ABSTRACT

NEWTON POLYGONS ON P-ADIC NUMBER FIELDS

by

Jacek Teller

April, 2012

Chair: Dr. Zachary Robinson

Major Department: Mathematics

This thesis offers a clear introduction to p-adic number fields, and the method of Newton polygons to approximate the size of roots of polynomials in the completion of the algebraic closure of p-adic number fields. Ostrowski's theorem is also proved herein. The thesis is intended to serve as an *aperitif* to further study in the area.

NEWTON POLYGONS ON P-ADIC NUMBER FIELDS

A Thesis

Presented to

The Faculty of the Department of Mathematics

East Carolina University

In Partial Fulfillment

of the Requirements for the Degree

Master of Arts in Mathematics

by

Jacek Teller

April, 2012

NEWTON POLYGONS ON P-ADIC NUMBER FIELDS

by

Jacek Teller

APPROVED BY:

DIRECTOR OF THESIS:

Dr. Zachary Robinson

COMMITTEE MEMBER:

Dr. Chris Jantzen

COMMITTEE MEMBER:

Dr. David Pravica

COMMITTEE MEMBER:

Dr. Heather Ries

CHAIR OF THE DEPARTMENT
OF MATHEMATICS:

Dr. Johannes H. Hattingh

DEAN OF THE
GRADUATE SCHOOL:

Dr. Paul Gemperline

ACKNOWLEDGEMENTS

I wish to express my deepest thanks to my thesis advisor, Dr. Zach Robinson. His guidance, friendship, and innumerable cups of coffee, made it possible for me to complete this thesis, and my degree, with my sanity intact. I wish, also, to thank Dr. Chris Jantzen, Dr. David Pravica, and Dr. Heather Ries for their their roles as my teachers and for agreeing to act as thesis committee members. They all gave warm words of encouragement to me at just the right times over the last years. There are a great many other faculty, staff, and graduate students, in the Mathematics Department who deserve special mention here–they are too many to list, but that is all right, they know who they are.

TABLE OF CONTENTS

CHAPTER 1: p is for Prime

In this chapter, the reader is offered an introduction to the basic elements of p-adic number theory. We begin by noting that the "p" in "p-adic" stands for a prime number. For example, taking p to be 3, we may talk about the 3-adic numbers. The particular choice of p is for the most part not going to matter in here, though it should be noted that it certainly has deep implications.

The theory of p-adic numbers may seem very strange when one first encounters it, so we begin where the theory appears most familiar. In the decimal notation system we express integers by a clever shorthand notation that, essentially, describes an integer as a sum of powers of 10.

Example 1.1. $1848 = 1(10^3) + 8(10^2) + 4(10^1) + 8(10^0)$.

Note that the number of terms in such sums is finite. Also note that an integer gets bigger as more (and higher) powers of 10 are added. A p-adic integer is simply one that has been expanded in terms of powers of a prime p. We call such a summation a p-adic expansion. The higher powers of p are added to the right, however, instead of the left as in the decimal notation.

Example 1.2. Set $p = 7$, then $5(7^1) + 2(7^2) + 5(7^3)$ is the 7-adic expansion of 1848.

This seems simple enough. However, as we elaborate, it will become clear that p-adic expansions of integers, or simply "p-adic integers," need not be sums with a finite number of terms–in fact we will think of them all as infinite sums. It will become clear that as more (and higher) powers of p are added, the number does not become any bigger. This assertion will seem sensible very shortly.

Example 1.3. Set $p = 7$, then 1848 can be expressed as the infinite sum $5(7^1) + 2(7^2) + 5(7^3) + \mathbf{0}(\mathbf{7^4}) + \mathbf{0}(\mathbf{7^5}) + \mathbf{0}(\mathbf{7^6}) + \mathbf{0}(\mathbf{7^7}) + \mathbf{0}(\mathbf{7^8}) + \mathbf{0}(\mathbf{7^9}) + \cdots$.

Example 1.4. Given any prime number p, we can write

$$-1 = (p-1) + (p-1)p + (p-1)p^2 + (p-1)p^3 + (p-1)p^4 + \cdots$$

because

$$\begin{aligned}
0 = 1 - 1 &= 1 + (p-1) + (p-1)p + (p-1)p^2 + (p-1)p^3 + (p-1)p^4 + \cdots \\
&= \Big[1 + (p-1)\Big] + (p-1)p + (p-1)p^2 + (p-1)p^3 + (p-1)p^4 + \cdots \\
&= \mathbf{p} + (p-1)p + (p-1)p^2 + (p-1)p^3 + (p-1)p^4 + \cdots \\
&= \Big[p + (p-1)p\Big] + (p-1)p^2 + (p-1)p^3 + (p-1)p^4 + \cdots \\
&= \mathbf{p^2} + (p-1)p^2 + (p-1)p^3 + (p-1)p^4 + \cdots \\
&= \Big[p^2 + (p-1)p^2\Big] + (p-1)p^3 + (p-1)p^4 + \cdots \\
&= \mathbf{p^3} + (p-1)p^3 + (p-1)p^4 + \cdots \\
&= ...
\end{aligned}$$

and so on, canceling all terms in the entire sum.

Our elaboration begins with a definition of the p-adic order function. The function may seem contrived and quite abstract, but it is worth taking time to understand the nature of this function well, as it will become central to our discussion of the size of p-adic numbers.

Definition 1.5. Fix p, prime. Define the p-adic order function $ord_p : \mathbb{Z} \to \mathbb{Z}$ by:

(i) $ord_p(n) = l$, where $p^l \mid n$, but $p^{l+1} \nmid n$, and $n \neq 0$.

(ii) $ord_p(0) = \infty$.

What we are really after from the p-adic order function is for it to give us the highest power of p that divides a given number n. A note on parlance: If $ord_p(n) = k$, then we say that k is the p-adic order of n.

Example 1.6. $ord_3(7) = 0$, $ord_3(-18) = 2$, $ord_5(100) = 2$.

The following two theorems expose some of the properties of the order function.

Theorem 1.7. $ord_p(nm) = ord_p(n) + ord_p(m)$.

Proof. If $n = 0$ or $m = 0$, then we have that $ord_p(nm) = ord_p(n) + ord_p(m) = \infty$. Otherwise, $ord_p(n)$ is the greatest power of p that divides n, and $ord_p(m)$ is the greatest power of p that divides m. Hence, we have that $n = p^{ord_p(n)} \cdot r$, for some $r \in \mathbb{Z}$, and $m = p^{ord_p(m)} \cdot s$, for some $s \in \mathbb{Z}$, with $p \nmid r$ and $p \nmid s$. Furthermore, because p is prime, and $p \nmid r$ and $p \nmid s$, we have that $p \nmid rs$.

Because, $mn = p^{ord_p(n)} \cdot p^{ord_p(m)} \cdot r \cdot s = p^{ord_p(n)+ord_p(m)} \cdot r \cdot s$ and $p \nmid rs$, we conclude that $ord_p(nm) = ord_p(n) + ord_p(m)$. □

Theorem 1.8. $ord_p(n + m) \geq \min\{ord_p(n), ord_p(m)\}$.

Proof. This is clear if either m or n is equal to 0. Otherwise, because $ord_p(n)$ is the greatest power of p that divides n, and $ord_p(m)$ is the greatest power of p that divides m, we have that $n = p^{ord_p(n)} \cdot r$, for some $r \in \mathbb{Z}$, and $m = p^{ord_p(m)} \cdot s$, for some $s \in \mathbb{Z}$, with $p \nmid r$ and $p \nmid s$.

Without loss of generality, we may assume that $ord_p(m) \geq ord_p(n)$. That is, assume that $ord_p(n) = \min\{ord_p(n), ord_p(m)\}$.

Now $m + n = p^{ord_p(n)} \cdot r + p^{ord_p(m)} \cdot s = p^{ord_p(n)}(s + p^{ord_p(m)-ord_p(n)} \cdot r)$, where $(s + p^{ord_p(m)-ord_p(n)} \cdot r)$ is an integer, hence $p^{ord_p(n)} \mid p^{ord_p(n)}(s + p^{ord_p(m)-ord_p(n)} \cdot r)$. Therefore, $ord_p(n + m) \geq \min\{ord_p(n), ord_p(m)\}$. □

Now that we have defined the order function, we are ready to define the p-adic absolute value. And it will become clear why the p-adic order function is so important.

Definition 1.9. Fix p, prime. Define the p-adic absolute value, $|\cdot|_p : \mathbb{Z} \to \mathbb{R}_+$ by:

(i) $|n|_p = 2^{-ord_p(n)}$, if $n \neq 0$.

(ii) $|0|_p = 0$.

We take $2^{-\infty}$ to be 0.

The absolute value of a number is understood to represent its size, or magnitude. The following example illustrates how the p-adic absolute value works in practice.

