A BRIEF OVERVIEW OF P-ADIC NUMBERS

Megan Kress

Mathematics Major Capstone Project

Advisor: Kevin McLeod

December 2014

1. Introduction

For my Capstone project I covered the first three chapters of Fernando Q. Gouvêa's *p-adic Numbers: An Introduction.* The first chapter served as an introduction, giving a definition of p-adic numbers and providing practice problems to understand p-adic expansions In the second chapter, Gouvêa introduced properties of the field of p-adic numbers including its absolute value (based on p-adic valuations) and topology. The third chapter utilized the foundations of Chapter 2 to prove that assumptions made in Chapter 1 were well-founded. In this Capstone paper, I will give an overview of the field of p-adic numbers in a similar fashion to Gouvêa's approach and summarize important points that lead to the definition of p-adic numbers.

1.1 Hensel's Analogy

In an 1897 paper on power series of algebraic numbers, German mathematician K. Hensel first introduced the idea of p-adic numbers. Hensel's motivation was his analogy between the primes (p) and the linear polynomials $(X - \alpha)$. Hensel noted that the two were analogous in that they had converging expansions if we pick a "prime":

$$P(X) = \sum_{i=0}^{n} a_i(X - \alpha)^i$$

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

Likewise, the "rational" polynomials and the rational numbers have finite-tailed Laurent series expansions so that for a, b $\in \mathbf{Z}$: $\quad x = \frac{a}{b} = \sum_{n \geq n_0} a_n p^n$

Hensel's analogy, along with a geometric analogy is summarized below:

A "Rosetta Stone"

Geometry	Function Fields	Number Theory
"Riemann sphere"	$\mathbb{C}(X)$	$\mathbb{Q}$
complex plane	$\mathbb{C}[X]$	$\mathbb{Z}$
point $\alpha \in \mathbb{C}$	irreducible $X - \alpha$	prime p
Riemann surface	finite extension $K/\mathbb{C}(X)$	finite extension $K/\mathbb{Q}$
"local" behavior	Laurent series around α	!??

From a presentation on p-adic number history by Gouvêa [2]

The set of all these p-adic expansions forms the field of p-adic numbers, $\mathbf{Q}_p$. $\mathbf{Q}_p$ is the completion of $\mathbf{Q}$ when $\mathbf{Q}$ has the metric of $|\cdot|_p$, the p-adic absolute value or norm.

Thus, we have a definition of a p-adic number, which will be formally proved later in this paper. We do know, however that our series must converge, so somehow as n grows, p^n must get smaller. We will formally see why this is true when we see the definition of a p-adic absolute value.

1.2 Periodic Expansions of Rational Numbers

It may seem that p-adic numbers are very different than real numbers, but one way in which they are similar is that every rational number has an eventually periodic p-adic expansion. The proof of this fact is Problem 6 in Section 1.1:

Proof:

x is rational $\Leftarrow$ x has eventually periodic p-adic expansion

Proving that an eventually periodic p-adic expansion represents a rational number is relatively straight-forward.

$$x = a_0 + a_1p^1 + \cdot\cdot\cdot + ap^n + bp^{n+1} + ap^{n+2} + \cdot\cdot\cdot$$

$$x \cdot p^n = a_0p^n + a_1p^{n+1} + \cdot\cdot\cdot + ap^{2n} + bp^{2n+1} + ap^{2n+2} + \cdot\cdot\cdot$$

$$x - x \cdot p^n = x(1 - p^n) = a_0 + a_1p^1 + \cdot\cdot\cdot + ap^n + bp^{n+1} + ap^{n+2} + \cdot\cdot\cdot + bp^{2n-1}$$

$$x = \frac{a_0 + a_1p^1 + \cdot\cdot\cdot + ap^n + bp^{n+1} + ap^{n+2} + \cdot\cdot\cdot + bp^{2n-1}}{1 - p^n} \in \mathbf{Q}$$

