THE P-ADICS, HENSEL'S LEMMA, AND NEWTON POLYGONS

JULIAN MAROHNIC

Abstract. This paper aims to develop the theory of p-adic integers and their basic algebraic and topological properties. It introduces the field of p-adic numbers and the p-adic completion of the rationals, though this is not the main focus of the paper and some proofs are omitted in the interest of brevity. Hensel's lemma concerning roots of polynomials over $\mathbb{Z}_p$ is introduced along with limits, concluding with a discussion of Newton polygons. This paper assumes a basic knowledge of analysis, abstract algebra, and Galois theory, though many of the most important definitions are nonetheless provided.

Contents

Date: DEADLINES: Draft AUGUST 19 and Final version AUGUST 30, 2013.

1. The p-adic Integers

Definition 1.0.1. Let p be a fixed prime number. A p-adic integer is defined as a series of the form:

$$\sum_{i=0}^{\infty} a_i p^i = a_0 + a_1 p + a_2 p^2 + \cdots$$

where each coefficient is an integer with $0 \leq a_i \leq p-1$.

We denote the set of p-adic integers $\mathbb{Z}_p$. Just as we would express a natural number in alternative base, we can express any natural number in base p as a p-adic integer with finitely many non-zero coefficients. Note that $\mathbb{Z}_p$ is uncountable. Suppose we express the natural numbers as a sequence of p-adic integers:

$$1 = \sum_{i \geq 0} a_i p^i, \quad 2 = \sum_{i \geq 0} b_i p^i, \cdots .$$

Here $a_0 = 1$ and $a_i = 0$ for all $i \geq 1$, and similarly for all other natural numbers. Now, we can construct a new p-adic integer $x = \sum_{i \geq 0} x_i p^i$, letting

$$x_0 \neq a_0, \;\; x_1 \neq b_1, \;\; \cdots$$

so that $x \neq n$ for all $n \in \mathbb{N}$, and thus $\mathbb{N} \subset \mathbb{Z}_p$.

1.1. **Addition in $\mathbb{Z}_p$.** For two p-adic integers, $a = \sum_{i \geq 0} a_i p^i$, $b = \sum_{i \geq 0} b_i p^i$, we define the sum $c = a + b$ as $c = \sum_{i \geq 0} c_i p^i$, where c_0 is defined as $a_0 + b_0$ if $a_0 + b_0 \leq p - 1$ and if not, we let $c_0 = a_0 + b_0 - p$ and add a "carry" term to the next coefficient, as we would when adding real numbers. We define each subsequent c_i similarly.

1.2. **Multiplication in $\mathbb{Z}_p$.** The product of two p-adic integers is defined as the product of their respective series expansions. As with addition, we carry when the product of two coefficients is greater than $p-1$ (following the same procedure that we use when multiplying real numbers).

2. What is $\mathbb{Z}_p$?

2.1. **$(\mathbb{Z}_p, +)$ is an Abelian Group.** In order to study further the properties of the p-adic integers, we want to know what sort of object $\mathbb{Z}_p$ is. By analogy with real numbers, it is clear that addition of p-adic integers is closed, associative, and commutative, and that the additive identity element is just the series with all coefficients equal to 0. What about additive inverses? Let's start with -1. We want to find a p-adic integer $a = \sum_{i \geq 0} a_i p^i$ such that $a + 1 = 0$. Keeping in mind the carry system, we see that if we let a be the series

$$a = \sum_{i \geq 0} (p-1) p^i = (p-1) + (p-1)p + (p-1)p^2 + \cdots$$

the first component of the sum will be $1 + (p-1) = p$. We carry and are left with 0. The next term is $0 + (p-1) + 1$ (once we add the carry term) which becomes zero once we carry again, and so on. The desired equality holds, and we see that $a = -1$. Now, if we have any p-adic integer $\alpha = \sum_{i \geq 0} \alpha_i p^i$, we can define an additive inverse:

$$\gamma = \sum_{i \geq 0} (p - 1 - \alpha_i) p^i$$

This number is well-defined as a p-adic integer since $0 \leq \alpha_i \leq p-1 \implies 0 \leq p-1-\alpha_i \leq p-1$. By the above argument, $\alpha + \gamma + 1 = 0$, so for any $\alpha \in \mathbb{Z}_p$ we have an additive inverse, specifically, $\gamma + 1$. Since the p-adic integers have additive inverses, $\mathbb{Z}_p$ together with addition form an abelian group. As a consequence, we see that we can now represent the negative integers as p-adic integers. In other words, $\mathbb{Z} \subset \mathbb{Z}_p$.

