P-ADIC NUMBERS AND THE LOCAL-TO-GLOBAL PRINCIPLE

KELSEA HULL

Abstract. We introduce the notion of p-adic absolute value on the rationals. We prove up to equivalence that these and the Euclidean absolute value are the only non-trivial absolute values. Then we discuss the completion of the rationals under the p-adic absolute value to obtain p-adic numbers. Finally we discuss applications of p-adic numbers to problems in number theory, in particular we explore the local to global principle.

Contents

1. Introduction to P-adic Absolute Values

1.1. Trivial and Non-trivial Absolute Values.

When discussing a p-adic absolute value, we must first look at the general idea for an absolute value on $\mathbb{Q}$.

An absolute value on $\mathbb{Q}$ is a map

$$|.| : \mathbb{Q} \to [0, \infty)$$

that satisfies the following conditions:

- $|x| = 0$ iff $x = 0$
- $|1| = 1$
- $|xy| = |x||y|$
- $|x + y| \leq |x| + |y|$

The usual absolute value, given by:

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

satisfies these properties.

Date: May 3, 2017.

Thanks to Dr. Fili for his continued guidance in the writing of this paper.

The trivial absolute value, given by:

$$|x|_{\text{trivial}} = \begin{cases} 0 & \text{if } x = 0 \\ 1 & \text{if } x \neq 0 \end{cases}$$

satisfies these as well.

Now we must look at other non-trivial absolute values. In $\mathbb{Z}$, the p-adic absolute value is as follows: For a prime p in $\mathbb{Z}$,

$$|n|_p = \begin{cases} 0 & \text{if } n = 0, \\ p^{-\operatorname{ord}_p(n)} & \text{if } n \neq 0 \end{cases}$$

where $\operatorname{ord}_p(n)$ is given by the exponent of p in the prime power factorization of n.

Example 1.1. Let $p = 3$ and $n = 12$. Let us see how to compute $|12|_3$.

We must first find the prime power factorization of 12.

$$12 = 2^3 \cdot 3^1$$

so $\operatorname{ord}_3(12) = \operatorname{ord}_3(2^2 \cdot 3^1) = 1$.

then

$$|12|_3 = p^{-\operatorname{ord}_3(12)} = 3^{-1} = \frac{1}{3}$$

read the 3-adic absolute value of 12 is $\frac{1}{3}$.

Similarly,

$$|12|_2 = 2^{-2} = \frac{1}{2^2} = \frac{1}{4}$$

and

$$|12|_5 = 5^{-0} = 1$$

Since $12 = 2^2 \cdot 3^1 \cdot 5^0$.

This method of finding the absolute value can be extended to $\mathbb{Q}$ as follows:

$$\left|\frac{a}{b}\right|_p = \frac{|a|_p}{|b|_p} = p^{\operatorname{ord}_p(b) - \operatorname{ord}_p(a)}$$

for $a, b \in \mathbb{Z}$ and $b \neq 0$.

Example 1.2. Let us compute $|\dfrac{25}{18}|_3$. We begin by factoring:

$$25 = 2^0 \cdot 3^0 \cdot 5^2, \quad \text{so} \quad \operatorname{ord}_3(25) = 0.$$

$18 = 2^1 \cdot 3^2 \cdot 5^0$ so $\operatorname{ord}_3(18) = 2$. Thus,

$$\left|\frac{25}{18}\right|_3 = 3^{\operatorname{ord}_3(18) - \operatorname{ord}_3(25)} = 3^{2-0} = 3^2 = 9$$

Similarly,

$$\left|\frac{25}{18}\right|_5 = 5^{\operatorname{ord}_5(18) - \operatorname{ord}_5(25)} = 5^{0-2} = \frac{1}{5^2} = \frac{1}{25}.$$

The question, then, is does the p-adic absolute value satisfy the criteria previously stated:

(1) $|x| = 0$ iff $x = 0$
(2) $|1| = 1$
(3) $|xy| = |x| \cdot |y|$

(4) $|x+y| \leq |x| + |y|$

Proof. We break the proof into cases:

Condition I. For $p \in \mathbb{Z}$ prime and $n = 0$, we have

$$|0|_p = p^{-\operatorname{ord}_p(0)} = 0$$

as by convention $p^{-\infty} = 0$.

Condition II. For $p \in \mathbb{Z}$ prime and $n = 1$, we have

$$|1|_p = p^{-\operatorname{ord}_p(1)} = p^0 = 1$$

for any prime $p > 1$.