Example 1.10. We calculate:

$$|1848|_7 = 2^{-ord_7(1848)} = 2^{-1} = 1/2.$$

$$|2401|_7 = 2^{-ord_7(2401)} = 2^{-4} = 1/16.$$

Hence $|1848|_7 > |2401|_7$.

A rather peculiar result! Below, is another peculiar result.

Example 1.11. We calculate:

$$|1800|_7 = 2^{-ord_7(1800)} = 2^{-0} = 1.$$

$$|1900|_7 = 2^{-ord_7(1900)} = 2^{-0} = 1.$$

Hence $|1800|_7 = |1900|_7$.

We can get a better understanding of these results by looking at some theorems about the p-adic absolute value. We begin by demonstrating that the p-adic absolute value is indeed an absolute value.

Definition 1.12. A function $|\cdot| : S \to \mathbb{R}_+$ is an absolute value on a ring S if it satisfies:

(i) $|n| = 0$ iff $n = 0$.

(ii) $|n| \geq 0$.

(iii) $|n \cdot m| = |n| \cdot |m|$.

(iv) $|n| + |m| \geq |n + m|$.

where $n, m \in S$.

If, in addition to (i)-(iv), the condition $|n+m| \leq \max\{|n|, |m|\}$ holds, then we say the absolute value is non-Archimedean. (This condition is known as the ultrametric inequality.)

We wish to prove two theorems regarding the ultrametric inequality. These theorems will prove to be very useful in later chapters. For now, simply consider them as a means to better understand the ultrametric inequality.

Theorem 1.13. *Suppose S is a ring endowed with a non-Archimedean absolute value, $|\cdot|$. Then $|m| \neq |n|$ implies that $|m + n| = \max\{|m|, |n|\}$, where $m, n \in S$.*

Proof. Since $|\cdot|$ is non-Archimedean, the ultrametric inequality holds. That is, given $m, n \in S$

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

Without loss of generality, we may assume that $|m| > |n|$, hence

$$|n + m| \leq \max\{|n|, |m|\} = |m|.$$

Now, we write

$$|m| = |m + n - n| = |(m + n) - n| \leq \max\{|m + n|, |n|\}.$$

If $\max\{|m + n|, |n|\} = |n|$, then we conclude $|m| \leq| n|$, a contradiction. Therefore, $\max\{|m + n|, |n|\} = |m + n|$. Hence $|m| = |m + n|$. □

Theorem 1.14. *Suppose S is a ring endowed with a non-Archimedean absolute value, $|\cdot|$. If the sum*

$$\sum_{i=1}^{n} a_i = 0,$$

where $a_i \in S$ for all $1 \leq i \leq n$, and $n \geq 2$, then $|a_j| = |a_k|$ for some $k \neq j$, $1 \leq j, k \leq n$. Moreover,

$$\max_{1 \leq i \leq n} \{|a_i|\} = |a_j| = |a_k|.$$

Proof. Suppose, that $|a_j| \neq |a_k|$ for all $j \neq k$. Without loss of generality, we further assume that $j < k$ implies $|a_j| < |a_k|$. Then, by the previous theorem, we have

$$\sum_{i=1}^{n} |a_i| = |a_n| > 0,$$

a contradiction. □

Theorem 1.15. *We now resume our discussion of the p-adic absolute value. The p-adic absolute value function is an absolute value on $\mathbb{Z}$.*

Proof. Fix p, a prime number. We demonstrate that the four conditions of definition

1.12 are satisfied by the p-adic absolute value:

(i) If $n = 0$, then $|n|_p = 0$, by definition. If $|n|_p = 0$. Then $2^{-ord_p(n)} = 0$ implies that $ord_p(n) = \infty$. Since any integer not equal to 0 will have a finite order, we can conclude that $n = 0$.

(ii) The p-adic absolute value of a number n is defined by $|n|_p = 2^{-ord_p(n)}$, and since all powers of 2 are positive, and $|0|_p = 0$, we can conclude that $|n|_p \geq 0$.

(iii) We have already shown that $|mn|_p = 2^{-ord_p(mn)} = 2^{-(ord_p(m)+ord_p(n))} = 2^{-ord_p(m)}2^{-ord_p(n)} = |m|_p|n|_p$.

(iv) We know that $|n+m|_p = 2^{-ord_p(n+m)} \leq \max\{2^{-ord_p(n)}, 2^{-ord_p(m)}\} = \max\{|n|_p, |m|_p\}$. Without loss of generality, we assume that $|n|_p \leq |m|_p$, and hence $|n + m|_p \leq |m|_p$. And since $|n|_p \geq 0$ we have that $|n + m|_p \leq |m|_p + |n|_p$.

□

Part (iv) of the proof of Theorem 1.15, contains an important result. One that is worth identifying in a separate theorem.

Theorem 1.16. $|n + m|_p \leq \max\{|n|_p, |m|_p\}$

Proof. We simply write $|n+m|_p = 2^{-ord_p(n+m)} \leq \max\{2^{-ord_p(n)}, 2^{-ord_p(m)}\} = \max\{|n|_p, |m|_p\}$.

□

The fact that the ultrametric inequality holds for the p-adic absolute value will prove to have profound implications. We will see exactly what these implications are soon enough. Right now, however, we wish to extend the ideas developed on the integers to the field of rational numbers.

Definition 1.17. Fix p, a prime number. Let $n, m \in \mathbb{Z}$. Define $ord_p(n/m) = ord_p(n) - ord_p(m)$.

It is important to note that the p-adic order function is well defined on the equivalence class of fractions. Meaning that the order of a fraction is the same regardless of how the fraction is written. The following theorem states this more precisely.

Theorem 1.18. *Given $c \in \mathbb{Z}$, $ord_p(cn/cm) = ord_p(n/m)$.*

Proof. We simply note that

$$\begin{aligned} ord_p(cn/cm) &= ord_p(cn) - ord_p(cm) \\ &= ord_p(c) + ord_p(n) - ord_p(c) - ord_p(m) \\ &= ord_p(n) - ord_p(m). \end{aligned}$$

□

The following theorem illustrates that the order function, as extended to the rationals, behaves exactly as one would hope.

Theorem 1.19. *Given $m, n, r, s \in \mathbb{Z}$, $ord_p(m/n \cdot r/s) = ord_p(m/n) + ord_p(r/s)$.*

Proof. We simply note that

$$\begin{aligned} ord_p(m/n \cdot r/s) &= ord_p(mr/ns) \\ &= ord_p(mr) - ord_p(ns) \\ &= ord_p(m) + ord_p(r) - ord_p(n) - ord_p(s) \\ &= ord_p(m/n) + ord_p(r/s). \end{aligned}$$

□

Now that we have extended the order function to the rationals, we may extend the p-adic absolute value to the rationals, too.

Definition 1.20. Fix p, a prime number. Let $n, m \in \mathbb{Z}$. Define $|\frac{n}{m}|_p = \frac{|n|_p}{|m|_p} = 2^{-ord_p(n/m)}$.

The p-adic absolute value, as extended to the rationals, also behaves as one would hope. The following theorem serves to illustrate this.

Theorem 1.21. *Given $m, n, r, s \in \mathbb{Z}$, $n, s \neq 0$, $|m/n + r/s|_p \leq \max\{|m/n|_p, |r/s|_p\}$.*

Proof. We note that

$$\begin{aligned} ord_p\left(\frac{m}{n} + \frac{r}{s}\right) &= ord_p\left(\frac{ms + rn}{ns}\right) \\ &= ord_p(ms + rn) - ord_p(ns) \\ &= ord_p(ms + rn) - ord_p(n) - ord_p(s) \\ &\geq \min\{ord_p(ms), ord_p(rn)\} - ord_p(n) - ord_p(s) \\ &= \min\{ord_p(m) + ord_p(s), ord_p(r) + ord_p(n)\} - ord_p(n) - ord_p(s). \end{aligned}$$

Without loss of generality, assume that $\min\{ord_p(m) + ord_p(s), ord_p(r) + ord_p(n)\} = ord_p(m) + ord_p(s)$, then $ord_p(m/n + r/s) \geq ord_p(m) - ord_p(n) = ord_p(m/n)$. And so $2^{-ord_p(m/n+r/s)} \leq 2^{-ord_p(m/n)}$, or simply $|m/n + r/s|_p \leq |m/n|_p = \max\{|m/n|_p, |r/s|_p\}$. □

Next, we point out that the p-adic absolute value is a metric on $\mathbb{Q}$.

Definition 1.22. A metric on a set S is a function $d : S \times S \to \mathbb{R}_+$, that satisfies:

(i) $d(m, n) \geq 0$, and $d(m, n) = 0$ iff $m = n$, where $m, n \in S$.

(ii) $d(m,n) = d(n,m)$, for all $m, n \in S$.

(iii) $d(m,n) + d(n,r) \geq d(m,r)$, for all $m, n, r \in S$.

