P-ADIC NUMBERS

by

PAUL JAMES HOLLOWAY

A Thesis Submitted in Partial Fulfilment of
the Requirements for the Degree of

BACHELOR OF SCIENCE

in the Undergraduate Academic Unit of Mathematics and Statistics

Supervisor: Dr. Colin Ingalls

THE UNIVERSITY OF NEW BRUNSWICK

May 2014

Abstract

This paper focuses on the p-adic numbers and some of the properties of them. We start by defining a norm and the p-adic absolute value and prove that it is a norm on the rational numbers. In doing do we also show that the p-adic norm is a non-Archimedean norm which has strange properties compared to the ordinary (Archimedean) norm. Then we define the p-adic numbers and show that it is a field that is complete with respect to the p-adic norm. Then we introduce Hensel's lemma which we can use for showing that p-adic solutions exist to polynomial equations and then find them. Then we expand Hensel's lemma to apply to a system of multivariable polynomials, and show that Fermat's last theorem has p-adic solutions. Finally we extend the p-adic norm to finite field extensions of the p-adic numbers.

Table of Contents

Abstract **ii**

Table of Contents **iii**

Chapter 1. *p*-adic Numbers **1**

1.1 Norms 1
1.2 p-adic Norm 2
1.3 Review of building up Complex numbers 5
1.4 The field of p-adic numbers 7
1.5 Arithmetic in $\mathbb{Q}_p$ 12

Chapter 2. Hensel's Lemma **17**

2.1 Hensel's Lemma 17
2.2 Expanding Hensel's Lemma 19
2.3 Hensel's Lifting 24

Chapter 3. Field extensions of $\mathbb{Q}_p$ **29**

3.1 Field extensions of $\mathbb{Q}_p$ 29

Bibliography **37**

Chapter 1
p-adic Numbers

Before we can use the p-adic numbers we first have to define them, but to do that we will first need to define a few other basic terms.

1.1 Norms

Definition 1.1.1 Let X be a non-empty set. A **metric** on X is a function d taking a pairs of elements (x, y) of X to the non-negative real numbers such that:

(1) $d(x, y) = 0$ *iff* $x = y$

(2) $d(x, y) = d(y, x)$

(3) $d(x, y) \leq d(x, z) + d(z, y), \forall z \in X$ (triangle inequality).

A set with a metric, such as d in the definition above, is called a *metric space*.

Definition 1.1.2 A **norm**, denoted $\| \ \|$, on a field F is a map from F to the non-negative real numbers such that:

(1) $\|x\| = 0$ *iff* $x = 0$

(2) $\|x \cdot y\| = \|x\| \cdot \|y\|$

(3) $\|x+y\| \leq \|x\| + \|y\|$.

The metric d we are dealing with is $d(x,y) = \|x-y\|$. The normal absolute value, $|x|$, is an example of a norm on the rational numbers and the metric $d(x,y) = |x-y|$ is the usual concept of distance on the on the number line.

1.2 *p*-adic Norm

Now that we have a norm defined, we can work towards defining the p-adic norm.

Definition 1.2.1 Let p be any prime number. For any non-zero integer a, let $\mathrm{ord}_p\, a$ be the higest power p which divides a, i.e., the greatest m such that $a \equiv 0 \pmod{p^m}$. Recall that $a \equiv b \pmod{p} \Rightarrow c \mid (a-b)$.

Example 1.2.2 $\mathrm{ord}_5\, 125 = 3$, $\mathrm{ord}_5\, 50 = 2$, $\mathrm{ord}_2\, 32 = 5$, $\mathrm{ord}_2\, 96 = 5$, $\mathrm{ord}_7\, 98 = 2$, $\mathrm{ord}_7\, 99 = 0$ (we agree that if $a = 0$ then $\mathrm{ord}_p\, a = \infty$).

Note: These behave in a similiar fashion to logarithms:

$$\mathrm{ord}_p(a \cdot b) = \mathrm{ord}_p\, a + \mathrm{ord}_p\, b$$

$$\mathrm{ord}_p(a/b) = \mathrm{ord}_p\, a - \mathrm{ord}_p\, b$$

Also $\mathrm{ord}_p(ab+cd) \geq \min(\mathrm{ord}_p\, ab + \mathrm{ord}_p\, cd)$, because if n is the minimum order then $p^n|ab$, $p^n|cd$, and $p^n|(ab+cd)$.

Definition 1.2.3 Now we define the map $|\ |_p$ on $\mathbb{Q}$ as:

$$|x|_p = \begin{cases} 1/p^{\mathrm{ord}_p\, x}, & \text{if } x \neq 0 \\ 0, & \text{if } x = 0 \end{cases}$$

We call this map the **p-adic absolute value**.

Example 1.2.4 $|25|_5 = \frac{1}{5^2} = \frac{1}{25}$

$|25|_3 = \frac{1}{5^0} = 1$

$|\frac{18}{27}|_3 = \frac{3^3}{3^2} = \frac{27}{9} = 3$

$|1 - 50|_7 = |-49|_7 = \frac{1}{7^2} = \frac{1}{49}$ (7-adic "distance" between 1 and 50)

$|\frac{1}{9} + \frac{1}{16}|_5 = |\frac{25}{144}|_5 = \frac{5^0}{5^2} = \frac{1}{25}$ (5-adic "distance" between $\frac{1}{9}$ and $-\frac{1}{16}$).

Proposition 1.2.5 The p-adic absolute value $|\ |_p$ is a norm on $\mathbb{Q}$.

Proof: We need to check the three properties of a norm.

Property (1) says $|x|_p = 0$ *iff* $x = 0$. Let us assume $x = 0$, then by the definition of the p-adic norm $|x|_p = 0$. Now we assume $|x|_p = 0$, then:

$$|x| = 1/p^{\mathrm{ord}_p\, x} = 0 \Rightarrow \mathrm{ord}_p\, x = \infty \Rightarrow x = 0.$$

This proves property (1).

The second property of a norm states $|x \cdot y|_p = |x|_p \cdot |y|_p$, then:

$$|x \cdot y|_p = \frac{1}{p^{\mathrm{ord}_p(x \cdot y)}} = \frac{1}{p^{\mathrm{ord}_p\, x + \mathrm{ord}_p\, y}} = \frac{1}{p^{\mathrm{ord}_p\, x} \cdot p^{\mathrm{ord}_p\, y}} = \frac{1}{p^{\mathrm{ord}_p\, x}} \cdot \frac{1}{p^{\mathrm{ord}_p\, y}} = |x|_p \cdot |y|_p$$

this proves property (2).

Property (3) states $|x+y|_p \leq |x|_p + |y|_p$. If $x = 0, y = 0$, or $x+y = 0$ then property (3) becomes trivial, so let us assume they are all non-zero. Let $x = \frac{a}{b}$ and $y = \frac{c}{d}$, then $x + y = (ad + bc)/bd$. This implies that $\mathrm{ord}_p(x + y) = \mathrm{ord}_p(ad + bc) - \mathrm{ord}_p\, bd$. Now the higest power of p dividing $x + y$ is greater than or equal to the minimum of the higest power dividing x and the higest power dividing y:

$$\begin{aligned}
\mathrm{ord}_p(x + y) &\geq \min(\mathrm{ord}_p\, ad, \mathrm{ord}_p\, bc) - \mathrm{ord}_p\, bd \\
&= \min(\mathrm{ord}_p\, a + \mathrm{ord}_p\, d, \mathrm{ord}_p\, b + \mathrm{ord}_p\, c) - \mathrm{ord}_p\, b - \mathrm{ord}_p\, d \\
&= \min(\mathrm{ord}_p\, a - \mathrm{ord}_p\, b, \mathrm{ord}_p\, c - \mathrm{ord}_p\, d) \\
&= \min(\mathrm{ord}_p\, x, \mathrm{ord}_p\, y).
\end{aligned}$$

So, $|x+y|_p = 1/p^{\mathrm{ord}_p(x+y)} \leq \max(1/p^{\mathrm{ord}_p x}, 1/p^{\mathrm{ord}_p y}) = \max(|x|_p, |y|_p) \leq |x|_p + |y|_p$. This proves property (3) and thus finishes the proof. □

So we have now defined $|\ |_p$ to be the p-adic norm. But you might notice, from the proof, that this norm has a stronger property than an ordinary norm.

Definition 1.2.6 If $\|x+y\| \leq \max(\|x\|, \|y\|)$ for a norm always holds, then that norm is called **non-Archimedean**. If $d(x,y) \leq \max(d(x,z), d(z,y))$, then the metric defined by d is non-Archimedean. More particularly, a non-Archimedean metric is a metric that is induced by a non-Archimedean norm:
$d(x,y) = |x-y| = |(x-z)+(z-y)| \leq \max(|x-z|, |z-y|) = \max(d(x,z), d(z,y))$.

This is the stronger property that is mentioned above. In the proof above we showed that $|x+y|_p \leq \max(|x|_p, |y|_p)$. Thus, $|\ |_p$ is a non-Archimedean norm on $\mathbb{Q}$.

A norm or metric is called *Archimedean* simply if said norm or metric is not non-Archimedean. An example of an Archimedean norm on $\mathbb{Q}$ is the ordinary absolute value.

In any metric space X, a *Cauchy sequence* $\{a_0, a_1, a_2, \ldots\}$ of elements of X is defined that for any $\varepsilon > 0$, there exists an N such that $d(a_m, a_n) < \varepsilon$, when $n, m > N$.

If we have a metric d_1 on X and there is a sequence S that is Cauchy with respect to d_1, then a metric d_2 on X is *equivalent* to d_1 if and only if S is also Cauchy with respect to d_2. We say two norms are equivalent if they induce equivalent metrics.