Condition III. For $n.m \in \mathbb{Z}$ and prime $p \in \mathbb{Z}$,

$$|nm|_p = p^{-\operatorname{ord}_p(nm)}$$

By the Unique Factorization Theorem, $\operatorname{ord}_p(nm) = \operatorname{ord}_p(n) + \operatorname{ord}_p(m)$. Then,

$$\begin{aligned} p^{-\operatorname{ord}_p(nm)} &= p^{-(\operatorname{ord}_p(n)+\operatorname{ord}_p(m))} \\ &= p^{-\operatorname{ord}_p(n)} \cdot p^{-\operatorname{ord}_p(m)} \\ &= |n|_p \cdot |m|_p. \end{aligned}$$

Condition IV. The last condition, or the triangle inequality, requires:

$$|n+m|_p \leq |n|_p + |m|_p$$

for $n, m \in \mathbb{Z}$ and prime $p \in \mathbb{Z}$.

To start, we need to factor n, m.

$$n = p^k \cdot a \quad \text{for} \qquad k, a \in \mathbb{Z}$$

$$m = p^l \cdot b \quad \text{for} \quad l, b \in \mathbb{Z}$$

Then, by assuming $k \geq l$,

$$\begin{aligned} n + m &= p^k \cdot a + p^l \cdot b \\ &= p^l(p^{k-l}a + b) \end{aligned}$$

Thus there are at least l powers of p in $n+m$, so $\operatorname{ord}_p(n+m) \geq l$. Then,

$$|n+m|_p = p^{-\operatorname{ord}_p(n+m)} \leq p^{-l} = |m|_p$$

So

$$|n+m|_p \leq |m|_p \leq |m|_p + |n|_p.$$

This in fact proves the Strong Triangle Inequality:

$$|n+m|_p \leq \max\{|n|_p, |m|_p\}$$

since, $|n|_p = p^{-k} \leq p^{-l} = |m|_p$ as by assumption $k \geq l$.

This holds true for p-adic absolute values in $\mathbb{Q}$ as well.

$$\left|\frac{a}{b} + \frac{c}{d}\right|_p = \left|\frac{ad+cb}{bd}\right|_p = \left|\frac{n+m}{D}\right|_p$$

for $n = ad$, $m = cb$, and $D = bd$,

$$\left|\frac{n+m}{D}\right|_p = \frac{|n+m|_p}{|D|_p} \leq \frac{\max\{|n|_p, |m|_p\}}{|D|_p}$$

$$\frac{\max\{|n|_p, |m|_p\}}{|D|_p} = \max\left\{\frac{|n|_p}{|D|_p}, \frac{|m|_p}{|D|_p}\right\} = \max\left\{\left|\frac{ad}{bd}\right|_p, \left|\frac{cb}{bd}\right|_p\right\}$$

$$\max\left\{\left|\frac{ad}{bd}\right|_p, \left|\frac{cb}{bd}\right|_p\right\} = \max\left\{\left|\frac{a}{b}\right|_p, \left|\frac{c}{d}\right|_p\right\}$$

for $a, b, c, d \in \mathbb{Z}$, $b, d \neq 0$. □

1.2. **Ostrowski's Theorem and Proof.** Now that we have defined one family of non-trivial absolute values on $\mathbb{Q}$, the question arises: are there others? We will prove through Ostrowski's Theorem that the answer is no.

Theorem 1.1. Ostrowski's Theorem states that up to equivalences by scaling by a power, the only non-trivial absolute values on $\mathbb{Q}$ are the usual and the p-adic absolute values.

Proof. This must be proved in two cases: either $|a| > 1$ for some $a \in \mathbb{Z}$ or $|a| \leq 1$ for all $a \in \mathbb{Z}$.

Case 1:

If there exists $a \in \mathbb{Z}$ such that $|a| > 1$, then $|a| = |a|_\infty^\theta$ for some $\theta > 0$, $|a|_\infty$ being the usual absolute value. Assuming for the moment that

$$|b| = |a|^{\frac{\log b}{\log a}} \tag{1}$$

for all $a, b \in \mathbb{Z}, a, b > 1$, we will prove that this absolute value must be the usual absolute value up to the scaling factor θ, that is, that $|\cdot| = |\cdot|_\infty^\theta$.