Theorem 1.23. *Given p, a prime number, the function $d_p : \mathbb{Q} \times \mathbb{Q} \to \mathbb{R}_+$, defined by $d_p(m,n) = |m-n|_p$, is a metric on $\mathbb{Q}$.*

Proof. Fix p prime, and let $m, n, r \in \mathbb{Q}$.

(i) By Theorem 1.15, part (i), we know that $d(m,n) = |m-n|_p \geq 0$. Furthermore we demonstrate that $d_p(m,n) = 0$ iff $m = n$, by first assuming that $m = n$. From this we deduce that $d_p(m-n) = |m-n|_p = 2^{-ord_p(m-n)} = 2^{-ord_p(0)} = 2^{-\infty}$, which we take to be 0. Next we assume, instead, that $d_p(m-n) = 0$, and hence $2^{-ord_p(m-n)} = 0$, which implies that $ord_p(m-n) = \infty$, hence $m - n = 0$.

(ii) We simply note that

$$\begin{aligned} d_p(m,n) &= |m-n|_p \\ &= 2^{-ord_p(m-n)} \\ &= 2^{-ord_p(n-m)} \\ &= |n-m|_p \\ &= d_p(n,m). \end{aligned}$$

(iii) We see that

$$\begin{aligned} d_p(m,r) &= |m-r|_p \\ &= |m-n+n-r|_p \\ &= |(m-n)+(n-r)|_p \\ &\leq |m-n|_p + |n-r|_p \\ &= d_p(m,n) + d_p(n,r). \end{aligned}$$

□

Endowed with this metric, the rationals poses a rather strange property: all triangles are isosceles. What is more, the sides that are equal are longer than the third.

Theorem 1.24. *Fix p prime. Given $a, b, c \in \mathbb{Q}$ with $|a-c|_p \geq |a-b|_p \geq |b-c|_p$, it is always true that $|a-c|_p = |a-b|_p$. (All triangles are isosceles.)*

Proof. Fix p prime. and let $a, b, c \in \mathbb{Q}$. We have that

$$d_p(a,b) = |a-b|_p$$

$$d_p(a,c) = |a-c|_p$$

$$d_p(b,c) = |b-c|_p.$$

The assumption $|a-c|_p \geq |a-b|_p \geq |b-c|_p$ can be made with no loss of generality. Noting that $(a-b)+(b-c) = (a-c)$ we use the ultrametric inequality to demonstrate that $|a-c|_p = |(a-b)+(b-c)|_p \leq max\{|a-b|_p, |b-c|_p\} = |a-b|_p$. Since we have assumed that $|a-c|_p \geq |a-b|_p$, and then subsequently shown that $|a-c|_p \leq |a-b|_p$, we have that $|a-c|_p = |a-b|_p$. □

CHAPTER 2: Ostrowski's Theorem

In the previous chapter, we defined an absolute value, $|\cdot|_p$, on $\mathbb{Q}$ that is very different from the one we are used to. One may be left wondering how many other strange and exotic absolute values may be contrived on $\mathbb{Q}$. As it turns out, the only absolute values possible on $\mathbb{Q}$ are ones that are: absolute values equivalent to the usual absolute value, absolute values equivalent to one of the infinitely many p-adic absolute values, and the trivial absolute value. This fact was realized and proved by Ostrowski.

We wish, however, to postpone formal presentation of the theorem and its proof in order to develop a better sense of why such a result should seem believable. Lets begin by getting a few preliminaries out of the way.

Definition 2.1. Define the trivial absolute value, $|\cdot|_t : \mathbb{Q} \to \mathbb{R}_+$ by:

(i) $|n|_t = 1, \quad \text{if } n \neq 0$

(ii) $|0|_t = 0.$

Definition 2.2. Define the usual absolute value, $|\cdot|_\infty : \mathbb{Q} \to \mathbb{R}_+$ by:

(i) $|n|_\infty = n, \quad \text{if } n \geq 0$

(ii) $|n|_\infty = -n, \quad \text{if } n \leq 0.$

To prove that the previous two definitions indeed define absolute value functions is trivial and we do not bother to do it. We do however need to prove the following theorem, as the result is used in the proof of Ostrowski's theorem.

Theorem 2.3. *Given an absolute value $|\cdot|$ on $\mathbb{Z}$, the following are equivalent:*

(i) $|z| \leq 1$ *for all* $z \in \mathbb{Z}$.

(ii) $|\cdot|$ *is non-Archimedean.*

Proof. Assume that $|x| \leq 1$ for all $x \in \mathbb{Z}$. Let $x, y \in \mathbb{N}$ and put $z = x/y$. By the binomial theorem

$$|z+1|^n = \left| \sum_{r=0}^{n} \binom{n}{r} z^r \right| \leq \sum_{r=0}^{n} \binom{n}{r} |z|^r.$$

Since $\binom{n}{r}$ is an integer, it has absolute value at most 1. If $|z| > 1$ then $|z|^r \leq |z|^n$ for all $r = 0, 1, ..., n$. If $|z| \leq 1, then |z|^r \leq 1$. Consequently, $|z+1|^n \leq (n+1)\max\{|z|^n, 1\}$. Taking n^{th} roots and letting $n \to \infty$, we get $|z+1| \leq \max\{|z|, 1\}$. Multiplying both sides of the inequality $|z+1| \leq \max\{|z|, 1\}$ by $|y|$ yields $|x+y| \leq \max\{|x|, |y|\}$.

Assume that $|\cdot|$ is non-Archimedean, that is, the ultrametric inequality holds. Since every integer z can be written

$$z = \pm(\underbrace{1+1+1+\cdots+1}_{n}),$$

by repeated application of the ultrametric inequality, we conclude that $|z| \leq 1$ for all $z \in \mathbb{Z}$. □

Again, what Ostrowski proved was that the only possible non-trivial absolute values on $\mathbb{Q}$ are ones that are equivalent to either the usual absolute value or to one of the p-adic absolute values. We should be specific about what we mean by equivalent:

Definition 2.4. We say that two absolute values $|\cdot|_1$, and $|\cdot|_2$, on $\mathbb{Q}$, are equivalent

if there exists an $\alpha > 0$ such that

$$|\cdot|_1{}^{\alpha} = |\cdot|_2.$$

We may now offer an exposition of the dominant idea behind the the proof of Ostrowski's theorem. The case of the trivial absolute value is not very interesting, and is easily dispensed with, so the ensuing discussion pertains to non-trivial absolute values. The general course of action in proving Ostrowski's theorem is to first assume that an absolute value on $\mathbb{Q}$ is Archimedean, and to show that it must be equivalent to the usual absolute value. Then, it is assumed that an absolute value on $\mathbb{Q}$ is non-Archimedean, and it is shown that, in this case, it must be equivalent to one of the infinitely many p-adic absolute values. The part of the theorem that we wish to focus on is the part where the absolute value on $\mathbb{Q}$ is assumed to be non-Archimedean. Lets get to it!

(Remember, this is not a proof!) Suppose $|\cdot|$ is a non-trivial, non-Archimedean absolute value on $\mathbb{Z}$. This means that the ultrametric inequality holds, and $|n| \leq 1$ for all $n \in \mathbb{Z}$. Now, suppose $|n| = 1$ for all $0 \neq n \in \mathbb{Z}$, then clearly $|\cdot|$ is the trivial absolute value, a contradiction. Hence $|n|$ cannot be 1 for all non-zero n in $\mathbb{Z}$. Or, equivalently, $|n| < 1$ for some $n \in \mathbb{Z}$. Let p be the least positive integer such that $|p| < 1$. We intentionally choose to use p for this integer, but point out that no assumptions have been made about p. In particular, we do not assume that p is prime, though we do anticipate that p will necessarily be prime if it is to play the role we have chosen for it. We will demonstrate this shortly.

Next we define $I = \{x \in \mathbb{Z} : |x| < 1\}$. Here, again, we make no assumptions about I, but anticipate that it will necessarily be an ideal of $\mathbb{Z}$, hence the choice of the letter I. By the ultrametric inequality, I is closed under addition, and if $n \in \mathbb{Z}$

and $k \in I$, then $|nk| = |n| \cdot |k| \leq 1 \cdot |k| < 1$. Thus, I is an ideal of $\mathbb{Z}$. In fact, $I = p\mathbb{Z}$. (Recall that $\mathbb{Z}$ is a principal ideal domain.)

Suppose, now, that $x, y \in \mathbb{Z}$ and $x, y \in I$, that is, $|xy| < 1$, or $|x| \cdot |y| < 1$. This implies that either $|x| < 1$ or $|y| < 1$. Thus I is a prime ideal, and so p is necessarily prime.

Now, let $n \in \mathbb{Z}$. Then write $n = p^r \cdot u$, where $n \in I$ and $p \nmid u$. Then $|n| = |p^r| \cdot |u| = |p|^r \cdot |u| = |p|^r$ because $n \notin I$.