The way we usually think about distance is obviously based on the Archimedean norm $\|\ \|$. The non-Archimedean metric has properties that seem unusual or strange, here is an example:

For any field the triangle inequality ($\|x+y\| \leq \|x\| + \|y\|$) says that the sum of two sides is greater than or equal to the third side. But what about when we have a non-Archimedean norm on a field? The triangle inequality for a non-Archimedean norm is $\|x+y\| \leq \max(\|x\|, \|y\|)$. Now suppose that $\|x\| < \|y\|$, then $\|x+y\| \leq \|y\|$. But $\|y\| = \|(x+y)-x\| \leq \max(\|x+y\|, \|x\|)$ and we have $\|y\| > \|x\|$ so $\|y\| \leq \|x+y\|$. This implies that $\|y\| = \|x+y\|$. This means that at least two sides of a "triangle" in a non-Archimedean field are equal, which means that every "triangle" is isosceles.

In the case of $|\ |_p$ on $\mathbb{Q}$, this says that if two rational numbers are divisible by different powers of p, then the sum of the two numbers is divisible by the lower power of p.

The "isosceles triangle principle" is what we call the non-Archimedean principle that $\|x \pm y\| \leq \max(\|x\|, \|y\|)$, with equality holding when $\|x\| \neq \|y\|$.

1.3 Review of building up Complex numbers

Now we have a new concept of distance between two rational numbers: if two rational numbers have a difference divisible by a large power of p, they are considered to be close. For us to work with the "p-adic metric" we have to expand $\mathbb{Q}$, the in a way similar to how the real numbers, $\mathbb{R}$, and then the complex number, $\mathbb{C}$, are constructed in the usual Archimedean metric $|\ |$.

Let us now review how this is done:

Let us start with the natural numbers, $\mathbb{N} = \{1, 2, 3, \ldots\}$. Evey step in going from $\mathbb{N}$ to $\mathbb{C}$ can be analyzed in terms of a desire to do two things:

(1) Solve polynomial equations

(2) Find the limit of Cauchy sequences (i.e., "complete" the number system such

that every Cauchy sequence has a limit in the new number system).

From $\mathbb{N}$ we can introduce the integers, $\mathbb{Z}$, as solutions to equations of the form:

$$a + x = b \quad a, b \in \mathbb{N}.$$

Now the rationals can be introduced as solutions to equations of the form:

$$ax = b \quad a, b \in \mathbb{Z}.$$

One way to build up the real numbers is to consider the set S of Cauchy sequences of rational numbers. Let $s_1 = \{a_j\} \in S$ and $s_2 = \{b_j\} \in S$ be two Cauchy sequences that are equivalent, and write $s_1 \sim s_2$ if $|a_j - b_j| \to 0$ as $j \to \infty$. We now define $\mathbb{R}$ to be the set of *equivalence classes* of Cauchy sequences of rational numbers.

Showing that $\mathbb{R}$ is a field by defining addition, multiplication, and the additive and multiplicative inverses of the equivalence classes of the Cauchy sequences is not hard.

Next, we wanted numbers that could solve $x^2 + 1 = 0$. Then when $i = \sqrt{-1}$ was introduced and the field of complex numbers of the form:

$$a + bi \quad a, b \in \mathbb{R}.$$

was defined, it turned out that $\mathbb{C}$ was algebraically closed (this means that every polynomial equation with coefficients in $\mathbb{C}$ have solutions in $\mathbb{C}$. This is the fundamental theorem of algebra) and $\mathbb{C}$ is complete with respect to a unique norm ($|a + bi| = \sqrt{a^2 + b^2}$) that extends the usual norm $|\ |$ on $\mathbb{R}$.

Since $\mathbb{C}$ is complete the process of finding field extensions stops here. The completion of $\mathbb{C}$ was done with only a quadratic extension of $\mathbb{R}$, which means it was obtained by adjoining solutions to the quadratic equation $x^2 + 1 = 0$. So $\mathbb{C}$ is algebraically

closed with respect to the Archimedean metric, but it is not algebraically closed with respect to $|\ |_p$.

1.4 The field of p-adic numbers

Let $\{a_i\}$ be a sequence of rational numbers such that, if given an $\varepsilon > 0$, there exists an N such that $|a_i - a_j|_p < \varepsilon$ if both $i, j > N$. For two Cauchy sequences $\{a_i\}$ and $\{b_i\}$, if $|a_i - b_i|_p \to 0$ as $i \to \infty$, then the two Cauchy sequences are equivalent. The set of equivalence classes of Cauchy sequences we call $\mathbb{Q}_p$, the p-adic numbers.

Definition 1.4.1 The p-adic norm of an equivalence class a is $\lim_{i\to\infty} |a_i|_p$, where $\{a_i\}$ is any representative of a.

If we have two equivalence classes a and b of Cauchy sequences with representatives $\{a_i\}$ and $\{b_i\}$ respectively, we can define $a \cdot b$ to be the equivalence class that is represented by the Cauchy sequence $\{a_i b_i\}$. If we also have $\{a'_i\}$ and $\{b'_i\}$ then we would have

$$\begin{aligned} |a'_i b'_i - a_i b_i|_p &= |a'_i(b'_i - b_i) + b_i(a'_i - a_i)|_p \\ &\leq \max(|a'_i(b'_i - b_i)|_p, |b_i(a'_i - a_i)|_p). \end{aligned}$$

The expressions approach $|a|_p \cdot \lim |b'_i - b_i|_p = 0$ and $|b|_p \cdot \lim |a'_i - a_i|_p = 0$ as $i \to \infty$. This implies that $\{a'_i b'_i\} \sim \{a_i b_i\}$.

The multiplicative inverse $\{1/a_i\}$ will be Cauchy unless $|a_i|_p \to 0$. And if $\{a_i\} \sim \{a'_i\}$, then $a_i = a'_i$ for all i, then $1/a_i = 1/a'_i$, which implies $\{1/a_i\} \sim \{1/a'_i\}$ (if all a_i and a'_i are non-zero).

Now we define $a + b$ to be equivalence class represented by the Cauchy sequence $\{a_i + b_i\}$. Once again if we have another two Cauchy sequences then we would have:

$$\begin{aligned} |(a_i' + b_i') - (a_i + b_i)|_p &= |a_i' - a_i + b_i' - b_i|_p \\ &\leq \max(|a_i' - a_i|_p, |b_i' - b_i|_p) \end{aligned}$$

As $i \to \infty$ the two expressions go to $\lim(|a_i' - a_i|_p) = 0$ and $\lim(|b_i' - b_i|_p) = 0$ respectively. Hence $\{a_i' + b_i'\} \sim \{a_i + b_i\}$. The additive inverse is defined very easily.

Now with addition, multiplication,and inverses as defined above we show that the set of equivalence classes of Cauchy sequences, $\mathbb{Q}_p$, is a field.

Let the Cauchy sequences $\{a_i\}, \{b_i\}, \{c_i\}$ be representatives of $a, b, c \in \mathbb{Q}_p$.

Now let us check for the distributive law; $a(b + c)$ is the equivalence class of:

$$\{a_i(b_i + c_i)\} = \{a_i b_i + a_i c_i\}.$$

So $ab + ac$ is also an equivalence class. Hence $a(b + c) = ab + bc$, so the distributive law holds.

Now the associative law; $a + (b + c)$ is the equivalence class of:

$$\{a_i + (b_i + c_i)\} = \{a_i + b_i + c_i\} = \{(a_i + b_i) + c_i\}.$$

So $(a + b) + c$ is also an equivalence class. Hence $a + (b + c) = (a + b) + c$, so the associative law holds.

Now commutative law; $a + b$ is the equivalence class of:

$$\{a_i + b_i\} = \{b_i + a_i\}.$$

So $b + a$ is also an equivalence class. Hence $a + b = b + a$, so the commutative law holds. This proves that $\mathbb{Q}_p$ is a field.

Proposition 1.4.2 The field of p-adic numbers, $\mathbb{Q}_p$, is complete with respect to $|\ |_p$.

Proof: Suppose we have a Cauchy sequence $\{x_n\}$ in $\mathbb{Q}_p$. Then given an $\varepsilon > 0$, there exists an N such that $|x_i - x_j| < \varepsilon$ when $i, j > N$. Now let $\varepsilon = 1/p^k$, then since $\{x_i\}$ is Cauchy, then $|x_i - x_j|_p < 1/p^k$ which implies:

$$1/p^{\mathrm{ord}_p(x_i - x_j)} < 1/p^k \Longrightarrow p^{\mathrm{ord}_p(x_i - x_j)} > p^k \Longrightarrow \mathrm{ord}_p(x_i - x_j) > k.$$

But this implies that the first k terms of x_i and x_j are the same, and this is the same as making the sequence terms arbitrarily close to some p-adic number. So any sequence in $\mathbb{Q}_p$ that is Cauchy with respect to $|\ |_p$ will converge. Thus the field $\mathbb{Q}_p$ is Complete. □

Lemma 1.4.3 If $x \in \mathbb{Q}$ and $|x|_p \leq 1$, then for any i there exists an integer α such that $|\alpha - x|_p \leq p^i$. We can choose α the set $\{0, 1, 2, \ldots, p^i - 1\}$.