Since $a, b > 1$, $|b|_\infty = b$ and $|a|_\infty = a$. If $|a| = |a|_\infty^\theta$ and we chose $\theta = \frac{\log|a|}{\log a}$, then

$$\begin{aligned}
|b| = |a|^{\frac{\log b}{\log a}} &= (|a|_\infty^\theta)^{(\log b/\log a)} \\
&= (|a|_\infty^{(\log b/\log a)})^\theta \\
&= (a^{\log b/\log a})^\theta = (a^{\log_a b})^\theta \\
&= b^\theta \quad \text{since } b > 0, \quad |b|_\infty = b \\
&= (|b|_\infty)^\theta = |b|_\infty^\theta
\end{aligned}$$

thus

$$|b| = |b|_\infty^\theta.$$

This is true for all $a, b > 0$ and through the following lemma, is true for all negatives as well.

Lemma 1.1. For any nontrivial absolute value $|\cdot|$, we have $|-1| = 1$.

Proof of Lemma. We know that $|1| = 1$. Then, because $|x \cdot 1| = |x| \cdot |1| = |x|$ and $1 = (-1)^2$ we get $|(-1)^2| = |1| = 1$. We also know that $|(-1)^2| = |-1|^2$. This tells us $|-1| = 1$ since $|-1| \geq 0$. □

We will now continue with the proof of Ostrowski's Theorem. To get equation (1), write a^N in base b expansion where $M = \left\lfloor \frac{\log a^N}{\log b} \right\rfloor$. Then,

$$a^N = d_0 + d_1 b + d_2 b^2 + \ldots + b_M b^M$$

with $d_m \in \{0, , 2, \ldots, b-1\} \quad \text{for} \quad m = 0, 1, 2, \ldots, M$. Thus

$$|a^N| \leq |d_0| + |d_1||b| + ... + |d_M||b|^M \leq (M+1)\max\{|1|, |2|, ..., |b-1|\}\max\{1, |b|\}^M$$

Where $(M+1)$ represents the number of terms and there are d terms in the $\max\{|a| \ldots |b-1|\}$ function. Then $\max\{1, |b|\}^M$ has b terms and we know the following:

$$\text{if} \quad |b| < 1, \quad \text{then} \quad \max\{1, |b|\}^M \quad \text{is replaced by} \quad 1$$

$$\text{however, if} \quad |b| > 1, \max\{1, |b|\}^M \quad \text{gives} \quad b^M.$$

Next, we take the N^{th} root of both sides, and apply the limit as n approaches infinity. This gives

$$|a| \leq \left(\left\lfloor \frac{\log a^N}{\log b} \right\rfloor + 1 \right)^{\frac{1}{N}} \cdot \max\{1, 2, \ldots, b-1\}^{\frac{1}{N}} \cdot \max\{1, b\}^{\frac{M}{N}}$$

We will analyze the three terms of the right-hand side separately. For the first term:

$$(M+1)^{\frac{1}{N}} = \left(\left\lfloor \frac{\log a^N}{\log b} \right\rfloor + 1 \right)^{\frac{1}{N}}$$

Due to the floor function, we know

$$\left(N \frac{\log a}{\log b} \right)^{\frac{1}{N}} \leq \left(\left\lfloor N \frac{\log a}{\log b} \right\rfloor + 1 \right)^{\frac{1}{N}} \leq \left(N \frac{\log a}{\log b} + 1 \right)^{\frac{1}{N}}.$$

Since we are taking the limit as N approaches infinity, this goes to 1 by the Squeeze Theorem since both $\left(N \frac{\log a}{\log b} \right)^{\frac{1}{N}}$ and $\left(N \frac{\log a}{\log b} + 1 \right)^{\frac{1}{N}}$ approach 1 as N approaches ∞ because they follow the form

$$(ax+b)^{\frac{1}{x}} \quad \text{goes to} \quad 1 \quad \text{as} \quad x \quad \text{goes to} \quad \infty.$$

For the second term, $\max\{1, 2, \ldots, b-1\}^{\frac{1}{N}}$, taking the limit as N approaches ∞ causes the term to go to 1. This is due to the limit resulting in a constant raised to a zero power, since $\frac{1}{N}$ is zero as N approaches ∞.