Extending to $\mathbb{Q}$ we let $m, n \in \mathbb{Z}$ and write $m = p^r \cdot u$ and $n = p^s \cdot v$. Hence $|\frac{m}{n}| = \frac{|m|}{|n|} = \frac{|p^r \cdot u|}{|p^s \cdot v|} = |p^{r-s}| \cdot |\frac{u}{v}| = |p|^{r-s} \cdot |\frac{u}{v}| = |p|^{r-s}$.

It should be clear that the absolute value here is equivalent to the p-adic absolute value on account of its dependence on divisibility by the highest possible power of p, a prime number!

The full proof is written below. This particular version is based on the proof offered by Fernando Q. Gouvêya's *p-adic Numbers: An Introduction*, with only minor alterations. (See bibliography for full reference.)

Theorem 2.5. *Every non-trivial absolute value on $\mathbb{Q}$ is equivalent to one of the p-adic absolute values, where either p is prime or $p = \infty$. (The case where $p = \infty$ is the usual absolute value.)*

Proof. Let $|\cdot|$ be a non-trivial absolute value on $\mathbb{Q}$. Now, $|\cdot|$ can be either Archimedean, or non-Archimedean. We proceed by treating each case separately:

(i) Suppose $|\cdot|$ is Archimedean. We will show that $|\cdot|$ must be equivalent to the "usual" absolute value, i.e., $p = \infty$. Let

$$n_0 = \min\{n \in \mathbb{Z} : n > 0, |n| > 1\}.$$

Such an n_0 must exist, otherwise $|\cdot|$ would be non-Archimedean. Furthermore, we can find a positive, real α such that $|n_0| = {n_0}^{\alpha}$. We wish to prove that for every $x \in \mathbb{Q}$ we have $|x| = {|x|_\infty}^{\alpha}$. It suffices to show that this holds for all

$x \in \mathbb{N}$. We know that $|n| = n^\alpha$ holds for $n = n_0$. To prove this in general, we take $n \in \mathbb{N}$ and write it as an expansion in powers of n_0, in the form

$$n = a_0 + a_1 n_0 + a_2 {n_0}^2 + a_3 {n_0}^3 + \cdots + a_k {n_0}^k$$

where $0 < a_i < n_0 - 1$ and $a_k \neq 0$. Since k is determined by the inequality ${n_0}^k \leq n < {n_0}^{k+1}$. Hence we can write

$$k = \left\lfloor \frac{\log n}{\log n_0} \right\rfloor$$

where $\lfloor \cdot \rfloor$ denotes the "floor" function. (The "floor" function produces the greatest integer less than, or equal to, the input.) Taking absolute values, we obtain

$$\begin{aligned} |n| &= |a_0 + a_1 n_0 + a_2 {n_0}^2 + a_3 {n_0}^3 + \cdots + a_k {n_0}^k| \\ &\leq |a_0| + |a_1||n_0| + |a_2||{n_0}^2| + |a_3||{n_0}^3| + \cdots + |a_k||{n_0}^k| \end{aligned}$$

Since we chose n_0 to be the smallest positive integer whose absolute value was greater than 1, we know that $|a_i| \leq 1$. Hence,

$$\begin{aligned} |n| &\leq 1 + {n_0}^\alpha + {n_0}^{2\alpha} + {n_0}^{3\alpha} + \cdots + {n_0}^{k\alpha} \\ &= {n_0}^{k\alpha}(1 + {n_0}^{-\alpha} + {n_0}^{-2\alpha} + {n_0}^{-3\alpha} + \cdots + {n_0}^{-k\alpha}) \\ &\leq {n_0}^{k\alpha} \sum_{i=0}^{\infty} {n_0}^{-i\alpha} \\ &= {n_0}^{k\alpha} \frac{{n_0}^\alpha}{{n_0}^\alpha - 1} \end{aligned}$$

Set $C = \frac{{n_0}^\alpha}{{n_0}^\alpha - 1}$ and note that $C > 0$. Since $k = \log_{n_0} n$, the above yields

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

Note that this formula applies for any $n \in \mathbb{N}$, as the n we chose was arbitrary. Applying the formula to an integer of the form n^N we obtain

$$|n|^N = |(n^N)| \leq (n^N)^\alpha C.$$

Taking the N-th roots, we get

$$|n| \leq \sqrt[N]{C} n^\alpha.$$

Taking $N \to \infty$ we get $\sqrt[N]{C} \to 1$, hence $|n| \leq n^\alpha$. It remains to show that this

inequality holds in the opposite direction, also. Going back to the expression of n in powers of n_0

$$n = a_0 + a_1 n_0 + a_2 {n_0}^2 + a_3 {n_0}^3 + \cdots + a_k {n_0}^k$$

we note that since ${n_0}^{k+1} > n > {n_0}^k$, we can write

$$ {n_0}^{(k+1)\alpha} = |{n_0}^{k+1}| = |n + {n_0}^{k+1} - n| \leq | n| + |{n_0}^{k+1} - n|,$$

and so

$$|n| \geq {n_0}^{(k+1)\alpha} - |{n_0}^{(k+1)} - n| \geq {n_0}^{(k+1)\alpha} - ({n_0}^{k+1} - n)^\alpha$$

where we have invoked the inequality $|n| \leq n^\alpha$. Now, since $n \geq {n_0}^k$, we have

$$\begin{aligned} |n| &\geq {n_0}^{(k+1)\alpha} - ({n_0}^{k+1} - {n_0}^k)^\alpha \\ &= {n_0}^{(k+1)\alpha}\left(1 - \left(1 - \frac{1}{n_0}\right)^\alpha\right) \\ &= C' {n_0}^{(k+1)\alpha} \\ &> C' n^\alpha. \end{aligned}$$

We note that $C' = 1 - (1 - \frac{1}{n_0})^\alpha > 0$ does not depend on n. Now, by the same process as above, we derive the opposite inequality $|n| \geq n^\alpha$ and hence we have that $|n| = n^\alpha$. This proves that $|\cdot|$ is equivalent to the "usual" absolute value $|\cdot|_\infty$, as claimed.

(ii) Suppose $|\cdot|$ is non-Archimedean. Recalling that this implies $|n| \leq 1$, for all integers n, and hence, since $|\cdot|$ is non-trivial, there must exist an $n_0 = \min\{n \in \mathbb{N} : |n| \leq 1\}$. We demonstrate that n_0 must be prime by supposing the contrary, hence $n_0 = ab$ for some $a, b \in \mathbb{N}$ with $0 \neq a, b < n_0$. Now, by our choice of n_0 we have $|a| = |b| = 1$, and $|n_0| < 1$. This is a contradiction, hence n_0 is prime. Setting $n_0 = p$ (for prime) we proceed to show that $|\cdot|$ is equivalent to $|\cdot|_p$ for the particular value of p. We now show that if $n \in \mathbb{Z}$ is not divisible by p, then $|n| = 1$. Dividing n by p we are left with a remainder r such that $0 < r < p$, as in

$$n = ps + r.$$

Recalling that

$$p = n_0 = \min\{n \in \mathbb{Z} : |n| \leq |1|,$$

we can conclude that $|r| = 1$. We can also conclude that $|sp| < 1$, because $|\cdot|$ is non-Archimedean. Recalling that $|p| < 1$, it follows that $|n| = 1$. Finally, given

any $n \in \mathbb{Z}$ we write it as $n = p^v n'$ with $p \nmid n'$. So

$$|n| = |p|^v |n'| = |p|^v = c^{-v}$$

where $c = |p|^{-1} > 1$, so that $|\cdot|$ is equivalent to the p-adic $|\cdot|_p$ as claimed.

□

CHAPTER 3: Some Topology

In the previous chapters we have defined a notion of the size of p-adic numbers by the p-adic absolute value. We also showed that such a definition is quite natural, as it is one of only three types of absolute values possible on $\mathbb{Q}$.

In this chapter we offer a different approach to the theory of p-adic numbers. We will define a topology on the set of infinite sums in x with complex coefficients, then show how such a structure can be used to describe p-adic numbers. As the title of this chapter suggests, we will need to take the completion of the space we create, which will be a metric space, of course. The particular type of topology that we need to construct relies on the use of an ideal, I, in its formulation, hence the name I-adic.

We begin by clarifying some notation used in this chapter:

$\mathbb{C}[x]$ - ring of polynomials in x with complex coefficients.

$\mathbb{C}[[x]]$ - ring of infinite sums in x with complex coefficients.

$\mathbb{C}\{x\}$ - ring of convergent series in x with complex coefficients.

$\mathbb{C}(x)$ - field of rational functions in x with complex coefficients.

$\mathbb{C}((x))$ - field of Laurent series in x with complex coefficients.