We know x is a rational number because the numerator and denominator are integers. The numerator is an integer because it is a finite p-adic expansion and the denominator is obviously an integer (1 minus an integer squared is an integer).

x is rational $\Rightarrow$ *x has eventually periodic p − adic expansion*

Since x is rational, x has a p-adic expansion in the following form:

$$x = \frac{r}{s} = a_0 + a_1p^1 + a_2p^2 + a_3p^3 + \cdot\cdot\cdot$$

We know

$$a_0 = \tfrac{r}{s}\ (mod\ p)$$

$$sa_0 = r\ (mod\ p)$$

$$sa_0 \ = \ b_0\ (mod\ p)$$

By the expansion,

$$a_1 p = \tfrac{r}{s} - a_0$$

$$a_1 p \equiv \tfrac{r}{s} - b_0 \equiv \tfrac{r - b_0 s}{s} \ \ (mod\ p^2)$$

Because we know $r - b_0 s \equiv 0\ (mod\ p)$, we know $p|(r - b_0 s)$. Thus, we can divide the congruence by p

$$a_1 \equiv \tfrac{r - b_0 s}{sp}\ (mod\ p)$$

$$sa_1 \equiv \tfrac{r - b_0 s}{p}\ (mod\ p) \equiv b_1\ (mod\ p)$$

If we continue in this pattern, we find that any coefficient b_k is an integer between 0 and p - 1, so there are a finite number of values that any b value can take. Thus, a value of b must be repeated that for some $i, j, j > i,\ b_i = b_j$. This means that the expansion starting at step j will be a repeated expansion of the expansion beginning at step i. Thus, the expansion is eventually repeating.

2. Properties of the p-adic Fields

2.1 P-Adic Valuations

To define the p-adic absolute value, we must first explore p-adic valuations. The valuation, $v_p(x)$, for a rational number x, can be found through the equation:

$x = p^{v_p(x)} \cdot \frac{a}{b}$ where p does not divide a or b [1, Section 2.1]

Example:

$v_5(400)$

$400 = 5^2 \cdot \frac{16}{1}$

Thus, $v_5(400) = 2$

From the definition and this example, we can see that a number that is divisible by a higher power of p will have a larger valuation whereas a number that is not divisible by p will have a valuation of zero.

2.2 P-Adic Absolute Value

This leads to the definition of p-adic absolute value:

$|x|_p = p^{-v_p(x)}$ [1, Section 2.1]

Thus, a number's being more divisible by p leads to a higher valuation, which leads to a smaller absolute value. The properties of the p-adic absolute value make the function a non-archimedean absolute value on **Q**. This leads to many interesting qualities of the topology of fields of p-adic numbers including the fact that it is an ultrametric space, which implies that all "triangles" are isosceles.

The idea of distance or "closeness" on $\mathbf{Q}_p$ may seem strange or unintuitive as seen in this example.

Example:

(1) $|135 - 10|_5 = |125|_5$

$125 = 5^3$, so $v_5(125) = 3$

$|135 - 10|_5 = 5^{-3} = 1/125$

(2) $|135 - 35|_5 = |100|_5$

$100 = 4 \cdot 5^2$, so $v_5(100) = 2$

$|135 - 35|_5 = 5^{-2} = 1/25$

Using the definition of p-adic absolute value and valuation, we find that the distance between 135 and 10 (1) is actually five times less than the distance between 135 and 35 (2) for $p = 5$.

2.3 Ostrowski's Theorem

Ostrowski's Theorem tells us that once we have defined the p-adic absolute value, we have found every absolute value on **Q**:

(Theorem 3.1.3) Every non-trivial absolute value on **Q** is equivalent to one of the absolute values $| \ |_p$, where either p is a prime number or p = ∞. [1, Section 3.1]

Gouvêa provides a proof that shows that $| \ |_\infty$ is the "usual" absolute value.