For the final term, we are mostly interested in the power $\frac{M}{N}$. We know that $\frac{M}{N}$ satisfies:

$$\frac{N \frac{\log a}{\log b} - 1}{N} \leq \frac{M}{N} \leq \frac{N \frac{\log a}{\log b}}{N}$$

because $M = \left\lfloor \frac{\log a}{\log b} \right\rfloor$. When we apply the limit as N approaches ∞, both $\frac{N \frac{\log a}{\log b} - 1}{N}$ and $\frac{N \frac{\log a}{\log b}}{N}$ are equal to $\frac{\log a}{\log b}$. This tells us that $\frac{M}{N}$ limits to $\frac{\log a}{\log b}$.

After combining these three terms, we get

$$1 \cdot 1 \cdot \max\{1, |b|\}^{\frac{\log a}{\log b}}.$$

Since $|a| > 1$, we need $|b|^{\frac{\log a}{\log b}} > 1$ so we need $|b|$ to be the maximum, so $|b| > 1$ and thus we conclude that equation (1),

$$|a| \leq |b|^{\frac{\log a}{\log b}},$$

does hold.

Also,

$$|b|^{\frac{\log a}{\log b}} \leq \left(|a|^{\frac{\log b}{\log a}}\right)^{\frac{\log a}{\log b}}$$

Now we have $|a| \leq |b|^{\frac{\log a}{\log b}}$ and by reversing $|b|^{\frac{\log a}{\log b}} \leq |a|$. Putting these together gets equality, so $|a| = |b|^{\frac{\log a}{\log b}}$.

This implies (1), that $|b| = |a|^{\frac{logb}{\log a}}$ as desired.

Case 2:

For this case, we assume that $|n| \leq 1$ for all $n \in \mathbb{Z}$, and that $|n|$ is nontrivial. Then there exists some $n \neq 0$ such that $0 < |n| < 1$. We can assume such an n is positive since $|n| = |-n|$, and we choose p to be the minimum element of $\mathbb{N}$ with $|p| < 1$. Note that p must be prime, otherwise we can write $p = ab$ with $1 < a, b < p$, and $|p| = |a||b| < 1$ which then gives $|a| < 1$ or $|b| < 1$ and which contradicts the assumption that p is the minimum element.

For this p, choose $\theta > 0$ with

$$|p| = |p|_p^\theta = \left(\frac{1}{p}\right)^\theta$$

from the definition of the p-adic absolute value.

Then

$$\log|p| = -\theta \log p$$

which gives

$$\theta = \frac{-\log|p|}{\log p} > 0.$$

We will show that $|n| = |n|_p^\theta$ for all $n \in \mathbb{Z}$. To do so, we need to show that if $\gcd(n,p) = 1$ then $|n| = 1$. If we know this, then for any number n, we can write $n = mp^k$ with $\gcd(m,p) = 1$, and then

$$\begin{aligned} |n| = |m \cdot p^k| &= |m||p|^k \\ &= |p|^k \\ &= \left(|p|_p^\theta\right)^k \\ &= |mp^k|_p^\theta \\ &= |n|_p^\theta \end{aligned}$$

which is what we wanted to show.

Now, to prove the claim, suppose for contradiction that the $\gcd(m,p) = 1$ but $|m| < 1$. By the Bézout theorem, there exists $k, l \in \mathbb{Z}$ such that $mk + pl = 1$. Then

$$|mk + pl| = 1$$

$$1 \leq |mk| + |pl| \leq |m| \cdot |k| + |p| \cdot |l|.$$

We know that $|k|$ and $|l|$ are less than or equal to 1 due to the earlier assumption. This gives us

$$1 \leq |m| + |p|$$

Which allows us to get the following equation.

$$1 - |p| \leq |m|$$

We can repeat the same process with m^N and it still holds that $1 - |p| \leq |m^N| = |m|^N$. If $|m| < 1$ and we take the limit as N goes to ∞, then $|m|^N$ goes to 0, giving

$$0 < 1 - |p| \leq 0$$

This contradiction shows that $|m| \geq 1$ and also that $|m| \leq 1$, so $|m| = 1$ if $\gcd\{p, m\} = 1$. Because we had $n = p^k \cdot m$, we now have

$$\begin{aligned} |n| &= |p^k| \\ &= \left(|p|_p^\theta\right)^k \\ &= |n|_p^\theta \end{aligned}$$

as we wanted earlier, thus we have shown $|n| = |n|_p^\theta$ for every $n \in \mathbb{Z}$. □