We define a topological space, $(\mathcal{T}_x, \mathbb{C}[[x]])$, by taking, as open sets, all unions of sets of the form $f(x) + x^n \cdot \mathbb{C}[[x]]$, where $f(x)$ is a polynomial in x with complex coefficients. We also consider the empty set as open. Note that if we endow $\mathbb{C}$ with the discrete topology, and identify the set of formal power series, $\mathbb{C}[[x]]$ by $\mathbb{C}^{\mathbb{N}} = \{(a_0, a_1, a_2, ...) : a_i \in \mathbb{C}\}$, then $(\mathcal{T}_x, \mathbb{C}[[x]])$ is a product topology.

To get a better grip on $(\mathcal{T}_x, \mathbb{C}[[x]])$ as a mathematical object we offer the following example.

Example 3.1. Let

$$\begin{aligned} U = \{&(\mathbf{1}+\mathbf{i})+(\mathbf{9}+\mathbf{2i})\mathbf{x}+\mathbf{8x^2}+\mathbf{x^3}+0x^4+0x^5+0x^6+0x^7+\cdots,\\ &(\mathbf{1}+\mathbf{i})+(\mathbf{9}+\mathbf{2i})\mathbf{x}+\mathbf{8x^2}+\mathbf{x^3}+1x^4+6x^5+(4+7i)x^6+3x^7+\cdots,\\ &(\mathbf{1}+\mathbf{i})+(\mathbf{9}+\mathbf{2i})\mathbf{x}+\mathbf{8x^2}+\mathbf{x^3}+(2+2i)x^4+3x^5+4x^6+7x^7+\cdots,\\ &(\mathbf{1}+\mathbf{i})+(\mathbf{9}+\mathbf{2i})\mathbf{x}+\mathbf{8x^2}+\mathbf{x^3}+9x^4+6x^5+(3-3i)x^6+9x^7+\cdots,\\ &(\mathbf{1}+\mathbf{i})+(\mathbf{9}+\mathbf{2i})\mathbf{x}+\mathbf{8x^2}+\mathbf{x^3}+4x^4+0x^5+(1+9i)x^6+6x^7+\cdots,\\ &(\mathbf{1}+\mathbf{i})+(\mathbf{9}+\mathbf{2i})\mathbf{x}+\mathbf{8x^2}+\mathbf{x^3}+2x^4+(6-i)x^5+0x^6+2x^7+\cdots,\\ &(\mathbf{1}+\mathbf{i})+(\mathbf{9}+\mathbf{2i})\mathbf{x}+\mathbf{8x^2}+\mathbf{x^3}+7x^4+8x^5+7x^6+(4+i)x^7+\cdots,\\ &(\mathbf{1}+\mathbf{i})+(\mathbf{9}+\mathbf{2i})\mathbf{x}+\mathbf{8x^2}+\mathbf{x^3}+(9-4i)x^4+9x^5+9x^6+6x^7+\cdots,\\ &...\}. \end{aligned}$$

Then U is an open set in $(\mathcal{T}_x, \mathbb{C}[[x]])$, as it is of the form $f(x) + x^n \cdot \mathbb{C}[[x]]$, with $f(x) = (1+i) + (9+2i)x + 8x^2 + 1x^3$, and $n = 4$.

We should be thorough and, before continuing, prove that $\mathcal{T}_x$ is indeed a topology on $\mathbb{C}[[x]]$.

Definition 3.2. A topology on a set S is a collection $\mathcal{T}$ of subsets of X having the following properties.

(i) $\varnothing$ and S are in $\mathcal{T}$.

(ii) The union of the elements of any subcollection of open sets is open, as the union .

(iii) The intersection of the elements of any finite subcollection of $\mathcal{T}$ is in $\mathcal{T}$.

A set S endowed with a topology $\mathcal{T}$ is called a topological space and is denoted by $(\mathcal{T}, S)$.

Theorem 3.3. *Taking as open sets,the empty set, and all unions of sets of the form $f(x) + x^n \cdot \mathbb{C}[[x]]$, where $f(x)$ is a polynomial in x with complex coefficients, forms the topological space $(\mathcal{T}_x, \mathbb{C}[[x]])$.*

Proof. We choose a descriptive proof style to better convey the nature of the open sets in $(\mathcal{T}_x, \mathbb{C}[[x]])$.

(i) By definition, $\varnothing$ is an open set, and $\mathbb{C}[[x]]$ is open by taking $f(x) = 0$, with $n = -1$. (We take the degree of $f(x) = 0$ to be -1.)

(ii) The union of the elements of any subcollection of open sets is open by definition.

(iii) The intersection of the elements of any finite subcollection of open sets is open because

$$S = \bigcap_{0<j\leq k} \left(\bigcup_{i\in I_j} f_{i,j}(x) + x^{n_{i,j}} \cdot \mathbb{C}[[x]] \right),$$

is open. To see why S is open, we note that S is a finite intersection of (possibly infinite) collections of sets of the form $f(x) + x^n \cdot \mathbb{C}[[x]]$. Each such collection in U is indexed by an index set I_j. Furthermore, each such collection, indexed by j, with $0 < j < k$, has a smallest $n_{i,j}$, call it N_j, and so defines a set of the form

$$\bigcup_{i\in I_j} f_{i,j}(x) + x^{n_{i,j}} \cdot \mathbb{C}[[x]] = a_{0,j} + a_{1,j}x + a_{2,j}x^2 + \cdots + a_{N_j-1}x^{N_j-1} + x^{N_j} \cdot \mathbb{C}[[x]]$$

where $a_{0,j}$ is an element of a set $A_{0,j}$ of possible coefficients of x^0 defined by the j-th union, $a_{1,j}$ is an element of a set $A_{1,j}$ of possible coefficients of x^1 defined by the j-th union, and so on. Notice that any combination of complex numbers is possible for each $A_{m,j}$. (This describes the nature of open sets in this topology, in general.)

Now, taking the intersection of any finite number of such unions yields a set, we called it S, of the form

$$S = a_0 + a_1x + a_2x^2 + \cdots a_{N-1}x^{N-1} + x^N \cdot \mathbb{C}[[x]],$$

where

$$a_0 \in \bigcap_j A_{0,j}, \quad a_1 \in \bigcap_j A_{1,j}, \quad a_2 \in \bigcap_j A_{2,j}, \quad ...$$

and $N = \max\{N_j : 0 < j \leq k\}$. This is clearly an open set, as it neatly fits the general description of open sets mentioned in the previous paragraph.

□

The topological space $(\mathcal{T}_x, \mathbb{C}[[x]])$ satisfies a condition that is a little more stringent than just being a topological space:

Definition 3.4. A topological space $(\mathcal{T}, S)$ is said to be Hausdorff if for each pair s_1, s_2 of distinct points of S, there exist disjoint open sets U_1, U_2 in $(\mathcal{T}, S)$, such that $s_1 \in U_1$ and $s_2 \in U_2$.

Theorem 3.5. *The topological space $(\mathcal{T}_x, \mathbb{C}[[x]])$ is Hausdorff.*

Proof. Suppose that s_1 and s_2 are distinct infinite sums of powers of x, that is

$$s_1 = a_0x^0 + a_1x^1 + a_2x^2 + a_3x^3 + \cdots$$

$$s_2 = b_0x^0 + b_1x^1 + b_2x^2 + b_3x^3 + \cdots$$

where $a_n \neq b_n$ for at least one $n \in \mathbb{N}$. In fact, set $m = \min\{n \in \mathbb{N} : a_n \neq b_n\}$. Now we define the open sets:

$$U_1 = a_0x^0 + a_1x^1 + a_2x^2 + \cdots + a_mx^m + x^{m+1} \cdot \mathbb{C}[[x]],$$

$$U_2 = b_0x^0 + b_1x^1 + b_2x^2 + \cdots + b_mx^m + x^{m+1} \cdot \mathbb{C}[[x]].$$

The open sets U_1 and U_2 are disjoint, as $a_m \neq b_m$, and $s_1 \in U_1$ and $s_2 \in U_2$. □

This result allows us to make use of the following theorem in our discussion of $(\mathcal{T}_x, \mathbb{C}[[x]])$:

Theorem 3.6. *If $(\mathcal{T}, S)$ is a Hausdorff topological space, then a sequence of points of $(\mathcal{T}, S)$ converges to at most one point of $(\mathcal{T}, S)$.*

Proof. Suppose that $\{s_n\}$ is a sequence of points in $(\mathcal{T}, S)$ that converges to s. If $s \neq t$, let U and V be disjoint neighborhoods of s and t, respectively. Since U contains $\{s_n\}$ for all but finitely many values of n, the set V cannot. Therefore, $\{s_n\}$ cannot converge to t. □

To continue our discussion, we need to define the x-adic order function and the x-adic absolute value for polynomials.