Proof: Let $x = \frac{a}{b}$ be in lowest terms. Now p does not divide b since $|x|_p \leq 1$, so b and p^i are relatively prime. So now we can find integers n, m such that $mb - np^i = 1$. Now let $\alpha = am$ and we have:

$$\begin{aligned} |\alpha - x|_p &= \left|am - \frac{a}{b}\right|_p = \left|\frac{a}{b}(mb - 1)\right|_p = \left|\frac{a}{b}\right|_p |mb - 1|_p \\ &\leq |mb - 1|_p \\ &= |np^i|_p = |n|_p / p^i \\ &= 1/p^i. \end{aligned}$$

Now, we can add a multiple of p^i to α to get a number in the set $\{0, 1, 2, \ldots, p^i - 1\}$ for which $|\alpha - x|_p \leq \frac{1}{p^i}$ still holds. This proves the lemma. □

Theorem 1.4.4 Evey equivalence class $a \in \mathbb{Q}_p$ for which $|a|_p \leq 1$ has exactly one representative Cauchy sequence of the form $\{a_i\}$ for which:

(1) $0 \leq a_i < p^i$, for $i = 1, 2, 3, \ldots$

(2) $a_i \equiv a_{i+1} \pmod{p^i}$, for $i = 1, 2, 3, \ldots$

Proof: First we have to prove uniqueness. Assume $\{a_i'\} \neq \{a_i\}$ is also a sequence that satisfies properties (1) and (2). If $a_{i_0}' \neq a_{i_0}$ then $a_{i_0}' \not\equiv a_{i_0} \pmod{p^{i_0}}$, since both a_{i_0}', a_{i_0} are in the set $\{0, 1, 2, \ldots, p^i - 1\}$. Then, for all $i \geq i_0$, we will have $a_i \equiv a_{i_0} \not\equiv a_i' \equiv a_{i_0}' \pmod{p^{i_0}}$, which implies $a_i \not\equiv a_i'$. So

$$|a_i - a_i'|_p \leq \frac{1}{p^{i_0}}, \text{ for all } i \geq i_0$$

Hence, $\{a_i\} \not\sim \{a_i'\}$.

Now suppose that we have a Cauchy sequence $\{b_i\}$, we want to find a similar sequence $\{a_i\}$ that satisfy (1) and (2). For every $j = 1, 2, 3, \ldots$, let $N(j)$ be a natural number such that $|b_i - b_{i'}|_p \leq 1/p^j$, when $i, i' \geq N(j)$. For all $i' \geq N(1)$, if $i \geq N(1)$ then

$$\begin{aligned} |b_i|_p &\leq \max(|b_{i'}|_p, |b_i - b_{i'}|_p) \\ &\leq \max(|b_{i'}|_p, \frac{1}{p}) \end{aligned}$$

which implies that $|b_i|_p \leq 1$ and as $i' \to \infty, |b_{i'}|_p \to |a|_p \leq 1$.

Using the lemma above we can find a sequence of integers $a_j \in \{0, 1, 2, \ldots, p_j\}$, such that $|a_j - b_{N(j)}|_p \leq 1/p^j$. For $\{a_j\}$ to be such a sequence we need $a_{j+1} \equiv a_j \pmod{p^j}$ and $\{b_i\} \sim \{a_j\}$.

$$\begin{aligned} |a_{j+1} - a_j|_p &= |a_{j+1} - b_{N(j+1)} + b_{N(j+1)} - b_{N(j)} - (a_j - b_{N(j)})|_p \\ &\leq \max(|a_{j+1} - b_{N(j+1)}|_p, |b_{N(j+1)} - b_{N(j)}|_p, |a_j - b_{N(j)}|_p) \\ &\leq \max(1/p^{j+1}, 1/p^j, 1/p^j) \\ &= 1/p^j. \end{aligned}$$

This implies that $a_{j+1} \equiv a_j \pmod{p^j}$.

$$\begin{aligned}
|a_i - b_i|_p &= |a_i - a_j + a_j - b_{N(j)} - (b_i - b_{N(j)})|_p \\
&\leq \max(|a_i - a_j|_p, |a_j - b_{N(j)}|_p, |b_i - b_{N(j)}|_p) \\
&\leq \max(1/p^j, 1/p^j, 1/p^j) \\
&= 1/p^j.
\end{aligned}$$

As $i \to \infty, |a_i - b_i|_p \to 0$ which implies that $\{a_i\} \sim \{b_i\}$. This proves the theorem. $\square$

If $a \in \mathbb{Q}_p$ does not satisfy $|a|_p \leq 1$, then we can multiply a by the power of p that equals $|a|_p$, say the m^{th} power of p, to get an $a' = ap^m \in \mathbb{Q}_p$ that does satisfy $|a'|_p \leq 1$. Then, as in the theorem, a' is represented by the sequence $\{a'_i\}$ and $a = a'/p^m$ is represented by the sequence $\{a_i\}$.

We can now write all a'_i in the sequence $\{a'_i\}$ to the base p with coefficients $b_0, b_1, \ldots, b_{i-1} \in \{0, 1, 2, \ldots, p-1\}$:

$$a'_i = b_0 + b_1 p + b_2 p^2 + \ldots + b_{i-1} p^{i-1}.$$

The condition $a'_i \equiv a'_{i+1} \pmod{p^i}$ means that:

$$a'_{i+1} = b_0 + b_1 p + b_2 p^2 + \ldots + b_{i-1} p^{i-1} + b_i p^i.$$

So a'_i can be thought of as a number to the base p.

Then the original p-adic number a can be thought of as decimal number to the base p that has finitely many digits corresponding to negative powers of p, but infinitely many digits corresponding to positive powers of p:

$$a = \frac{b_0}{p^m} + \frac{b_1}{p^{m-1}} + \frac{b_2}{p^{m-2}} + \ldots + \frac{b_{m-1}}{p} + b_m + b_{m+1} p + b_{m+2} p^2 + \ldots$$

We call this equality the "p-adic expansion" of of a.

We define the set of p-adic integers to be:

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

Let $a \in \mathbb{Q}_p$ then, $|a|_p = 1/p^{\text{ord}_p\, a} \leq 1 \implies \text{ord}_p\, a \geq 0 \implies$ all powers of p are positive. So if the p-adic expansion of a numbers in $\mathbb{Q}_p$ has no negative powers of p, that number is a p-adic integer. Addition and multiplication in $\mathbb{Z}_p$ is closed so $\mathbb{Z}_p$ is a subring of $\mathbb{Q}_p$.

Now we define the p-adic units to be:

$$\mathbb{Z}_p^* = \{x \in \mathbb{Z}_p \mid 1/x \in \mathbb{Z}_p\} = \{x \in \mathbb{Z}_p \mid |x|_p = 1\} = \{x \in \mathbb{Z}_p \mid x \not\equiv 0 \pmod{p}\}.$$

Theorem 1.4.5 A series converges in $\mathbb{Q}_p$ *iff* its terms approach zero.

Proof: Suppose that $\{a_i\}$ is a sequence in $\mathbb{Q}_p$ such that $|a_i|_p \to 0$ as $i \to \infty$. Then the partial sums $S_n = a_0 + a_1 + \ldots + a_n$ are Cauchy since for $n > m$:

$$|S_n - S_m|_p = |a_{m+1} + \ldots + a_n|_p \leq \max(|a_{m+1}|_p, \ldots, |a_n|_p)$$

which goes to zero and both $n, m \to \infty$. Since $\mathbb{Q}_p$ is complete this implies convergence.

Now suppose we have a series that converges in $\mathbb{Q}_p$, then it is Cauchy. Given an $\varepsilon > 0$ there exists an N such that for $n, m > N$, $|S_n - S_m|_p < \varepsilon$. In particular $|S_{n+1} - S_n|_p = |a_{n+1}|_p < \varepsilon$. Thus as $n \to \infty$, the terms approach zero. □

1.5 Arithmetic in $\mathbb{Q}_p$

Addition, subtraction, multiplication, and division of the p-adic numbers works a lot like the same operations on decimals, but with p-adic numbers you work from left to right instead of right to left.

Example 1.5.1 Some examples in $\mathbb{Q}_7$:

(a)
$$\begin{array}{rccccccc}
 & 6 & + & 3\cdot 7 & + & 2\cdot 7^2 & + & \dots \\
\times & 4 & + & 1\cdot 7 & + & 5\cdot 7^2 & + & \dots \\
\hline
 & 3 & + & 1\cdot 7 & + & 3\cdot 7^2 & + & \dots \\
 & & & 6\cdot 7 & + & 3\cdot 7^2 & + & \dots \\
+ & & & & & 2\cdot 7^2 & + & \dots \\
\hline
 & 3 & + & 0\cdot 7 & + & 2\cdot 7^2 & + & \dots
\end{array}$$

(b)
$$\begin{array}{rccccccc}
 & 3\cdot 7^{-1} & + & 2\cdot 7^0 & + & 2\cdot 7^1 & + & \dots \\
- & 4\cdot 7^{-1} & + & 4\cdot 7^0 & + & 5\cdot 7^1 & + & \dots \\
\hline
 & 6\cdot 7^{-1} & + & 4\cdot 7^0 & + & 3\cdot 7^1 & + & \dots
\end{array}$$

(c)
$$\begin{array}{r|l}
 & 5 + 1\cdot 7 + 6\cdot 7^2 + \dots \\
\hline
3+5\cdot 7+1\cdot 7^2+\dots \;\Big)\; & 1 + 2\cdot 7 + 4\cdot 7^2 + \dots \\
 & 1 + 6\cdot 7 + 1\cdot 7^2 + \dots \\
\hline
 & 3\cdot 7 + 2\cdot 7^2 + \dots \\
 & 3\cdot 7 + 5\cdot 7^2 + \dots \\
\hline
 & 4\cdot 7^2 + \dots \\
 & 4\cdot 7^2 + \dots \\
\hline
\end{array}$$

If $a = \sum_{i=k}^{\infty} a_i p^i$ is the p-adic expansion of a, where $k < 0$, then another way to represent the p-adic expansion is $\dots a_4 a_3 a_2 a_1 a_0 . a_{-1} a_{-2} \dots a_k$. An example is if $b = 2p^{-2} + 6p^{-1} + 1 + 2p + 3p^2 + 5p^3 + \dots$, then b can also be represented as $b = \dots 5321.62$.

The example 1.5.1(a) above can also be represented like this:

$$\begin{array}{rr} & \ldots 236 \\ \times & \ldots 514 \\ \hline & \ldots 313 \\ & \ldots 360 \\ + & \ldots 200 \\ \hline & \ldots 346 \end{array}$$

Which as you can see makes it easier to represent more digits in a p-adic number.