2. Completions under p-adic absolute value and Hensel's Lemma

2.1. **Completion of $\mathbb{Z}$ by $\mathbb{Z}_p$.** We denote by $\mathbb{Z}_p$ the completion of $\mathbb{Z}$ under the absolute value $|\cdot|_p$. This means the following: We take all sequences $x = (n_1, n_2, n_3, \dots) \in \mathbb{Z}^{\mathbb{N}}$ and we say that x is *Cauchy* (in the p-adic absolute value) if it satisfies:

$$\text{for any} \quad \epsilon > 0, \quad \text{there exists } M \text{ such that whenever } k, l > M, \quad |x_k - x_l|_p < \epsilon.$$

The space of p-adic integers $\mathbb{Z}_p$ is then the space of Cauchy sequences in $\mathbb{Z}$ under the equivalence relation where

$$x = \ (n_1 n_2, n_3, \dots) \sim y = \ (m_1, m_2, m_3, \dots) \quad \text{iff} \quad |n_k - m_k|_p \to 0 \quad \text{as} \quad k \to \infty.$$

This is analogous to how we can complete $\mathbb{Q}$ to get $\mathbb{R}$ via Cauchy sequences under the usual Euclidean absolute value.

Lemma 2.1. Every series

$$\sum_{n=0}^{\infty} a_n p^n \quad \text{with} \quad a_n \in \{0, 1, \dots, p-1\}$$

converges in p-adic absolute value.

Proof. Let $x = (x_1, x_2, \dots)$ be the sequence of integers given by the partial sums:

$$x_n = \sum_{n=0}^{N} a_n p^n.$$

Notice that if $l > k > M$, then

$$\begin{aligned} x_k - x_l &= a_{k+1} p^{k+1} + \dots + a_l p^l \\ &= p^{k+1}(a_{k+1} + p a_{k+2} + \dots + a_l p^{l-k-1}) \end{aligned}$$

Then the p-adic absolute value of this is equal to:

$$\begin{aligned} |x_k - x_l|_p &= |p^{k+1}|_p \cdot |a_{k+1} + \dots + p a_{k+2} + \dots + a_l p^{l-k-1}|_p \\ &= \frac{1}{p^{k+1}} \cdot |n|_p \end{aligned}$$

where $|n|_p \leq 1$ for any $n \in \mathbb{Z}$. Then

$$|x_k - x_l|_p \leq \frac{1}{p^{k+1}} \cdot 1 < \frac{1}{p^M}.$$

So this goes to 0 as $M \to \infty$. If we choose for any given $\epsilon > 0$ an M such that $\frac{1}{p^M} < \epsilon$, then $|x_k - x_l| < \epsilon$ for all $k, l > M$, so the sequence is Cauchy. □

For example,

$$\pi = \left(3, \frac{31}{10}, \frac{314}{100}, \frac{3141}{1000}, \ldots\right)$$

and other sequences would work too. These sequences under equivalence give $\mathbb{R}$ with the following operations: For

$$x = (x_1, x_2, x_3, \ldots) \quad \text{and} \quad y = (y_1, y_2, y_3, \ldots),$$

we let

$$x + y = (x_1 + y_1, x_2 + y_2, x_3 + y_3, \ldots)$$

and

$$xy = (x_1y_1, x_2y_2, x_3y_3, \ldots).$$

For example, to calculate $\pi + 1$,

$$\pi + 1 = \left(3, \frac{31}{10}, \frac{314}{100}, \ldots\right) + (1, 1, 1, \ldots) = \left(4, \frac{41}{10}, \frac{414}{100}, \ldots\right)$$

Writing $\mathbb{Q}^{\mathbb{N}}$ for the space of rational sequences, we let $X \subseteq \mathbb{Q}^{\mathbb{N}}$ be the subset of all Cauchy sequences. Then $\mathbb{R}$ can be defined as:

$$\mathbb{R} = X/\sim.$$

which is read X modulo the equivalence relation. Likewise, $\mathbb{Z}_p$ is the space of p-adic convergent sequences, from $\mathbb{Z}^{\mathbb{N}}$ modulo p-adic equivalence. Each $x \in \mathbb{Z}_p$ is represented by a sequence $(n_1, n_2, n_3, \ldots)$ where $n \in \mathbb{Z}$ and $|n_k - n_l| \to 0$ as $k, l \to \infty$.