Definition 3.7. Define the x-adic order function as $ord_x : \mathbb{C}[x] \to \mathbb{Z}$ by

(i) $ord_x(f(x)) = l$, where $x^l \mid f(x)$, but $x^{l+1} \nmid f(x)$, and $f(x) \neq 0$

(ii) $ord_x(0) = \infty$.

Definition 3.8. Define the x-adic absolute value as $|\cdot|_x : \mathbb{C}[x] \to \mathbb{R}_+$ by

(i) $|n|_x = 2^{-ord_x(f(x))}$

(ii) $|0|_x = 0$. (We define $2^{-\infty} = 0$.)

The theorems in chapter 1 regarding the p-adic order function and p-adic absolute value all have their counterparts for the x-adic order function and x-adic absolute value. To document the theorems and their proofs adds nothing to our discussion, so we proceed without doing so. The similarity between the the p-adic and x-adic absolute values should make the following theorem quite palatable without any proof.

Theorem 3.9. *The function $d_x : \mathbb{C}[x] \times \mathbb{C}[x] \to \mathbb{R}_+$, defined by $d_x(f(x), g(x)) = |f(x) - g(x)|_x$, is a metric on $\mathbb{C}[x]$.*

We are now in a position to sensibly state some theorems about the topological space, $(\mathcal{T}_x, \mathbb{C}[[x]])$, that we have constructed. First, we recall the definitions of the limit of a sequence, and of a Cauchy sequence:

Definition 3.10. If the sequence $\{s_n\}$ of points of the Hausdorff topological space $(\mathcal{T}, S)$ converges to the point s of $(\mathcal{T}, S)$, we often write $\lim_{n\to\infty} s_n = s$, and say that s is the limit of the sequence $\{s_n\}$.

Definition 3.11. Let $(\mathcal{T}, S)$ be a metric space under the metric d. A sequence $\{s_n\}_{n\in\mathbb{N}}$ of points in $(\mathcal{T}, S)$ is said to be Cauchy in $(\mathcal{T}, S)$ under the metric d, if it has the property that given $\epsilon > 0$, there is an integer N such that $d(x_n, x_m) < \epsilon$ whenever $n, m \geq N$. The metric space is said to be complete if every Cauchy sequence converges.

Theorem 3.12. *In the topological space* $(\mathcal{T}_x, \mathbb{C}[[x]])$, $\{x^n\}_{n\in\mathbb{N}}$ *is a Cauchy sequence and* $\lim_{n\to\infty} x^n = 0$.

Proof. Let U be an open set in $(\mathcal{T}_x, \mathbb{C}[[x]])$ containing $0 = 0 + 0x + 0x^2 + 0x^3 + \cdots$. Then

$$U = \bigcup_i x^{n_i}\mathbb{C}[[x]]$$

or

$$U = x^n\mathbb{C}[[x]]$$

where

$$n = \min_i(n_i).$$

Now if $k > n$, then $x^k \in U$. Therefore

$$\lim_{k\to\infty} x^k = 0 + 0 + 0 + 0 + \cdots = 0.$$

□

In fact, we can we can claim a more general, result.

Theorem 3.13. *Fix $a_0, a_1, a_2, ... \in \mathbb{C}$. Consider the sequence $\{s_n\}_{n\in\mathbb{N}}$ where*

$$s_n = \sum_{k=0}^{n} a_k x^k.$$

Then $\{s_n\}$ is a Cauchy sequence and

$$\lim_{n\to\infty} s_n = \sum_{k=0}^{\infty} a_k x^k.$$

Proof. Let U be an open set in $(\mathcal{T}_x, \mathbb{C}[[x]])$ containing 0. Then there is an $N \in \mathbb{N}$ such that if $k, l > N$, then $a_k - a_l \in U$. Let

$$f = x^n \sum_{n=0}^{\infty} a_k x^k,$$

where $a_0 \neq 0$. Here n is the order of f, and $|f| = 2^{-n}$. We can write

$$U = \bigcup_i x^{n_i}\mathbb{C}[[x]]$$

or simply

$$U = x^n\mathbb{C}[[x]]$$

where

$$n = \min_i(n_i).$$

Now if $k \geq l > n$, then

$$s_l - s_k = \sum_{i=l}^{k} a_i x_i \in x^n \mathbb{C}[[x]] = U.$$

Furthermore, if $l > n$, then

$$\sum_{k=0}^{\infty} a_k x^k - s_l = \sum_{k=l+1}^{\infty} a_k x^k = x^n \sum_{k=l-n+1} a_{k+n} x^k \in U.$$

□

We are nearing the main result of the chapter, the definition of $\mathbb{Z}_p$ and $\mathbb{Q}_p$. To understand the definitions, we need to define the completion of a topological space.

Definition 3.14. Let $(\mathcal{T}, S)$ be a metric topological space. If $h : (\mathcal{T}, S) \to (\mathcal{T}', S')$ is an isometric imbedding of $(\mathcal{T}, S)$ into a complete metric topological space $(\mathcal{T}', S')$, then the subspace $\overline{h((\mathcal{T}, S))}$ of $(\mathcal{T}', S')$ is a complete metric space. It is called the completion of $(\mathcal{T}, S)$.

It should be noted that the completion in the previous definition is uniquely determined up to isometry. A fact we do not concern ourselves with too much, and hence offer no proof.

Theorem 3.15. *The completion of* $\mathbb{C}[x]$ *is* $\mathbb{C}[[x]]$ *under the* x*-adic metric.*

Proof. To show that the completion of $\mathbb{C}[x]$ is $\mathbb{C}[[x]]$ under the x-adic metric, it suffices to show that every Cauchy sequence converges in $\mathbb{C}[[x]]$. Let $\{f_n\}$ be a Cauchy sequence, then we can write $f_n = a_{n_0} + a_{n_1}x + a_{n_2}x^2 + a_{n_3}x^3 + \cdots$. Find N_0 such that for all $n, m \geq N_0$ we have $ord_x(f_n - f_m) > 0$. Define $b_0 = a_{N_0 0}$.

In general, for each $l \in \mathbb{N}$, find $N_l > N_{l-1}$ such that for all $n, m \geq N_l$ we have $ord_x(f_n - f_m) > l$. Define $b_l = a_{N_l l}$.

Define

$$g = \sum_{i=0}^{\infty} b_{N_i i} x^i \in \mathbb{C}[[x]].$$

We then note that

$$g = \lim_{n \to \infty} f_n.$$

□

CHAPTER 4: Hensel's Lemma

Very often it is helpful to work a few specific problems, to understand the general case of the problem. For example, it may be useful to solve several quadratic equations by completing the square in order to better understand the derivation of the quadratic formula. In this chapter we show that we can find better and better approximations of the root of a particular polynomial, and use this example to motivate the construction of an algorithm for approximating the roots of polynomials in general. The algorithm, known as Hensel's Lemma, is the subject of this chapter.

Example 4.1. We wish to find the roots of $f(x) = x^2 + 1$, that is we wish to solve $x^2 + 1 = 0$ for x. We will proceed by solving ${x_n}^2 + 1 \equiv 0 \mod 5^n$, for successively larger values of n. We will find the following solutions:

$$\begin{aligned} {x_1}^2 + 1 &\equiv 0 \mod 5 & x_1 &= 2 \\ {x_2}^2 + 1 &\equiv 0 \mod 5^2 & x_2 &= 7 \\ {x_3}^2 + 1 &\equiv 0 \mod 5^3 & x_3 &= 57 \\ {x_4}^2 + 1 &\equiv 0 \mod 5^4 & x_4 &= 182 \end{aligned}$$

The particular solutions here are less important to us than the method by which we will find them. We wish to demonstrate the application of an algorithm that produces x_n for progressively higher values of n. The algorithm begins with, by any method, finding a solution to

$${x_1}^2 + 1 \equiv 0 \mod 5.$$

This solution is $x_1 = 2$. We then note that the solution to ${x_2}^2 + 1 \equiv 0 \mod 5^2$ can

be found by substituting $x_2 = x_1 + 5h_1$. This makes finding x_2 a rather simple task. The new equation becomes:

$$\begin{aligned}
{x_2}^2 + 1 &\equiv 0 \mod 5^2 \\
(x_1 + 5h_1)^2 + 1 &\equiv 0 \mod 5^2 \\
{x_1}^2 + 10x_1h_1 + 5^2{h_1}^2 + 1 &\equiv 0 \mod 5^2 \\
{x_1}^2 + 10x_1h_1 + 1 &\equiv 0 \mod 5^2 \\
({x_1}^2 + 1) + x_1(10h_1) &\equiv 0 \mod 5^2 \\
(2^2 + 1) + 2(10h_1) &\equiv 0 \mod 5^2 \\
5 + 20h_1 &\equiv 0 \mod 5^2 \\
5(1 + 4h_1) &\equiv 0 \mod 5^2 \\
1 + 4h_1 &\equiv 0 \mod 5
\end{aligned}$$