Here are a few interesting things about p-adic numbers, 7-adics particularly in this case:

$$\begin{array}{rr} & \ldots 3333334 \\ + & \ldots 3333334 \\ \hline & \ldots 0000001 \end{array} \qquad \begin{array}{rr} & \ldots 6666666 \\ + & \ldots 0000001 \\ \hline & \ldots 0000000 \end{array}$$

Since a 7-adic integer added to itself equals 1, this implies that "one-half" is a 7-adic integer. Also $\ldots 666666$ is -1 in the 7-adics since we added 1 to it and got 0.

Now let us try to see if $\sqrt{n}$ is in $\mathbb{Q}_p$, where $n \in \mathbb{Z}$. In other words we want to find $a_0, a_1, a_2, \ldots \ ; \ 0 \leq a_i \leq (p-1)$, such that $(a_0 + a_1 \cdot p + a_2 \cdot p^2 + \ldots)^2 = n$

Example 1.5.2 Let us try with $n = 2$ and $p = 7$ (i.e., is $\sqrt{2}$ in $\mathbb{Q}_7$?).

$$\begin{aligned} (a_0 + a_1 \cdot 7 + a_2 \cdot 7^2 + \ldots)^2 &= 2 + 0 \cdot 7 + 0 \cdot 7^2 + \ldots \\ (a_0 + a_1 \cdot 7 + a_2 \cdot 7^2 + \ldots)^2 &= 2 \\ \Rightarrow a_0^2 &\equiv 2 \pmod 7 \\ a_0^2 &\equiv 9 \pmod 7 \\ a_0 &\equiv 3 \pmod 7 \end{aligned}$$

So set $a_0 = 3$

$$\begin{aligned}
\text{So now we have: } (3 + a_1 \cdot 7)^2 &\equiv 2 && \pmod{7^2} \\
9 + 6a_1 \cdot 7 &\equiv 2 && \pmod{7^2} \\
6a_1 \cdot 7 &\equiv -7 && \pmod{7^2} \\
6a_1 &\equiv -1 && \pmod{7} \\
6a_1 &\equiv 6 && \pmod{7} \\
a_1 &\equiv 1 && \pmod{7} \\
\text{So set } a_1 &= 1
\end{aligned}$$

$$\begin{aligned}
\text{Now we have: } (3 + 1 \cdot 7 + a_2 \cdot 7^2)^2 &\equiv 2 && \pmod{7^3} \\
(10 + a_2 \cdot 7^2) &\equiv 2 && \pmod{7^3} \\
100 + 20a_2 \cdot 7^2 &\equiv 2 && \pmod{7^3} \\
20a_2 \cdot 7^2 &\equiv -98 && \pmod{7^3} \\
20a_2 &\equiv -2 && \pmod{7} \\
6a_2 &\equiv 12 && \pmod{7} \\
a_2 &\equiv 2 && \pmod{7} \\
\text{So set } a_2 &= 2
\end{aligned}$$

By Hensel's lemma, introduced in the next chapter, we can continue on this pattern and we get:

$$(3 + 1 \cdot 7 + 2 \cdot 7^2 + \ldots) = \sqrt{2} \in \mathbb{Q}_7.$$

Example 1.5.3 What about $n = 3$ and $p = 7$?

$$\begin{aligned}
(a_0 + a_1 \cdot 7 + a_2 \cdot 7^2 + \ldots)^2 &= 3 + 0 \cdot 7 + 0 \cdot 7^2 + \ldots \\
(a_0 + a_1 \cdot 7 + a_2 \cdot 7^2 + \ldots)^2 &= 3 \\
a_0^2 &\equiv 3 \pmod{7}
\end{aligned}$$

$$1^2 = 1,\ 2^2 = 4,\ 3^2 = 9 \equiv 2,\ 4^2 = 16 \equiv 2,\ 5^2 = 25 \equiv 4,\ 6^2 = 36 \equiv 1 \pmod 7.$$

As you can see no squares are equivalent to 3 (mod 7), so $a_0^2 \not\equiv 3 \pmod 7$, which implies $\sqrt{3} \notin \mathbb{Q}_7$.

Chapter 2
Hensel's Lemma

2.1 Hensel's Lemma

We now want to find p-adic solutions to polynomial equations, to do this we use Hensel's lemma.

Theorem 2.1.1 (Hensel's Lemma):

Let $F(x) = c_0 + c_1x + c_2x^2 + \ldots + c_nx^n$ be a polynomial whose coefficients are integers, with formal derivative $F'(x) = c_1 + 2c_2x + 3c_3x^2 + \ldots + nc_nx^{n-1}$. Let a_0 be in $\{0, 1, \cdots p-1\}$ such that $F(a_0) \equiv 0 \pmod{p}$ and $F'(a_0) \not\equiv 0 \pmod{p}$. Then there exists a unique p-adic integer a such that $F(a) = 0$ and $a \equiv a_0 \pmod{p}$.

Proof: We need to find a p-adic integer a such that $F(a) \equiv 0 \pmod{p^n}$ for all n which implies $F(a) = 0$. We need to construct a sequence of integers $a_1, a_2, a_3, \ldots$, such that the following 3 properties all hold when $n \geq 1$:

(1) $F(a_n) \equiv 0 \pmod{p^{n+1}}$

(2) $a_n \equiv a_{n-1} \pmod{p^n}$

(3) $0 \leq a_n < p^{n+1}$.

We use induction on n to prove that such an a_n exists.

Let us begin with $n = 1$, then there is a unique integer $\tilde{a}_0 \in \{0, 1, \ldots, p-1\}$ such that $\tilde{a}_0 \equiv a_0 \pmod{p}$. We need an a_1 that satisfies (2) and (3), so we need $a_1 \equiv a_0 \pmod{p^2}$ where $a_1 \in \{0, 1, \ldots, p^2 - 1\}$, this implies $a_1 = \tilde{a}_0 + b_1 p$, where $b_1 \in \{0, 1, \ldots, p-1\}$. Now we check property (1); since we are looking for solutions mod p^2, then any term where the power of p is 2 or more can be ignored:

$$\begin{aligned} F(a_1) = F(\tilde{a}_0 + b_1 p) &= \sum_{i=0}^{n} c_i (\tilde{a}_0 + b_1 p)^i \\ &= \sum_{i=0}^{n} (c_i \tilde{a}_0^i + i c_i \tilde{a}_0^{i-1} b_1 p + \text{terms divisible by } p^2) \\ &\equiv \sum_{i=0}^{n} c_i \tilde{a}_0^i + (\sum_{i=0}^{n} i c_i \tilde{a}_0^{i-1}) b_1 p \pmod{p^2} \\ &= F(\tilde{a}_0) + F'(\tilde{a}_0) b_1 p. \end{aligned}$$

Since $a_0 \equiv \tilde{a}_0 \pmod{p}$, then $F(a_0) \equiv F(\tilde{a}_0) \equiv 0 \pmod{p}$, then we can write $F(\tilde{a}_0) \equiv \alpha p \pmod{p^2}$ for some $\alpha \in \{0, 1, \ldots, p-1\}$. So in order to get $F(a_1) \equiv 0 \pmod{p^2}$ we must get $\alpha p + F'(\tilde{a}_0) b_1 p \equiv 0 \pmod{p^2}$ which is equivalent to $\alpha + F'(\tilde{a}_0) b_1 \equiv 0 \pmod{p}$. But, since $F'(\tilde{a}_0) \equiv F'(a_0) \not\equiv 0 \pmod{p}$, then we can solve for c_1. By using lemma 1.4.3 then we let $b_1 \in \{0, 1, \ldots, p-1\}$ be a unique integer so that $b_1 \equiv \frac{-\alpha}{F'(\tilde{a}_0)} \pmod{p}$. This b_1 for $a_1 = \tilde{a}_0 + b_1 p$ satisfies properties (1), (2), and (3).

Continuing with the induction, suppose we already have already found $a_1, a_2, \ldots, a_{n-1}$ that satisfy (1), (2), and (3). We want to find a_n that satisfy (2) and (3), So $a_n = a_{n-1} + b_n p^n$ with $b_n \in \{0, 1, \ldots, p-1\}$. We expand $F(a_{n-1} + b_n p^n)$ like we did in the first step of induction, but now terms that divisible by p^{n+1} are ignored:

$$\begin{aligned} F(a_n) &= F(a_{n-1} + b_n p^n) \\ &\equiv F(a_{n-1}) + F'(a_{n-1}) b_n p^n \pmod{p^{n+1}}. \end{aligned}$$

We know that $F(a_{n-1}) \equiv 0 \pmod{p^n}$ so we can write, by the induction assumption, $F(a_{n-1}) \equiv \beta p^n \pmod{p^{n+1}}$, now $F(a_n) \equiv 0 \pmod{p^{n+1}}$ becomes:

$$\beta p^n + F'(a_{n-1}) b_n p^n \equiv 0 \pmod{p^{n+1}}$$

$$\beta + F'(a_{n-1}) b_n \equiv 0 \pmod{p}.$$

Since $a_{n-1} \equiv a_0 \pmod{p}$, then like before $F'(a_{n-1}) \equiv F'(a_0) \not\equiv 0 \pmod{p}$, now we an find $b_n \in \{0, 1, \ldots, p-1\}$. Proceeding like we did when looking for b_1, we solve $b_n \equiv \frac{-\beta}{F'(a_{n-1})} \pmod{p}$. This $a_n = a_{n-1} + b_n p^n$ satisfies (1), (2), and (3) and proves the claim.