2.4 Geometry on Q_p:

P-adic numbers have special topological properties in addition to every triangle being isosceles. One of the most important qualities involves the balls $B(a,r) = \{x \in Q_p : |x-a|_p \leq r\}$. Important facts are as follows:

- Every point contained in a ball is a center of that ball.
- Any two balls are disjoint or subsets of each other.
- Balls have empty boundaries.

[1, Section 2.3]

3. Rigorous Definition

3.0 Important Definitions

I. Cauchy Sequence
II. Complete
III. Dense

These three definitions lead to the discovery that our definition of p-adic numbers from Section 1 can be proved rigorously.

3.1 Cauchy Sequence

A sequence of rational numbers under a non-archimedean absolute value satisfies the Cauchy condition iff $\lim_{n\to\infty} |x_{n+1} - x_n| = 0$. This quality makes analysis on non-archimedean fields like $\mathbf{Q}_p$ much simpler. [1, Section 3.2]

3.2 Complete

A field is complete with respect to a certain absolute value if every Cauchy sequence of the field has a limit. Gouvêa proves Lemma 3.2.3 which states that **Q** is not complete with respect any of its non-trivial absolute values. Thus, he spends a good amount of time proving a completion of **Q** in Section 3.2.

3.3 Dense

$S \subset k$ is dense in k if $\forall x \in k$ and $\forall \varepsilon > 0$, $B(x, \varepsilon) \cap S \neq \varnothing$.

This means that every ball around x in *k* will contain an element of the dense subset.

3.4 Construction of $\mathbf{Q}_p$

Gouvêa proves the completion of $\mathbf{Q}$ by showing that $\mathbf{Q}$ is dense in $\mathbf{Q}_p$ and that $\mathbf{Q}_p$ is complete, thus constructing $\mathbf{Q}_p$.

By proving the unique representation of the ring $\mathbf{Z}_p$ of p-adic integers, Gouvêa shows in Section 3.3 that elements of $\mathbf{Q}_p$ also have unique representations of the form

$$x = \sum_{n \geq n_0} b_n p^n$$

At this point, we are brought back to Section 1 where we assumed that we could represent p-adic numbers as unique p-adic expansions. Throughout Chapters 2 and 3, Gouvêa provided the basis for constructing $\mathbf{Q}_p$ and proved that the properties of $\mathbf{Q}_p$ that we assumed in the beginning are valid through rigorous proofs and definitions.

4. Conclusion

At the conclusion of my study of p-adic numbers, I find that there are many topics I would like to research in the future. A couple of the topics include:

- p-adic Analysis: Gouvêa covers this topic later in his book, and studying the basics would be a good way to test my understanding of the topic of p-adic numbers.
- Computer Science: 2's Complement numbers are precisely $\mathbf{Q}_2$. As someone interested in computer science, I would like to explore the consequences of this fact along with the many other applications of p-adic numbers in computer science.

I found the study of p-adic numbers to be a rewarding experience. Not only did it provide a good review of many Algebra and some Geometry concepts, but it also broadened my view of number systems in general. Thus, this Capstone Project was a good way to wrap up my Mathematics degree.

5. Sources

[1] Gouvêa, Fernando. *P-adic Numbers: An Introduction*. 2nd ed. Berlin: Springer-Verlag, 1993. Print.

[2] Gouvêa, Fernando. "Hensel's p-adic Numbers: early history." AMS regional meeting. AMS. Providence, RI. 2 Oct. 1999. Lecture.

[3] Rozikov, U A. "What Are P-Adic Numbers? What Are They Used For?" *Asia Pacific Mathematics Newsletter* 3.4 (2013). *Asia Pacific Mathematics Newsletter*. Asia Pacific Mathematics. Web. Dec. 2014. <http://www.asiapacific-mathnews.com/03/0304/0001_0006.pdf>.

[4] Bogomolny, Alexander. "P-adic Numbers." *Cut the Knot*. 1 Jan. 2014. Web. Dec. 2014.