Theorem 2.1. Each $x \in \mathbb{Z}_p$ has a unique representation as:

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

and the associated sequence is the sequence of partial sums $x = (x_1, x_2, x_3, \ldots)$ where

$$x_N = \sum_{n=0}^{N} a_n p^n \quad \text{with} \quad a_i \in \{0, 1, 2, \ldots, p-1\}.$$

Proof. Since there exists an N such that $|x_n - x_m|_p \leq \frac{1}{p}$ for all $n, m > N$, if we take $a_0 \equiv x_{N+1} \mod p$, we see that $x_n \equiv x_m \equiv a_0 \mod p$. If we now choose N' for which $|x_n - x_m| \leq \frac{1}{p^2}$ for $n, m > N'$, then $x_n \equiv x_m \mod p^2$ for all $n, m > N'$. Let a_1 be chosen so that $x_{N'+1} = a_0 + a_1 \cdot p \mod p^2$. We can make this choice because $x_{N'+1} \equiv a_0 \mod p$ by the fact that $N' > N$. Going from here, we can choose $x_1, x_2, x_3, \ldots, x_N, \ldots, x_{N'}, \ldots$ such that all are congruent modulo p. □

Example 2.1. For $x_n \equiv 25 \mod 27$ for all $n > N$, how could this be written as a Cauchy sequence? We know $27 = 3^3$ so our prime $p = 3$. We need $x_n = a_0 + a_1p + a_2p^2 + p^3(\ldots)$ to be congruent to $25 \mod p^3$ or $\mod 27$. To find a_0 we find what 25 is congruent to $\mod 3$. $25 = 3 \cdot 8 + 1$, so $a_0 = 1$. Then we need $a_0 + a_1p = 1 + a_1p \equiv 25 \mod 9$. We know $25 \equiv 7 \mod 9$ so we need to find a_1 such that $1 + a_0 \cdot 3$ is equal to 7. Thus $a_1 = 2$ and we have $x_n = 1 + 2 \cdot 3 + a_2p^2 + p^3(\ldots)$.

To find a_2 we know we need $25 \mod 27$. We have 7 already so we need $a_2 \cdot 3^2 = 18$, so $a_2 = 2$.

Now we have $x_n = 1 + 2 \cdot 3 + 2 \cdot 3^2 + 3^3 \cdot (\ldots)$ which is equivalent to 25 modulo 27.

2.2. **Completion of $\mathbb{Q}$ by $\mathbb{Q}_p$.** Now that we can use the p-adic absolute value to complete the integers, what about the rationals?

We can find the p-adic absolute value of a rational number by the following method:

$$|x|_p = \left|\frac{a}{b}\right|_p = p^{-\operatorname{ord}_p(b)+\operatorname{ord}_p(a)}$$

Basically, there is always a power of p^n that guarantees $|p^n x|_p \leq 1$. When we have this, we actually have the series

$$x = p^{-n}(a_0 + a_1 p + a_2 p^2 + \ldots) \quad \text{where} \quad a_0 \neq 0.$$

Think of this as when we multiply by p^n, we eliminate the powers of p in the denominator. This ensures $p^n x = \frac{a}{b}$ with the $\gcd(p, b) = 1$ and $\gcd(p, a) = 1$. Now, b^{-1} makes sense modulo p^n for all $n \in \mathbb{N}$ because there is no common factor between p and b.

This forms a Laurent series in p:

$$\sum_{i=N}^{\infty} a_i p^i \quad \text{for} \quad N \in \mathbb{Z}$$

or written out,

$$x = a_0 p^N + a_1 p^{N+1} + a_2 p^{N+2} \ldots$$

where N is any integer, possibly a negative.

This allows us to work with $\mathbb{Q}$ so we can now form the completion of $\mathbb{Q}$ under p-adic absolute value, which we denote by $\mathbb{Q}_p$. Our $\mathbb{Q}_p$ series will be

$$x = a_{-N} p^{-N} + a_{-N+1} p^{-N+1} + \ldots + a_0 + a_1 p + a_2 p^2 + \ldots \quad \text{for} \quad a_i \in \{0, 1, 2, \ldots p-1\}$$

Observe that the first power of p that occurs in the series determines the p-adic absolute value. Therefore $\mathbb{Z}_p$ consists of terms with absolute value ≤ 1.

It can also be noted that $\mathbb{Q}_p = \operatorname{Frac}(\mathbb{Z}_p)$.