Now, let

$$a = \tilde{a}_0 + b_1 p + b_2 p^2 + \ldots$$

Notice that $a \equiv a_n \pmod{p^{n+1}}$, so $F(a) \equiv F(a_n) \equiv 0 \pmod{p^{n+1}}$, for all n, it follows that the p-adic number $F(a) = 0$. Also $a = \tilde{a}_0 + b_1 p + b_2 p^2 + \ldots$ gives a unique sequence of a_n as in the claim, and that uniqueness implies the uniqueness of a. This proves Hensel's lemma. □

Now to apply Hensel's lemma. Finding $\sqrt{2} \in \mathbb{Q}_7$, like in example 1.5.2, is the same as finding p-adic solutions to the polynomial $x^2 - 2 = 0$.

Example 2.1.2 Let $f(x) = x^3 + 2x^2 + 2x + 4$, let us look for 5-adic solutions. You will notice that $x_0 = 3$ is a solution to $f(x_0) \equiv 0 \pmod{5}$. Also $f'(x_0) = 3x_0^2 + 4x_0 + 2 = 27 + 12 + 2 = 41 \not\equiv 0 \pmod{5}$. So $f(x)$ satisfies Hensel's lemma, this implies that there exists a unique p-adic number, x, that solves $f(x) = 0$.

2.2 Expanding Hensel's Lemma

Now we will expand Hensel's lemma to apply to a system of multivariable polynomials, as long as there are as many polynomials as variables.

Theorem 2.2.1 Let $f(x,y)$ and $g(x,y)$ be multivariable polynomials with integer coefficients and a Jacobian matrix of:

$$J(x,y) = \begin{pmatrix} \frac{\partial f}{\partial x} & \frac{\partial f}{\partial y} \\ \frac{\partial g}{\partial x} & \frac{\partial g}{\partial y} \end{pmatrix}$$

Let $x_0, y_0 \in \{0, 1, \ldots, p-1\}$ such that $f(x_0, y_0) \equiv g(x_0, y_0) \equiv 0 \pmod{p}$ and $\det\big(J(x_0, y_0)\big) \not\equiv 0 \pmod{p}$. Then there exists a unique x and y belonging to the p-adic integers such that $f(x,y) = g(x,y) = 0$ and $x \equiv x_0$ and $y \equiv y_0 \pmod{p}$.

Proof: First we construct two series $x_1, x_2, x_3, \ldots$ and $y_1, y_2, y_3, \ldots$ all in $\{0, 1, \ldots, p-1\}$ such that these three properties all hold for when $n \geq 1$:

(1) $f(x_n, y_n) \equiv g(x_n, y_n) \equiv 0 \pmod{p^{n+1}}$

(2) $x_n \equiv x_{n-1}, y_n \equiv y_{n-1} \pmod{p^n}$

(3) $0 \leq x_n, y_n < p^{n+1}$.

Let $n = 1$ to start this off. Choose $x_0, y_0 \in \{0, 1, \ldots, p-1\}$ that satisfy $f(x_0, y_0) \equiv g(x_0, y_0) \equiv 0 \pmod{p}$ and $\det(J(x_0, y_0)) \not\equiv 0 \pmod{p}$. Now we need x_1, y_1 that satisfy properties (2) and (3) above, so $x_1 = x_0 + t_1 p$ and $y_1 = y_0 + s_1 p$, where $t_1, s_1 \in \{0, 1, \ldots, p-1\}$. Then using multivariable Taylor series we get

$$\begin{aligned} f(x_1, y_1) &= f(x_0 + t_1 p, y_0 + s_1 p) \\ &\equiv f(x_0, y_0) + \frac{\partial f(x_0, y_0)}{\partial x}[(x_0 + t_1 p) - x_0] + \frac{\partial f(x_0, y_0)}{\partial y}[(y_0 + s_1 p) - y_0] \pmod{p^2} \\ &\equiv f(x_0, y_0) + \frac{\partial f(x_0, y_0)}{\partial x} t_1 p + \frac{\partial f(x_0, y_0)}{\partial y} s_1 p \pmod{p^2}. \end{aligned}$$

We ignore the later terms of the multivariable Taylor series because all of the later terms are divisible by p^2. The exact same process for g.

Since $f(x_0, y_0) \equiv g(x_0, y_0) \equiv 0 \pmod{p}$ this implies that $f(x_0, y_0) \equiv \alpha_1 p \pmod{p^2}$ and $g(x_0, y_0) \equiv \beta_1 p \pmod{p^2}$, for some $\alpha_1, \beta_1 \in \{0, 1, \ldots, p-1\}$. Since we are looking for x_1, y_1 to satisfy property (1), we are looking for $f(x_1, y_1) \equiv 0 \pmod{p^2}$. This implies that:

$$\begin{aligned} f(x_1, y_1) &= f(x_0 + t_1 p, y_0 + s_1 p) \\ &\equiv \alpha_1 p + \frac{\partial f(x_0, y_0)}{\partial x} t_1 p + \frac{\partial f(x_0, y_0)}{\partial y} s_1 p \equiv 0 \pmod{p^2} \\ &\equiv \alpha_1 + \frac{\partial f(x_0, y_0)}{\partial x} t_1 + \frac{\partial f(x_0, y_0)}{\partial y} s_1 \equiv 0 \pmod{p} \\ &\equiv \frac{\partial f(x_0, y_0)}{\partial x} t_1 + \frac{\partial f(x_0, y_0)}{\partial y} s_1 \equiv -\alpha_1 \pmod{p}. \end{aligned}$$

Do the same for g and get:

$$g(x_1, y_1) \equiv \frac{\partial g(x_0, y_0)}{\partial x} t_1 + \frac{\partial g(x_0, y_0)}{\partial y} s_1 \equiv -\beta_1 \pmod{p}.$$

Now we have:

$$\begin{pmatrix} \frac{\partial f(x_0,y_0)}{\partial x} & \frac{\partial f(x_0,y_0)}{\partial y} \\ \frac{\partial g(x_0,y_0)}{\partial x} & \frac{\partial g(x_0,y_0)}{\partial y} \end{pmatrix} \begin{pmatrix} t_1 \\ s_1 \end{pmatrix} \equiv \begin{pmatrix} -\alpha_1 \\ -\beta_1 \end{pmatrix}$$

and by using Cramer's rule we can uniquely solve for t_1 and s_1. Since t_1 and s_1 are unique it implies that $x_1 = x_0 + t_1 p$ and $y_1 = y_0 + s_1 p$ are also unique. These x_1, y_1 satisfy (1), so this proves this step of induction.

Now assume we found that the three properties hold for when $n = 2, 3, \ldots, i-1$, we will now see if it holds for $n = i$. We want x_i, y_i that satisfy properties (2) and (3) above, so $x_i = x_{i-1} + t_i p^i$ and $y_i = y_{i-1} + s_i p^i$, where $t_i, s_i \in \{0, 1, \ldots, p-1\}$. Then

$$\begin{aligned} f(x_i, y_i) &= f(x_{i-1} + t_i p^i, y_{i-1} + s_i p^i) \\ &\equiv f(x_{i-1}, y_{i-1}) + \frac{\partial f(x_{i-1}, y_{i-1})}{\partial x} t_i p^i + \frac{\partial f(x_{i-1}, y_{i-1})}{\partial y} s_i p^i \pmod{p^{i+1}}. \end{aligned}$$

The exact same process for g.

Since $f(x_{i-1}, y_{i-1}) \equiv g(x_{i-1}, y_{i-1}) \equiv 0 \pmod{p^i}$ this implies that $f(x_{i-1}, y_{i-1}) \equiv \alpha_i p^i \pmod{p^{i+1}}$ and $g(x_{i-1}, y_{i-1}) \equiv \beta_i p^i \pmod{p^{i+1}}$, where $\alpha_i, \beta_i \in \{0, 1, \ldots, p-1\}$. We are looking for $f(x_i, y_i) \equiv 0 \pmod{p^{i+1}}$. This implies that:

$$\begin{aligned} f(x_i, y_i) &\equiv \alpha_i p + \frac{\partial f(x_{i-1}, y_{i-1})}{\partial x} t_i p^i + \frac{\partial f(x_{i-1}, y_{i-1})}{\partial y} s_i p^i \equiv 0 \pmod{p^{i+1}} \\ &\equiv \alpha_i + \frac{\partial f(x_{i-1}, y_{i-1})}{\partial x} t_i + \frac{\partial f(x_{i-1}, y_{i-1})}{\partial y} s_i \equiv 0 \pmod{p} \\ &\equiv \frac{\partial f(x_{i-1}, y_{i-1})}{\partial x} t_i + \frac{\partial f(x_{i-1}, y_{i-1})}{\partial y} s_i \equiv -\alpha_i \pmod{p}. \end{aligned}$$

Do the same for g and get:

$$g(x_i, y_i) \equiv \frac{\partial g(x_{i-1}, y_{i-1})}{\partial x} t_i + \frac{\partial g(x_{i-1}, y_{i-1})}{\partial y} s_i \equiv -\beta_i \pmod{p}.$$

Then like before we can use Cramer's rule to uniquely solve for t_i and s_i. Since t_i and s_i are unique it implies that x_i and y_i are also unique. These x_i, y_i satisfy (1), so this proves this step of induction and therefore the induction. So the two sequences $\{x_i\}$ and $\{y_i\}$ exist for all i and are unique, so x and y exist and are unique. □

We can expand this version of Hensel's lemma to apply to n equations with n variables, instead of just two equations with two variables. The theorem and proof are the same as above but with more equations, variables, and notation.