2.2. $(\mathbb{Z}_p, +, \cdot)$ **is a Ring.** As with addition, multiplication of p-adic integers is closed, commutative, and associative by analogy with multiplication of real numbers. The multiplicative identity is just $1 = 1 + 0 \cdot p + 0 \cdot p^2 + \cdots$, so $(\mathbb{Z}_p, +, \cdot)$ is a ring.

2.3. $(\mathbb{Z}_p, +, \cdot)$ **is an Integral Domain.** We already have a commutative ring, so we only need to show that there are no zero divisors in $\mathbb{Z}_p$

Proposition 2.3.1.

$$\textit{For all } a, b \in \mathbb{Z}_p \;\; a \cdot b = 0 \iff a = 0 \textit{ or } b = 0$$

Proof. Let $a = \sum_{i \geq 0} a_i p^i, b = \sum_{i \geq 0} b_i p^i \in \mathbb{Z}_p$ and suppose $a \cdot b = c = \sum_{i \geq 0} c_i p^i$. If a and b are both non-zero, they each have some non-zero coefficient, say a_n for a and b_m for b. By definition of p-adic multiplication, we will have:

$$c_{n+m} \equiv a_n b_m \bmod p.$$

Since p doesn't divide a_n or b_m it does not divide $a_n b_m \Rightarrow c_{n+m} \neq 0$, so $c \neq 0$ and thus

$$a \cdot b = 0 \iff a = 0 \text{ or } b = 0$$

□

Since $\mathbb{Z}_p$ is clearly not just $\{0\}$, $\mathbb{Z}_p$ must be an integral domain.

2.4. $(\mathbb{Z}_p, +, \cdot)$ **Is Not a Field.** We have shown that $\mathbb{Z}_p$ is an integral domain, so the question becomes, "Do the p-adic integers form a field?" Unfortunately, the answer is no. As it turns out, most nonzero p-adic integers, specifically, those whose first coefficient is equal to zero, fail to have inverses. Before we prove this fact, we need a new definition.

Definition 2.4.1. We define *reduction modulo* p as the map $\varepsilon \colon \mathbb{Z}_p \to \mathbb{Z}/p\mathbb{Z}$ given by

$$a = \sum_{i \geq 0} a_i p^i \mapsto a_0 \bmod p.$$

It can easily be shown that ε is a surjective ring homomorphism. Note that the kernel of this map is the set $\{\sum_{i \geq 0} a_i p^i \colon a_0 = 0\} = p\mathbb{Z}_p$.

Proposition 2.4.2. *A p-adic integer $a = \sum_{i \geq 0} a_i p^i$ is invertible if and only if $a_0 \neq 0$. In other words,*

$$\mathbb{Z}_p^\times = \left\{ a = \sum_{i \geq 0} a_i p^i \in \mathbb{Z}_p \colon a_0 \neq 0 \right\}.$$

Proof. Since ε is a homomorphism, we know that if a p-adic integer has an inverse, then its reduction mod p must also have an inverse. Since the kernel of the reduction mod p map is the set of p-adic integers with first coefficients equal to zero, we must have $\mathbb{Z}_p^\times \subset \{\sum_{i\geq 0} a_i p^i \colon a_0 \neq 0\}$. Now we need to show that the sets are equal. Clearly, given $a \in \mathbb{Z}_p$ with $a_0 \neq 0$, $\varepsilon(a)$ is nonzero and, since p is prime, has an inverse b_0 satisfying $0 < b_0 < p$ and $a_0 b_0 \equiv 1 \bmod p$. We can express this congruence as $a_0 b_0 = 1 + kp$. If we let $a = a_0 + p\alpha$, we will have

$$a \cdot b_0 = (a_0 + p\alpha)b_0 = a_0 b_0 + p\alpha b_0 = 1 + tp$$

for some $t \in \mathbb{Z}_p$. If we can show that $1 + tp$ is invertible, then we will have an inverse for a, since we can write

$$a \cdot b_0(1+tp)^{-1} = 1, \;\; a^{-1} = b_0(1+tp)^{-1}.$$

We have shown that if we can find an inverse for p-adic integers of the form $a = 1 + tp$, then we can find an inverse for any p-adic integer whose first coefficient is nonzero. But we can always let

$$(1+tp)^{-1} = 1 - tp + (tp)^2 - \cdots = 1 + c_1 p + c_2 p^2 + \cdots,$$

ensuring that all coefficients c_i satisfy $0 \leq c_i \leq p-1$. Now that we have found an inverse for $1 + pt$, we have an inverse for any p-adic integer with a nonzero first coefficient, and we have proved the equality. □

Of course, most p-adic integers are of the form $p\alpha$, where $\alpha \in \mathbb{Z}_p$, so invertibility is actually a very special trait among the p-adic integers, and thus $\mathbb{Z}_p$ is not a field. However, there is another important property that the p-adic integers *do* have, which we will use later, but will not prove.