We solve this congruence by taking $h_1 = 1$. Then we find $x_2 = x_1 + 5h_1 = 2 + 5(1) = 7$. Repeating this procedure we substitute $x_3 = x_2 + 5^2h_2 = x_1 + 5h_1 + 5^2h_2 = 7 + 5^2h_2$, and take $h_2 = 2$ to obtain $x_3 = 57$. Repeating this procedure, we find $h_3 = 1$, hence $x_4 = x_3 + 5^3h_3 = 57 + 125 = 182$. Continuing, we find $h_4 = 3$, $h_5 = 4$ and $h_6 = 2$, and hence $x_5 = 2057$, $x_6 = 14557$ and $x_7 = 45807$. We need not stop. In fact, continuing this process we find sums of the form

$$x_n = x_1 + h_1 5 + h_2 5^2 + h_3 5^3 + h_4 5^4 + \cdots + h_{n-1} 5^{n-1},$$

that are progressively better (as we take higher and higher values of n) 5-adic approximations of the 5-adic solution to $f(x) = x^2 + 1$. Remember, the numbers we add to

the tail-end of the sum are divisible by higher and higher powers of 5, hence they are smaller and smaller. Taking $n \to \infty$ we obtain the 5-adic solution to $f(x) = x^2 + 1$.

The algorithm we have demonstrated can be generalized. It is known as Hensel's Lemma, for Kurt Hensel (1861-1941), one of the chief pioneers of p-adic number theory.

Theorem 4.2. *Let $F(X) = a_0 + a_1X + a_2X^2 + \cdots + a_nX^n$ be a polynomial with coefficients in $\mathbb{Z}_p$. Suppose that there exists a p-adic integer $\alpha_1 \in \mathbb{Z}_p$ such that the following two conditions hold:*

$$F(\alpha_1) \equiv 0 \mod p\mathbb{Z}_p, \quad \textit{and,}$$

$$F'(\alpha_1) \not\equiv 0 \mod p\mathbb{Z}_p$$

where $F'(X)$ is the formal derivative of $F(X)$. Then there exists a p-adic integer $\alpha \in \mathbb{Z}_p$ such that:

$$\alpha \equiv \alpha_1 \mod p\mathbb{Z}_p, \quad \textit{and,}$$

$$F(\alpha) = 0.$$

Proof. We wish to construct a sequence of integers $\alpha_1, \alpha_2, ...\alpha_n, ...$ such that for all $n \geq 1$ we have

(i) $F(\alpha_n) \equiv 0 \mod p^n$

(ii) $\alpha_n \equiv \alpha_{n+1} \mod p^n$.

Such a sequence will be Cauchy, and its limit, α, will satisfy $F(\alpha) = 0$ (by continuity), and $\alpha \equiv \alpha_1 \mod p$ (by construction). Thus, once we define α_{n+1} in terms of α_n, the proof will be complete.

We have assumed that α_1 exists, and proceed to find α_2 we note that by (ii), above, it must be that $\alpha_2 = \alpha_1 + b_1 p$ for some integer $b_1 \in \mathbb{Z}_p$. We plug this into the polynomial $F(X)$ to obtain

$$\begin{aligned} F(\alpha_2) &= F(\alpha_1 + b_1 p) \\ &= F(\alpha_1) + F'(\alpha_1) b_1 p + \text{terms in } p^n, n \geq 2 \\ &\equiv F(\alpha_1) + F'(\alpha_1) b_1 p \mod p^2. \end{aligned}$$

Now we must show that one can find b_1 such that $F(\alpha_1) + F'(\alpha_1) b_1 p \equiv 0 \mod p^2$. By condition$(i)$, above, we know that $F(\alpha_1) \equiv 0 \mod p$, so that $F(\alpha_1) = p x_1$ for some x_1. Thus we can write

$$p x_1 + F'(\alpha_1) b_1 p \equiv 0 \mod p^2.$$

Dividing by p, we obtain

$$x_1 + F'(\alpha_1) b_1 \equiv 0 \mod p.$$

Because $F'(\alpha_1)$ is an integer not divisible by p, there is an integer c, $0 < c < p$, such that

$$c F'(\alpha_1) \equiv 1 \mod p.$$

Hence we find

$$b_1 \equiv -c x_1 \mod p.$$

Note that it is possible to find $b_1 \in \mathbb{Z}$ such that $0 \leq b_1 \leq p - 1$. Given this choice of

b_1, we set $\alpha_2 = \alpha_1 + b_1 p$. This calculation can be performed, to find α_{n+1} from α_n. The calculation goes like this:

$$\begin{aligned} F(\alpha_{n+1}) &= F(\alpha_n + b_n p^n) \\ &= F(\alpha_n) + F'(\alpha_n) b_n p^n + \text{terms in } p^{nk}, k \geq 2 \\ &\equiv F(\alpha_n) + F'(\alpha_n) b_n p^n \mod p^{n+1}. \end{aligned}$$

Since $F(\alpha_n) \equiv 0 \mod p^n$, we may write $F(\alpha_n) = x_n p^n$ for some integer x_n. Thus we can write

$$p^n x_n + F'(\alpha_n) b_n p^n \equiv 0 \mod p^{n+1}.$$

Dividing by p^n, we obtain

$$x_n + F'(\alpha_n) b_n \equiv 0 \mod p.$$

Because $\alpha_1 \equiv \alpha_n \mod p$, $F'(\alpha_1) \equiv F'(\alpha_n) \mod p$. Hence,

$$cF'(\alpha_n) \equiv 1 \mod p,$$

and we find

$$b_n \equiv -cx_n \mod p.$$

Note that it is possible to find $b_n \in \mathbb{Z}$ such that $0 \leq b_n \leq p-1$. Put $\alpha_{n+1} = \alpha_n + b_n p^n$, and note that conditions (i) and (ii) are satisfied. □

Hensel's Lemma will prove to be essential to our discussion of Newton polygons in the coming chapters.

Meanwhile, we can use Hensel's lemma to show, for example, that the fields $\mathbb{Q}_3$ and $\mathbb{Q}_5$ are not isomorphic. Indeed, as suggested (but not stated) in Example 4.1, by Hensel's lemma the equation $x^2 + 1 = 0$ has a solution in $\mathbb{Q}_5$. However, since the equation $x^2 + 1 \equiv 0 \mod 3$ has no solution, the equation $x^2 + 1 = 0$ has no solution in $\mathbb{Q}_3$. Hence $\mathbb{Q}_3$ and $\mathbb{Q}_5$ are not isomorphic.

CHAPTER 5: Defining Newton Polygons

Given a polynomial over a field, the behavior of the roots (assuming they exist) can be discovered by a technique that utilizes Newton polygons. This chapter defines what a Newton polygon is, and describes a technique to construct one.

As with the previous chapter, it makes good sense here to begin with an example. We will take some polynomial in x over the field $\mathbb{Q}_p$ and construct its Newton polygon by plotting points on a plane, then connecting the points with line segments in a special way. The points we shall plot for a given polynomial

$$f(x) = a_0x^m + a_1x^{m+1} + a_2x^{m+2} + a_3x^{m+3} + \cdots + a_nx^{m+n},$$

where $a_i \in \mathbb{Q}_p[x]$, will be found by first factoring out any powers of x

$$f(x) = x^m(a_0 + a_1x + a_2x^2 + a_3x^3 + \cdots + a_nx^n).$$

And then factoring out a_0, leaving a polynomial of the form

$$f(x) = a_0x^m(1 + b_1x + b_2x^2 + b_3x^3 + \cdots + b_nx^n),$$

where

$$b_i = \frac{a_i}{a_0},$$

for $1 \leq i \leq n$. We now plot the points

$$(0,0), (1, ord_p(b_1)), (2, ord_p(b_2)), ..., (i, ord_p(b_i)), ...(n, ord_p(b_n))$$

on the plane representing $F \times \mathbb{R}$. Note that we need to fix some prime p in order to do

this. We then connect the points with line segments, beginning with the point $(0, 0)$ connected to the point, call it B the will produce the smallest possible slope for the line segment. Next, we connect B to a point to the right of it, one that will produce the smallest slope for the second line segment, and so on. A geometric way to visualize the construction is to think of a hanging string, pinned at one end to the point $(0, 0)$, being pulled widdershins around the points by the other end. In doing this, the points catch the string and form a "bend" in it. When all points not at infinity are wrapped in this way, the process stops. A note should be made here about points of the form $(i, ord_p(0))$. Since we take $ord_p(0)$ to be ∞, these points do not interfere with our construction, as they do not yield small slopes in the construction of line segments. It is just as well to ignore such points all together. The final construction is called the Newton polygon for $f(x)$.

At this point, a simple example may be beneficial to the reader.