Theorem 2.2.2 Let $f_1(x_1, \ldots, x_n), \ldots, f_n(x_1, \ldots, x_n)$ be multivariable polynomials with integer coefficients and a Jacobian matrix of:

$$J(x_1, \ldots, x_n) = \begin{pmatrix} \frac{\partial f_1}{\partial x_1} & \frac{\partial f_1}{\partial x_2} & \cdots & \frac{\partial f_1}{\partial x_n} \\ \frac{\partial f_2}{\partial x_1} & \frac{\partial f_2}{\partial x_2} & \cdots & \frac{\partial f_2}{\partial x_n} \\ \vdots & \vdots & \ddots & \vdots \\ \frac{\partial f_n}{\partial x_1} & \frac{\partial f_n}{\partial x_2} & \cdots & \frac{\partial f_n}{\partial x_n} \end{pmatrix}$$

Let $x_{1_0}, \ldots, x_{n_0} \in \{0, 1, \ldots, p-1\}$ such that:

$$f_1(x_{1_0}, \ldots, x_{n_0}) \equiv \ldots \equiv f_n(x_{1_0}, \ldots, x_{n_0}) \equiv 0 \pmod{p}$$

and $\det(J(x_{1_0}, \ldots, x_{n_0})) \not\equiv 0 \pmod{p}$. Then there exists a unique $x_1, \ldots, x_n$ belonging to the p-adic integers such that $f_1(x_1, \ldots, x_n) = \ldots = f_n(x_1, \ldots, x_n) = 0$ and $x_1 \equiv x_{1_0} \pmod{p}$ $, \ldots, x_n \equiv x_{n_0} \pmod{p}$.

The proof the this is similar to the proof for Theorem 2.2.1.

Now lets apply the multivariable Hensel's lemma.

Example 2.2.3 Let look for 11-adic solutions to:

$$\begin{cases} f(x, y, z) = x^3 + y^3 - z^3 \\ g(x, y, z) = y + z \\ h(x, y, z) = z^2 + 2 \end{cases}$$

You will notice that $x_0 = 1$, $y_0 = 3$, $z_0 = 8$ are solutions to $f(x_0, y_0, z_0) \equiv g(x_0, y_0, z_0) \equiv h(x_0, y_0, z_0) \equiv 0 \pmod{11}$. Also:

$$J(x_0, y_0, z_0) = \begin{pmatrix} \frac{\partial f(x_0,y_0,z_0)}{\partial x} & \frac{\partial f(x_0,y_0,z_0)}{\partial y} & \frac{\partial f(x_0,y_0,z_0)}{\partial z} \\ \frac{\partial g(x_0,y_0,z_0)}{\partial x} & \frac{\partial g(x_0,y_0,z_0)}{\partial y} & \frac{\partial g(x_0,y_0,z_0)}{\partial z} \\ \frac{\partial h(x_0,y_0,z_0)}{\partial x} & \frac{\partial h(x_0,y_0,z_0)}{\partial y} & \frac{\partial h(x_0,y_0,z_0)}{\partial z} \end{pmatrix} = \begin{pmatrix} 3x_0^2 & 3y_0^2 & 3z_0^2 \\ 0 & 1 & 1 \\ 0 & 0 & 2z_0 \end{pmatrix}$$

If you expand along the first column you get:

$$\det(J(x_0, y_0, z_0)) = 3x_0^2 \begin{vmatrix} 1 & 1 \\ 0 & 2z \end{vmatrix} = 3x_0^2[2z_0 - 0] = 6x_0^2 z_0 = 6(1)^2(8) = 48 \not\equiv 0 \pmod{11}.$$

Which implies that there exists unique 11-adic numbers, x, y, z, that solve $f(x, y, z) = g(x, y, z) = h(x, y, z) = 0$.

In the example above you will notice that $f(x, y, z) = 0$ is a form of Fermat's last theorem when $n = 3$. This implies that Fermat's last theorem has 11-adic solutions.

2.3 Hensel's Lifting

We can also use Hensel's lemma to actually find solutions, not just show that they exist. To do this we find solutions modulo p and then "lift" them to solutions modulo p^2 and further "lift" those solutions to solutions modulo p^3. Lifting all the way modulo p^i, for any i belonging to the positive integers, if need be.

Example 2.3.1 Lets try to solve $x^2+y^2 = 3$ and $xy = 4$. This has no solutions in $\mathbb{R}$, but what about in $\mathbb{Q}_p$? Let us try to find solutions in $\mathbb{Q}_7$. First we need our equations to be homogeneous, so set $f(x, y) = x^2 + y^2 - 3 = 0$ and $g(x, y) = xy - 4 = 0$. You will notice that $x = 1, y = 4$ are solutions to these two equations modulo 7, because $(1)^2 + (4)^2 - 3 = 14 \equiv 0$ and $(1)(4) - 4 = 0$, so set $x_0 = 1$ and $y_0 = 4$. Now we can "lift" it to solutions modulo 7^2 and then solutions modulo 7^3 and so on. To do this we need:

$$\begin{aligned}
f(x_1, y_1) &\equiv 0 && \pmod{7^2} \\
f(x_0 + 7t_1, y_0 + 7t_2) &\equiv 0 && \pmod{7^2} \\
f(x_0, y_0) + 7t_1\frac{\partial f(x_0, y_0)}{\partial x} + 7t_2\frac{\partial f(x_0, y_0)}{\partial y} &\equiv 0 && \pmod{7^2} \\
14 + 7t_1(2x_0) + 7t_2(2y_0) &\equiv 0 && \pmod{7^2} \\
2 + t_1(2x_0) + t_2(2y_0) &\equiv 0 && \pmod{7} \\
t_1(2) + t_2(8) &\equiv -2 && \pmod{7} \\
2t_1 + 1t_2 &\equiv 5 && \pmod{7}.
\end{aligned}$$

Now we need to do the same to g:

$$\begin{aligned}
g(x_1, y_1) &\equiv 0 && \pmod{7^2} \\
g(x_0 + 7t_1, y_0 + 7t_2) &\equiv 0 && \pmod{7^2} \\
g(x_0, y_0) + 7t_1 \frac{\partial g(x_0, y_0)}{\partial x} + 7t_2 \frac{\partial g(x_0, y_0)}{\partial y} &\equiv 0 && \pmod{7^2} \\
0 + 7t_1(y_0) + 7t_2(x_0) &\equiv 0 && \pmod{7^2} \\
0 + t_1(x_0) + t_2(y_0) &\equiv 0 && \pmod{7} \\
t_1(4) + t_2(1) &\equiv 0 && \pmod{7} \\
4t_1 + t_2 &\equiv 0 && \pmod{7}.
\end{aligned}$$

We now have two equations and two variables: $\begin{cases} 2t_1 + 1t_2 \equiv 5 \\ 4t_1 + t_2 \equiv 0 \end{cases}$

We can now solve for t_1 and t_2 using matrices and Cramer's rule:

$$\begin{pmatrix} 2 & 1 \\ 4 & 1 \end{pmatrix} \begin{pmatrix} t_1 \\ t_2 \end{pmatrix} \equiv \begin{pmatrix} 5 \\ 0 \end{pmatrix}$$

We label these matrices $J \cdot t \equiv d$ respectively.

$$\text{Now } J_{t_1} \equiv \begin{pmatrix} 5 & 1 \\ 0 & 1 \end{pmatrix} \text{ and } J_{t_1} \equiv \begin{pmatrix} 2 & 5 \\ 4 & 0 \end{pmatrix} \text{ and}$$

$$\det(J) = (2)(1) - (1)(4) = 2 - 4 = -2$$

$$\det(J_{t_1}) = (5)(1) - (1)(0) = 5 - 0 = 5$$

$$\det(J_{t_2}) = (2)(0) - (5)(4) = 0 - 20 = -20.$$

By Cramer's rule:

$$t_1 = \frac{\det(J_{t_1})}{\det(J)} = \frac{5}{-2} \equiv \frac{5}{5} \equiv 1 \quad \text{and}$$

$$t_2 = \frac{\det(J_{t_2})}{\det(J)} = \frac{-20}{-2} \equiv \frac{1}{5} \equiv \frac{15}{5} \equiv 3.$$

Now that we have t_1 and t_2 we can solve for x_1 and y_1.

$$x_1 = x_0 + 7t_1 = 1 + 7(1) = 8, \qquad y_1 = y_0 + 7t_2 = 4 + 7(3) = 25.$$

Let us now check if $x_1 = 8$ and $y_1 = 25$ do indeed give solutions to $f(x, y)$ and $g(x, y)$ modulo 7^2.

$$f(x_1, y_1) = f(8, 25) = (8)^2 + (25)^2 - 3 = 64 + 625 - 3 = 686 \equiv 0 \pmod{7^2}$$

$$g(x_1, y_1) = g(8, 25) = (8)(25) - 4 = 200 - 4 = 196 \equiv 0 \pmod{7^2}.$$

So $x_1 = 8$ and $y_1 = 25$ do give solutions modulo 7^2. Now we can "lift" again to solutions modulo 7^3. To do this wee need:

$$\begin{aligned}
f(x_2, y_2) &\equiv 0 && \pmod{7^3} \\
f(x_1 + 7^2 t_3, y_1 + 7^2 t_4) &\equiv 0 && \pmod{7^3} \\
f(x_1, y_1) + 7^2 t_3 \frac{\partial f}{\partial x_1} + 7^2 t_4 \frac{\partial f}{\partial y_1} &\equiv 0 && \pmod{7^3} \\
686 + 7^2 t_3 (2x_1) + 7^2 t_4 (2y_1) &\equiv 0 && \pmod{7^3} \\
686 + 7^2 t_3 (16) + 7^2 t_4 (50) &\equiv 0 && \pmod{7^3} \\
14 + 16t_3 + 50t_4 &\equiv 0 && \pmod{7} \\
2t_3 + 1t_4 &\equiv 0 && \pmod{7}.
\end{aligned}$$

and

$$\begin{aligned}
g(x_2, y_2) &\equiv 0 && \pmod{7^3} \\
g(x_1 + 7^2 t_3, y_1 + 7^2 t_4) &\equiv 0 && \pmod{7^3} \\
g(x_1, y_1) + 7^2 t_3 \frac{\partial g}{\partial x_1} + 7^2 t_4 \frac{\partial g}{\partial y_1} &\equiv 0 && \pmod{7^3} \\
196 + 7^2 t_3(y_1) + 7^2 t_4(x_1) &\equiv 0 && \pmod{7^3} \\
196 + 7^2 t_3(25) + 7^2 t_4(8) &\equiv 0 && \pmod{7^3} \\
4 + 25t_3 + 8t_4 &\equiv 0 && \pmod{7} \\
4t_3 + 8t_4 &\equiv -4 && \pmod{7} \\
4t_3 + 1t_4 &\equiv 3 && \pmod{7}.
\end{aligned}$$