Example 2.2. Can we find a series for $\frac{1}{2}$ in $\mathbb{Z}_3$?

With $p = 3$ as our prime, we need to find a_i's that make $\frac{1}{2} = a_0 + a_1 p + a_2 p^2 + \ldots \equiv \frac{1}{2} \mod p^n$.

To start, we know that $\frac{1}{2} = 2^{-1} \mod 3$, so $\frac{1}{2} = 2 \mod 3$. This gives us $a_0 = 2$. Then we take

$$\frac{1}{2} \equiv 5 \mod 9 \equiv 2 + a_1 \cdot 3 \mod 9 \equiv 2 + 1 \cdot 3 \mod 9$$

so we know $a_1 = 1$. For a_2, we work $\mod 27$ to get

$$\frac{1}{2} \equiv 14 \mod 27 \equiv 2 + 1 \cdot 3 + a_2 \cdot 3^2 \mod 27 \equiv 2 + 1 \cdot 3 + 1 \cdot 3^2 \mod 27$$

so $a_2 = 1$. We continue this for the powers of $p = 3^n$ to get the full series that will give us $\frac{1}{2} \in \mathbb{Z}_3$.

2.3. **Hensel's Lemma.** Just like the case of the real numbers, there exist irrational numbers in $\mathbb{Q}_p$. We can explicitly construct some of these numbers via Hensel's lemma for finding roots of polynomials in $\mathbb{Z}_p$:

Theorem 2.2 (Hensel's lemma)**.** Given a polynomial $f(x) \in \mathbb{Z}[x]$ (or $\mathbb{Z}_p[x]$), suppose f has an approximate root a:

$$f(a) \equiv 0 \mod p$$

and $f'(a) \not\equiv 0 \mod p$ then there exists a unique $\alpha \in \mathbb{Z}_p$ such that

(1) $f(\alpha) = 0 \quad \text{in} \quad \mathbb{Z}_p$
(2) $\alpha \equiv a \mod p$

Proof. We rely on Newton's root finding method for this proof. We will construct for series for α inductively. Assume that we have found

$$\alpha_n = a_0 + a_1 p + \ldots + a_{n-1}p^{n-1} \quad \text{with} \quad a_i \in \{0, \ldots, p-1\}$$

so that $f(\alpha_n) \equiv 0 \mod p^n$. The base case $n = 1$ is satisfied with $\alpha_1 = a_0$. We want to find (the unique) $a_n \in \{0, \ldots, p-1\}$ with $\alpha_{n+1} = a_0 + a_1 p + \ldots + a_n p^n$ such that $f(\alpha_{n+1}) \equiv 0 \mod p^{n+1}$. If we let d denote the degree of $f(x)$, then we can write:

$$f(x) = f(\alpha_n) + f'(\alpha_n)(x - \alpha_n) + \frac{f''(\alpha_n)(x-\alpha_n)^2}{2!} + \cdots + \frac{f^d(\alpha_n)(x-\alpha_n)^d}{d!}$$

Notice that for $x - \alpha_n \equiv 0 \mod p^n$, in particular, for $x = \alpha_{n+1}$, every term of degree greater than 1 has a power of at least p^{n+1} in the numerator after reducing, so we can conclude that:

$$f(\alpha_n + a_n p^n) \equiv bp^n + f'(\alpha_n)(a_n p^n) \mod p^{n+1},$$

where $b \in \mathbb{Z}$ is determined by: $f(\alpha_n) = bp^n$. Since $f(\alpha_n) \equiv 0 \mod p^n$ we know $f'(\alpha_n) \not\equiv 0 \mod p$ because α_n reduces to $a \mod p$ and $f(a) \not\equiv 0 \mod p$. Then

$$f'(\alpha_n) \in (\mathbb{Z}/p^n\mathbb{Z})^\times.$$

If we want

$$f(\alpha_n + a_n p^n) \equiv 0 \mod p^{n+1}$$

then we need to get

$$bp^n + f'(\alpha_n) \cdot a_n p^n \equiv 0 \mod p^{n+1}$$

which implies

$$(b + f'(\alpha_n)a_n)p^n \equiv 0 \mod p^{n+1},$$

which reduces to:

$$b + f'(\alpha_n)a_n \equiv 0 \mod p.$$

This gives us a unique solution:

$$a_n \equiv \frac{-b}{f'(\alpha_n)} \mod p.$$

This defines the next order approximation modulo p^{n+1}:

$$\alpha_{n+1} = a_0 + a_1 p + \ldots + a_{n-1}p^{n-1} + a_n p^n,$$

and continuing in this fashion constructs the series for α as a limit of the α_n. □

