1) = (c_{n-1})^2\binom{n}{2}\left(\frac{2(n-1)a_0(p-1)}{n^2a_0} + \frac{(p-1)^2a_0^2}{n^2a_0^2}\right)$$

$$c_{n-2} = \binom{n}{2}\left(\frac{c_{n-1}}{n}\right)^2\left(\frac{2p-2+p^2-2p+1}{p^2-1}\right)$$

$$c_{n-2} = \binom{n}{2}\left(\frac{c_{n-1}}{n}\right)^2$$

Now let's assume,

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

We induct on the index k:

$$c_{n-(k+1)} = \left(\frac{1}{p^n}\right)\left(c_{n-(k+1)}p^{n-(k+1)} + \binom{n-k}{1}a_0c_{n-k}p^{n-(k+1)} + \ldots + \binom{n}{k+1}a_0^{k+1}p^{n-(k+1)}\right)$$

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

$$= \sum_{j=1}^{k+1}\binom{n}{k-j+1}\left(\frac{a_0}{p-1}\right)^{k-j+1}\binom{n-(k-j+1)}{j}a_0^j$$

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

$$= \binom{n}{k+1}\left(\frac{a_0}{p-1}\right)^{k+1}\sum_{j=1}^{k+1}\binom{k+1}{j}(p-1)^j$$

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

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

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:

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

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 $F_j(x) = (x+1)^n$ or $F_j(x) = x^n$.
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 do not depend on a_1, we can replace a_1 with 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 $f(a_0 + xp) \equiv 0 \mod p^2$ 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:

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

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 $F_1'(a_1) \equiv 0 \mod p$, 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:

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

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 contradicts 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 $F_m'(a_m) \not\equiv 0 \mod p$. This results in the striking conclusion that it is possible to solve for all possible simple (non-multiple) roots in a finite number of steps. The process is as follows: first, we have to find a solution a_0 to $f(x) \equiv 0 \mod p$. Then find a solution a_1 to $F_1(x) \equiv 0 \mod p$. We have to 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.

Final Note

In this report, we have explored the realm of p-adic numbers and their fundamental properties, alongside the method of solving p-adic equations. Throughout the exploration, we encountered numerous key terminologies, theorems, and lemmas that provided the foundational understanding necessary for grasping the intricacies of p-adic numbers. We hope this exposition has clarified the theory and its applications.