Once again we have two equations and two variables so we can solve using matrices:

$$\begin{pmatrix} 2 & 1 \\ 4 & 1 \end{pmatrix} \begin{pmatrix} t_3 \\ t_4 \end{pmatrix} \equiv \begin{pmatrix} 0 \\ 3 \end{pmatrix}$$

We lable these matrices $J \cdot t' \equiv d'$ respectively.

$$\text{Now } J_{t_3} \equiv \begin{pmatrix} 0 & 1 \\ 3 & 1 \end{pmatrix} \text{ and } J_{t_4} \equiv \begin{pmatrix} 2 & 0 \\ 4 & 3 \end{pmatrix} \text{ and}$$

$$\det(J) = (2)(1) - (1)(4) = 2 - 4 = -2$$

$$\det(J_{t_3}) = (0)(1) - (1)(3) = 0 - 3 = -3$$

$$\det(J_{t_4}) = (2)(3) - (0)(4) = 6 - 0 = 6.$$

By Cramer's rule:

$$t_3 = \frac{\det(J_{t_3})}{\det(J)} = \frac{-3}{-2} \equiv \frac{4}{5} \equiv \frac{25}{5} \equiv 5$$

$$t_4 = \frac{\det(J_{t_4})}{\det(J)} = \frac{6}{-2} \equiv \frac{6}{5} \equiv \frac{20}{5} \equiv 4.$$

Now that we have t_3 and t_4 we can solve for x_2 and y_2.

$$x_2 = x_1+7^2t_3 = 8+7^2(5) = 8+245 = 253, \quad y_2 = y_1+7^2t_4 = 25+7^2(4) = 25+196 = 221$$

Let us now check if $x_2 = 253$ and $y_2 = 221$ do indeed give solutions to $f(x_2, y_2)$ and $g(x_2, y_2)$ modulo 7^3.

$$f(x_2, y_2) = f(253, 221) = (253)^2+(221)^2-3 = 64009+48841-3 = 112847 \equiv 0 \pmod{7^3}$$

$$g(x_2, y_2) = g(253, 221) = (253)(221) - 4 = 55913 - 4 = 55909 \equiv 0 \pmod{7^3}$$

So $x_2 = 253$ and $y_2 = 221$ do give solutions to f and g modulo 7^3. We can also "lift" this to get solutions modulo higher powers of 7 by doing exactly what we did above, but this quickly becomes time consuming.

The t_i and s_i are the coefficients to the p-adic expansions of x and y.

Chapter 3
Field extensions of $\mathbb{Q}_p$

3.1 Field extensions of $\mathbb{Q}_p$

For this section we let F be a locally compact field with a non-Archimedean norm $\| \|$.

Definition 3.1.1 Let V be a finite dimensional vector space over F. Then a norm on V, called a *field norm*, is a map $\| \|_V$, from V to the non-negative real numbers, satisfying:

(1) $\|x\|_V = 0$ *iff* $x = 0$

(2) $\|ax\|_V = \|a\|\|x\|_V$, for all $a \in F$ and $x \in V$

(3) $\|x + y\|_V \leq \|x\|_V + \|y\|_V$.

Theorem 3.1.2 If V is a finite dimensional vector space over a locally compact field F, then all norms on V are equivalent.

Corollary 3.1.3 Let $V = K$ be a field. Then there is at most one norm of K, denoted $\| \|_K$, as a field that extends $\| \|$ of F. i.e., such that $\|a\|_K = \|a\|$ for $a \in F$.

proof for this theorem and corollary is available in [1 pg 58-59].

Before we get into extensions of fields we must first define a different type of "norm" and then extend the p-adic norm to these fields.

Definition 3.1.4 Let $K = F(\alpha)$ be a finite extension of a field F generated by an element α which satisfies the monic irreducible polynomial $\text{irred}(\alpha) = x^n + a_1 x^{n-1} + \ldots + a_{n-1}x + a_n = 0$ for $a_i \in F$. Then the *norm of* α *from* K *to* F is:

$$\mathbb{N}_{K/F}(\alpha) = \det(A_\alpha)$$

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

Proposition 3.1.5 The norm of α form K to F, $\mathbb{N}_{K/F}(\alpha) = \det(A_\alpha)$ is equivalent the following:

(1) $\mathbb{N}_{K/F}(\alpha) = (-1)^n a_n$, where a_n is the constant term of $\text{irred}(\alpha)$ and n is its degree.

(2) $\mathbb{N}_{K/F}(\alpha) = \prod_{i=1}^{n} \alpha_i$, where α_i are the conjugates of $\alpha = \alpha_1$ over F.

Proof: Let us choose $\{1, \alpha, \ldots, \alpha^{n-1}\}$ as the basis for K over F. With this basis then:

$$A_\alpha = \begin{pmatrix} 0 & 0 & 0 & \cdots & 0 & -a_n \\ 1 & 0 & 0 & \cdots & 0 & -a_{n-1} \\ 0 & 1 & 0 & \cdots & 0 & -a_{n-2} \\ 0 & 0 & 1 & \cdots & 0 & -a_{n-3} \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & -a_1 \end{pmatrix}$$

which, if you expand along the first row it is easy to see that:

$$\det(A_\alpha) = (-1)^{n+1}(-a_n) = (-1)^{n+2}a_n = (-1)^n a_n.$$

This proves (1).

Factoring the monic irreducible polynomial gets:

$$\text{irred}(\alpha) = x^n + a_1 x^{n-1} + \ldots + a_{n-1}x + a_n = \prod_{i=1}^{n}(x - \alpha_i)$$

and it is easy to see that:

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

this proves (2). □

Notice that proposition 3.1.5 above implies that $\mathbb{N}_{K/F}(\alpha)$ belongs to the p-adic numbers, $\mathbb{Q}_p$. Also for any $\alpha \in K$, $\mathbb{N}_{K/F}(\alpha)$ is defined as the determinant of the matrix of multiplication by α in K, it follows that:

$$\mathbb{N}_{K/F}(\alpha\beta) = \mathbb{N}_{K/F}(\alpha)\mathbb{N}_{K/F}(\beta).$$

Now suppose α has degree n, i.e., $\text{irred}(\alpha) = x^n + a_1 x^{n-1} + \ldots + a_{n-1}x + a_n$ Let K be the field obtained by adjoining α and its conjugates to $\mathbb{Q}_p$, this is a finite Galois extension of $\mathbb{Q}_p$. Suppose we have an extension $\| \ \|$ of $| \ |_p$ to K. Then by corollary 3.1.3, such a field norm $\| \ \|$ is unique. Let σ be an automorphism that takes α to a conjugate α'. The map $\| \ \|' : F \to \mathbb{R}$ given by $\|x\|' = \|\sigma(x)\|$ is clearly a field norm which extends $| \ |_p$ on K. This means $\| \ \|' = \| \ \|$, so $\|\alpha\| = \|\alpha\|' = \|\sigma(\alpha)\| = \|\alpha'\|$. This implies that all conjugates have the same norm. Then the norm of $|\mathbb{N}_{\mathbb{Q}_p(\alpha)/\mathbb{Q}_p}(\alpha)|_p$, which is in $\mathbb{Q}_p$ is:

$$\begin{aligned}
|\mathbb{N}_{\mathbb{Q}_p(\alpha)/\mathbb{Q}_p}(\alpha)|_p &= \|\mathbb{N}_{\mathbb{Q}_p(\alpha)/\mathbb{Q}_p}(\alpha)\| \\
&= \Big\|\prod_{i=1}^{n} \alpha_i\Big\| \\
&= \prod_{i=1}^{n} \|\alpha_i\| \\
&= \|\alpha\|^n.
\end{aligned}$$

Which implies that $\|\alpha\| = |\mathbb{N}_{\mathbb{Q}_p(\alpha)/\mathbb{Q}_p}(\alpha)|_p^{1/n}$.

If K is any field containing α, then:

$$\mathbb{N}_{K/\mathbb{Q}_p}(\alpha) = (\mathbb{N}_{\mathbb{Q}_p(\alpha)/\mathbb{Q}_p}(\alpha))^{[K:\mathbb{Q}_p(\alpha)]},$$

and

$$n = [\mathbb{Q}_p(\alpha) : \mathbb{Q}_p] = \frac{[K : \mathbb{Q}_p]}{[K : \mathbb{Q}_p(\alpha)]},$$

so we can also define $\|\alpha\|$ to be

$$|\mathbb{N}_{K/\mathbb{Q}_p}(\alpha)|_p^{1/[K:\mathbb{Q}_p(\alpha)]}.$$

From now on we use $|\ |_p$ to denote the extension of the p-adic norm, instead of $\|\ \|$.

Theorem 3.1.6 Let K be a finite extension of $\mathbb{Q}_p$. Then there exists a field norm on K which extends the norm $|\ |_p$ on $\mathbb{Q}_p$.

Proof for this theorem is available in [1 pg 61].

Both theorem 3.1.6 and corollary 3.1.3 imply that there can be only one finite field extension of the p-adic norm to any finite extension field K on $\mathbb{Q}_p$.

Definition 3.1.7 Let K be a finite extension field of $\mathbb{Q}_p$, and let A be the set of all $x \in K$ such that x is a solution to polynomials of the form:

$$x^n + a_1 x^{n-1} + \ldots + a_{n-1}x + a_n = 0$$

with $a_i \in \mathbb{Z}_p$. Then we call A the *integral closure of* $\mathbb{Z}_p$ *in* K.