Example 2.3. Can we solve $f(x) = x^2 - 2$ in $\mathbb{Z}_7$? Modulo 7 this has a solution.
Start with $a = 3$

$$f'(x) = 2x$$

$$f'(3) = 6 \not\equiv 0 \mod 7$$

$$\begin{aligned} f(3 + 7a_1) &= f(3) + f'(3)(7a_1) + 7^2(\ldots) \\ &= 7 + 6(7a_1) \mod 7^2 \\ &= (1 + 6a_1)7 \equiv 0 \mod 7^2 \end{aligned}$$

$$0 \equiv 1 + 6a_1 \mod 7 \implies 1 \equiv a_1 \mod 7$$

then $\alpha = 3 + 1 \cdot 7$. Now we have

$$\begin{aligned} f(3 + 7) + f'(3 + 7)(a_2 7^2) &\equiv 0 \mod 7^3 \\ f(10) + f'(10)(a_2 7^2) &\equiv 0 \mod 7^3 \\ (2 \cdot 7^2) + (6 + 2 \cdot 7)(a_2 7^2) &\equiv 0 \mod 7^3 \\ 7^2(2 + (6 + 2 \cdot 7)a_2) &\equiv 0 \mod 7^3 \\ 2 + a_2(6 + 2 \cdot 7) &\equiv 0 \mod 7 \\ 2 + 6a_2 &\equiv 0 \mod 7 \end{aligned}$$

thus $2 \equiv a_2 \mod 7$ so we now have $3 + 1 \cdot 7 + 2 \cdot 7^2 + \ldots$ which is a solution in $\mathbb{Z}_7$.

3. Local-to-Global Principle

The idea of the Global-to-Local Principle is trivial for our purposes. Because $\mathbb{Q}$ is contained in $\mathbb{R}$ and $\mathbb{Q}_p$ for all prime p, any solutions in the global $\mathbb{Q}$ guarantee that there is a solution in a local field. We are concerned with the reverse of this: the Local-to-Global Principle. The Local-to-Global Principle is the idea that if I can solve an equation in $\mathbb{Q}_p$ and $\mathbb{R}$, do solutions exist in $\mathbb{Q}$? Local solutions are usually easy to find in both $\mathbb{Q}_p$ and $\mathbb{R}$.

In $\mathbb{Q}_p$ we work modulo p, we can check if solutions exist modulo p, and then if such a solution exists, refine it with Hensel's lemma to find a solution in $\mathbb{Q}_p$. In $\mathbb{R}$ we can find roots with Newton's method where $f(\alpha) = 0$ and $f'(\alpha) \neq 0$. These are "decidable" questions from computability point of view. The problem is knowing whether a solutions exists globally after having found solutions locally. This is extremely difficult to answer, and in some cases are "undecidable". However, there are cases where a local-to-global principle does work, and one famous example is the Hasse-Minkowski Theorem:

Theorem 3.1 (Hasse-Minkowski)**.** A binary quadratic form (i.e., $f(x, y) = ax^2 + bxy + cy^2$) with coefficients in $\mathbb{Q}$ admits a nontrivial zero over $\mathbb{Q}$ if and only if it does so over $\mathbb{Q}_p$ for all prime numbers p and over $\mathbb{R}$.

In general the Local-to-Global Principle is not so easy to put in practice as there are obstructions to applying to higher degree equations (elliptic curves, for example). These obstructions are discussed in more detail in the paper of Mazur. [2] One of the main advantages of p-adic numbers is that they treat the "arithmetic" side of $\mathbb{Q}$ on equal footing with the "analytic" side: their construction is analogous to the reals, and the completions $\mathbb{Q}_p$ are treated like $\mathbb{R}$ in the local-to-global principle.

References

[1] F. Q. Gouvêa. *p-adic numbers*. Universitext. Springer-Verlag, Berlin, second edition, 1997. An introduction.

[2] B. Mazur. On the passage from local to global in number theory. *Bull. Amer. Math. Soc. (N.S.)*, 29(1):14–50, 1993.

[3] A. M. Robert. *A course in p-adic analysis*, volume 198 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2000.

E-mail address: kmhull@okstate.edu