Example 5.1. Given $p = 5$, $f(x) = 5x^3 + \frac{1}{5}x^5 + 25x^6 + 125x^7 + 35x^8 + 3125x^9$, we construct the newton polygon by first writing

$$f(x) = 5x^3(1 + \frac{1}{25}x^2 + 5x^3 + 25x^4 + 7x^5 + 625x^6).$$

We then plot the points

$$(0, 0), (2, ord_p(\frac{1}{25})), (3, ord_p(5)), (4, ord_p(25)), (5, ord_p(7)), (6, ord(625)),$$

that is

$$(0, 0), (2, -2), (3, 1), (4, 2), (5, 0), (6, 4).$$

Plotting these points and connecting $(0, 0), (2, -2), (5, 0), (6, 4)$, we get the Newton polygon we desire. (The reader is encouraged to sketch this Newton polygon.)

Such a construction can be described as the lower convex hull of the points plotted. There are three things we wish to pay close attention to in the Newton polygon of a polynomial:

(i) The slopes of the line segments, which we shall call Newton slopes.

(ii) The length of the projection of each Newton slope onto the i-axis.

(iii) The values of i at each of the vertices of the Newton polygon.

The significance of these details shall be made clear in the next chapter, which explores the connection between Newton polygons and the roots of the polynomials that generate them.

CHAPTER 6: Newton Polygons and Roots of Polynomials

In this chapter we will demonstrate how Newton polygons can be used to approximate the zeros of polynomials. Given a polynomial of the desired form (as described in the previous chapter)

$$f(x) = a_0x^m(1 + b_1x + b_2x^2 + b_3x^3 + \cdots + b_nx^n),$$

we can construct the Newton polygon for $f(x)$ by plotting the points $(0, 0)$, $(1, ord_p(b_1))$, $(2, ord_p(b_2))$,... , $(n, ord_p(b_n))$.

We then wish to discover the size of the roots of $f(x)$, that is, the solutions to

$$0 = a_0x^m(1 + b_1x + b_2x^2 + b_3x^3 + \cdots + b_nx^n).$$

To do this, we collect the information stipulated by $(i) - (iii)$ at the end of the previous chapter. What to do with this information is best understood by looking at an example.

Example 6.1. Lets look at

$$f(x) = 5x^3(1 + \frac{1}{25}x^2 + 5x^3 + 25x^4 + 7x^5 + 625x^6).$$

again. (Recall that $p = 5$, here.) We plot the points

$$(0, 0), (2, -2), (3, 1), (4, 2), (5, 0), (6, 4),$$

and construct the lower convex hull to form the Newton polygon for $f(x)$. We note that the Newton slopes (from left to right) are -1, $\frac{2}{3}$, and 4. These have projections

onto the x-axis of length 2, 3, and 1, respectively, and the vertices of the Newton polygon have i-values 0, 2, 5, and 6.

From this information we can determine that $f(x)$ has, aside from the three roots of order ∞:

(i) 2 roots (in $\mathbb{C}_p$, counting multiplicities) of order -1,

(ii) 3 roots (in $\mathbb{C}_p$, counting multiplicities) of order $2/3$,

(iii) 1 root (in $\mathbb{C}_p$, counting multiplicities) of order 4.

This is a total of 9 roots, as expected. ($\mathbb{C}_p$ is the completion of algebraic closure of $\mathbb{Q}_p$) We constructed these conclusions by claiming that the lengths of the projections onto the x-axis of the Newton slopes gave us the number of roots of order given by the Newton slope that was projected. It may be useful to refer to the diagram in the previous chapter.

In general, this (chief result of the thesis) can be formulated as follows:

Theorem 6.2. *Fix a prime number p. Let $f(x) = 1 + a_1x + a_2x^2 + \cdots + a_nx^n$ be a polynomial in $\mathbb{Q}_p[x]$, with Newton slopes $m_1, m_2, ..., m_r$, in increasing order. Let $i_1, i_2, ..., i_r$, be the corresponding lengths of the projections of the Newton slopes. Then for each k, where $1 \leq k \leq r$, $f(x)$ has exactly i_k roots (in $\mathbb{C}_p$, counting multiplicities) of absolute value p^{m_k}. Furthermore, $i_1 + \cdots + i_r = n$.*

Proof. Following the notation above, we wish, first, to note that the slope defined by two points, $(i, |a_i|_p), (j, |a_j|_p)$, where $j > i$, is given by

$$m_{i,j} = -\frac{ord_p(a_i) - ord_p(a_j)}{j - i}.$$

Suppose that $m_{i,j} > m_{i,k}$, where $i < j < k$ that is

$$ord_p(a_j) > ord_p(a_i) + (j-i)m_{i,k}.$$

Supposing this, we assume the Newton polygon has been incorrectly constructed. (Sketch the scenario to discover exactly how.) We now wish to define two scaling factors, t, and α. We stipulate that $|t| = 1$, and set $\alpha = p^{-m_{i,j}}$. This gives us

$$ord_p(\alpha) = \frac{ord_p(a_i) - ord_p(a_j)}{j-i}.$$

We wish to show that $|a_k\alpha^k t^k|_p > |a_i\alpha^i t^i|_p$, thereby violating the requirement that the two largest terms must cancel. (See chapter 1 theorems regarding ultrametric inequality.) Since $m_{i,k} < m_{i,j}$, we can write $-m_{i,j} < -m_{i,k}$, then by substitution, we obtain

$$\begin{aligned}
& \frac{ord_p(a_i) - ord_p(a_k)}{k-i} > ord_p(\alpha) \\
\Rightarrow \quad & ord_p(a_i) - ord_p(a_k) > (k-i)ord_p(\alpha) \\
\Rightarrow \quad & ord_p(a_i) + (i)ord_p(\alpha) > ord_p(a_k) + (k)ord_p(\alpha) \\
\Rightarrow \quad & ord_p(a_i\alpha^i t^i) > ord_p(a_k\alpha^k t^k)
\end{aligned}$$

Now put $\alpha = p^{-m_{j,k}}$, so that

$$ord_p(\alpha) = \frac{ord_p(a_j) - ord_p(a_k)}{k-j}.$$

We wish to show that $|a_i\alpha^i t^i|_p > |a_j\alpha^j t^j|_p$, thereby violating the requirement that the

two largest terms must cancel. Since $m_{j,k} < m_{i,j}$, we can write $-m_{i,j} < -m_{j,k}$, then by substitution, we obtain

$$\begin{aligned} & \frac{ord_p(a_i) - ord_p(a_j)}{j-i} < ord_p(\alpha) \\ \Rightarrow \quad & ord_p(a_i) - ord(a_j) < (j-i)ord_p(\alpha) \\ \Rightarrow \quad & ord_p(a_i) + (i)ord(\alpha) < ord_p(a_j) + (j)ord_p(\alpha) \\ \Rightarrow \quad & ord_p(a_i\alpha^i t^i) < ord_p(a_j\alpha^j t^j) \end{aligned}$$

Assume that for $i < k$,

$$ord_p(a_k) \geq ord_p(a_j) + m_{i,j}(k-j),$$

and for $l < i$,

$$ord_p(a_l) \geq ord_p(a_i) + m_{i,j}(l-i).$$

Put $\alpha = p^{-m_{i,j}}$. We wish to show that there exists an $x = \alpha t$, where $|t|_p = 1$, such that $f(x) = 0$.

Note that

$$\frac{f(\alpha t)}{a_j \alpha}$$

is distinguished in t of degree j. Therefore, by the Weierstrass Preparation Theorem,

$$\frac{f(\alpha t)}{a_j \alpha} = g_0(t)g_1(t)h(t),$$

where $g_1(t) \in \mathbb{Z}_p[t]$ is a monic polynomial of degree $j-i$, with $|g(0)| = 1$, $h(t) \in \mathbb{Z}_p[t]$ is a polynomial of the form $c + h_1(t)$, where $|c| = 1$ and $h_0(t)$ is a polynomial whose

every coefficient has absolute value less than 1, and $g_0(t)$ is a monic polynomial of degree i, such that $|g(x)| < 1$ whenever $|x| < 1$.

It follows that all the zeros of $g_1(t)$ in $\mathbb{C}_p$ (of which there are $j - i$, counting multiplicity) are of absolute value 1. Thus, the original polynomial $f(x)$ has $j - i$ zeros of absolute value equal to the absolute value of α. □

Use it for good!

References:

Gouvêya, F. Q. *p-adic Numbers: An Introduction. - 2. ed.* Springer Verlag, Berlin, Heidelberg, New York, 1991.

Munkres, J. R. *Topology. - 2. ed.* Prentice-Hall, Upper Saddle River, New Jersey, 2000.

Artin, M. *Algebra.* Prentice-Hall, Upper Saddle River, New Jersey, 1991.

Strayer, J. K. *Elementary Number Theory.* Waveland Press, Long Grove Illinois, 1994.