Proposition 3.1.8 Let k be a finite extension of $\mathbb{Q}_p$ of degree n, and let:

$$A = \{x \in K \big| |x|_p \leq 1\}$$

$$M = \{x \in K \big| |x|_p < 1\}.$$

Then A is a ring, which is the integral closure of $\mathbb{Z}_p$ in K. M it its unique maximal ideal, and A/M is a finite extension of $\mathbb{F}_p$ of at most degree n.

Proof: First we need to show that A is a ring. A has the structure of K, so we just need to check if it is closed under addition and multiplication. If $x, y \in A$, then $|xy|_p \leq 1$, so $xy \in A$. We also have $|x+y|_p \leq \max(|x|_p, |y|_p) \leq 1$, so $x+y \in A$. And A is closed under addition and multiplication so A is a ring. For $a \in A$ and $m \in M$ we have $|am|_p = |a|_p|m|_p < 1$ which implies $am \in M$. M is an ideal because it is an additive subgroup of A.

Now to show that A is the integral closure os $\mathbb{Z}_p$ in K. Suppose $\alpha \in A$, then $|\alpha|_p \leq 1$. Since $\alpha \in K$, then α is algebraic over $\mathbb{Q}_p$ with:

$$\text{irred}(\alpha) = x^m + a_{m-1}x^{m-1} + \ldots + a_0 = \prod_{i=1}^{m}(x - \alpha_i)$$

where α_i are conjugates of α. All the conjugates of α have the same norm so $|\alpha_i|_p \leq 1$ and $\alpha_i \in A$. Also the coefficients of irred(α) are products and sums of the α_i, which implies $|a_i|_p \leq 1$. Which implies $a_i \in \mathbb{Z}_p$, and irred$(\alpha) \in \mathbb{Z}_p[x]$.

Also if $\alpha \in K$ is the root of a polynomial in $\mathbb{Z}_p[x]$, it also clear that irred$(\alpha) \in \mathbb{Z}_p[x]$. Now we let the degree of irred(α) be m so that $\alpha^m + a_{m-1}\alpha^{m-1} + \ldots + a_0 = 0$. Suppose $|\alpha|_p > 1$, then:

$$\begin{aligned}
|\alpha|_p^m = |\alpha^m|_p &= |-a_{m-1}\alpha^{m-1} - \ldots - a_0|_p \\
&\leq \max(|a_{m-1}\alpha^{m-1}|_p, \ldots, |a_{0|_p}|_p) \\
&\leq \max(|\alpha^{m-1}|_p, \ldots, 1), \text{ since } |a_i|_p \leq 1 \\
&= |\alpha^{m-1}|_p
\end{aligned}$$

but since $|\alpha|_p > 1$ this is a contradiction. So then $|\alpha|_p \leq 1$ and $\alpha \in A$. Then A is then integral closure of $\mathbb{Z}_p$ in K.

Now we try to see if M is a maximal ideal. Suppose N is an ideal such that $M \subset N \subset A$. Then there exists an $\alpha \in N$ but $\alpha \notin M$. Which implies $|\alpha|_p = 1$ so $|1/\alpha|_p = 1$ and $1/\alpha \in A$. But then $\alpha\frac{1}{\alpha} = 1 \in N$, but this is a contradiction since $N \neq A$. So M is a maximal ideal in A.

A is a ring and M is maximal, so A/M is a field. From the definition of M we have $M \cap \mathbb{Z}_p = p\mathbb{Z}_p$. If $a \in \mathbb{Z}_p$, then $|a|_p \leq 1$ so $a \in A$. If $a, b \in \mathbb{Z}_p$, then $a - b \in M \cap \mathbb{Z}_p = p\mathbb{Z}_p$ *iff* $a + M$ and $b + M$ represent the same coset. But this means that for $a + p\mathbb{Z}_p \in \mathbb{Z}_p/p\mathbb{Z}_p = \mathbb{F}_p$, there exists a corresponding $a + M \in A/M$, i.e., $\mathbb{F}_p$ lies in A/M. This means that A/M is an extension field of $\mathbb{F}_p$.

Now we need to show that $[A/M : \mathbb{F}_p] \leq n$, to do this we need to show that any linear combination of $n + 1$ elements over $\mathbb{F}_p$ is linearly dependent. So take:

$$a_1 + M, a_1 + M, \ldots, a_{n+1} + M \in A/M, \text{ for } a_i \in A.$$

Since each $a_i \in K$ then the a_i are linearly dependent over $\mathbb{Q}_p$. So:

$$b_1 a_1 + \ldots + b_{n+1} a_{n+1} = 0, \text{ for } b_i \in \mathbb{Q}_p.$$

If we let $m = \min(\operatorname{ord}_p b_1, \ldots, \operatorname{ord}_p b_{n+1})$, the we can multiply the above equation by p^{-m} and obtain a similar equation where all coefficients are in $\mathbb{Z}_p$ and at least one is not in $p\mathbb{Z}_p$ (if $m < 0$ then we multiply by $p^{|m|}$). Thus if be map the equation above onto A/M, then we get an equation of the form:

$$b_1 a_1 + \ldots + b_{n+1} a_{n+1} + M = 0, \text{ for } b_i \in \mathbb{F}_p.$$

Any $b_i \in p\mathbb{Z}_p$ is mapped to $0 + M$ in A/M, but this is not the case for all the b_i. Thus, the $\{a_i\}$ are linearly dependent. This proves the claim. □

Definition 3.1.9 The field A/M as described in theorem 3.1.8 is called the *residue field* of K.

Putting theorem 3.1.2 and 3.1.6 together, we can conclude that $|\ |_p$ has a unique extension to any finite field extension of $\mathbb{Q}_p$, that we also denoted $|\ |_p$. Since the algebraic closure of $\mathbb{Q}_p$, denoted $\overline{\mathbb{Q}}_p$, is the union of such extensions, then $|\ |_p$ extends uniquely to $\overline{\mathbb{Q}}_p$. This means that if $\alpha \in \overline{\mathbb{Q}}_p$ has $\text{irred}(\alpha) = x^n + a_1 x^{n-1} + \ldots + a_n$, then $|\alpha|_p = |a_n|_p^{1/n}$.

Let K be an extension of $\mathbb{Q}_p$ of degree n. For $\alpha \in K$ we define:

$$\text{ord}_p\, \alpha = -\log_p |\alpha|_p = -\log_p |\mathbb{N}_{K/\mathbb{Q}_p}(\alpha)|_p^{1/n} = -\frac{1}{n} \log_p |\mathbb{N}_{K/\mathbb{Q}_p}(\alpha)|_p.$$

For any $\alpha \in \mathbb{Q}_p$, this agrees with our earlier definition of ord_p, and clearly it still has the same multiplicative property.

The image of K under the ord_p map is contained in:

$$(1/n)\mathbb{Z} = \{x \in \mathbb{Q} \mid nx \in \mathbb{Z}\}$$

and the image is an additive subgroup of $(1/n)\mathbb{Z}$, so for some positive integer e dividing n, it is of the form $(1/e)\mathbb{Z}$.

Definition 3.1.10 The integer e mentioned above is called the **index of ramification** of K over $\mathbb{Q}_p$. If $e = 1$, then K is called an **unramified extension** of $\mathbb{Q}_p$. If $e = n$, then K is called **totally ramified**.

Our upcoming theorem will involve an "Eisenstein equation". It is well known that such equations are irreducible over $\mathbb{Q}$, but the same happens to be true over $\mathbb{Q}_p$. We will not prove it, but it is a useful fact for the proof of the upcoming theorem.

Theorem 3.1.11 If K is totally ramified and $\alpha \in K$ has the property $\operatorname{ord}_p \alpha = (1/e)$, then α satisfies an "Eisenstein equation":

$$x^e + a_{e-1}x^{e-1} + \ldots + a_0 = 0, \quad a_i \in \mathbb{Z}_p$$

where $a_i \equiv 0 \pmod{p}$ for all i, and $a_0 \not\equiv 0 \pmod{p^2}$. Conversely, if β is a root of such an Eisenstein equation over $\mathbb{Q}_p$, then $\mathbb{Q}_p(\beta)$ is totally ramified over $\mathbb{Q}_p$ of degree e.

Proof: The a_i are symmetric polynomials in the conjugates of α, and since $\operatorname{ord}_p \alpha = (1/e)$, all of the conjugates have $|\ |_p = 1/p^{1/e}$, which implies that $|a_i|_p \leq 1$. But for a_0 we have $|a_0|_p = |\alpha|_p^e = 1/p$ so $a_0 \not\equiv 0 \pmod{p^2}$.

Conversely, since an Eisenstein equation is irreducible over $\mathbb{Q}_p$, adjoining a root β gives us an extension of degree e. Since we have $a_0 = 1$, it implies:

$$\operatorname{ord}_p \beta = -\log_p |\beta|_p = -\frac{1}{e} \log_p |a_0|_p = (1/e) \operatorname{ord}_p a_0 = (1/e),$$

so $\mathbb{Q}_p(\beta)$ is totally ramified over $\mathbb{Q}_p$. $\square$

Bibliography

[1] Neal Koblitz *p-adic Numbers, p-adic Analysis, and Zeta-Functions, Second Edition* Springer-Verlag 1984.

[2] Evan Turner *The p-adic Numbers and Finite Field Extensions of* $\mathbb{Q}_p$ March 2014, url: http://www.math.uchicago.edu/ may/VIGRE/VIGRE2011/REUPapers/Turner.pdf

[3] Theodor Christian Herwig *The p-adic Completion of* $\mathbb{Q}$ *and Hensel's Lemma* April 2014, url: http://www.math.uchicago.edu/ may/VIGRE/VIGRE2011/REUPapers/Herwig.pdf