Proposition 2.4.3. *$\mathbb{Z}_p$ is a compact topological space.*

Now that we have seen that $\mathbb{Z}_p$ is not a field, we might wonder how to make it into one. Considering the analogy with the set of regular integers $\mathbb{Z}$, a natural way to approach the problem would be to use the *quotient field* of the p-adic integers.

Definition 2.4.4. Let R be an integral domain. We define the *field of fractions*, or *quotient field*, of R as the set

$$\left\{ \frac{a}{b} \colon a, b \in R, \;\; b \neq 0 \right\},$$

which we denote $\mathrm{Frac}(R)$. Given a/b and c/d in $\mathrm{Frac}(R)$, we define the sum and product:

(1) $\dfrac{a}{b} + \dfrac{c}{d} = \dfrac{ad + cb}{bd}$

(2) $\dfrac{a}{b} \cdot \dfrac{c}{d} = \dfrac{ac}{bd}$

It is easy enough to show that $\mathrm{Frac}(R)$ is always a field, and a very familiar example is the quotient field of the integers. In fact, by the definition of "normal fractions," we have $\mathrm{Frac}(\mathbb{Z}) = \mathbb{Q}$. The rules for "canceling," finding multiplicative inverses, and such that hold in $\mathbb{Q}$ hold in any quotient field. Just as we can build the rational numbers with the integers, we can construct a field of fractions using the p-adic integers. However, before we do this there are some essential preliminaries that we will have to address.

3. Valuations, the p-adic Absolute Value, and $\mathbb{Q}_p$, the Field of p-adic Numbers

3.1. **Valuations.** In order to continue our discussion of the p-adics, we will introduce a new absolute value function, but we will start by defining it on the rationals, and extend it to the p-adics later. Before we can do this, we need to introduce the idea of a *valuation*, with which the reader may not be familiar. Now we introduce the symbol ∞, along with the conventions $\infty + \infty = \infty$ and $a + \infty = \infty + a = \infty$ for all $a \in \mathbb{Z}_p$.

Definition 3.1.1. We define a valuation on a space K as a map $v\colon K \to \mathbb{R} \cup \{\infty\}$ satisfying the following properties for all $x, y \in K$:

(1) $v(x) = \infty \iff x = 0$
(2) $v(xy) = v(x) + v(y)$
(3) $v(x + y) \geq min\{v(x), v(y)\}$

Proposition 3.1.2. *The following hold for all valuations v.*

(1) $v(1) = 0$ *for any valuation v.*
(2) $v(x) \neq v(y) \implies v(x + y) = min\{v(x), v(y)\}$

Proof. Easy. □

Definition 3.1.3. First, note that any $x \in \mathbb{Q}$ can be written as

$$x = p^k \frac{a}{b}, \ ,$$

where p is a prime, $k, a, b \in \mathbb{Z}$, and $(p, a, b) = 1$. Let $x = p^k(a/b) \in \mathbb{Q}$. We define the p-adic valuation as $v(x) = k$, or the greatest power of p that divides x. The p-adic valuation of a number is also referred to as its *order*.

Proposition 3.1.4. *The map we have defined as the p-adic valuation satisfies the conditions requisite for a valuation.*

Proof. Easy. □

3.2. **The p-adic Norm.** Now that we have defined the p-adic valuation, we can define a p-adic norm and corresponding metric, giving us an alternate way to compare the sizes of rational numbers (instead of the usual absolute value) and, eventually, p-adic numbers.

Definition 3.2.1. If x is some rational number we define the p-adic norm $|\cdot|_p\colon \mathbb{Q} \to \mathbb{R}$ as

$$|x|_p = \begin{cases} p^{-v(x)} & , \ x \neq 0 \\ 0 & , \ x = 0 \end{cases} .$$

This definition of absolute value gives us a corresponding metric, or a way to measure the distance between two rational numbers x and y: $d_p(x, y) = |x - y|_p$.

Proposition 3.2.2. *Let $x, y \in \mathbb{Q}$. The p-adic absolute value satisfies the following properties*

(1) $|xy|_p = |x|_p \cdot |y|_p$
(2) $|x + y|_p \leq max\{|x|_p, |y|_p\} \leq |x|_p + |y|_p$
(3) $|x|_p = 0 \iff x = 0$

Proof. Left to the reader. □

Notice that the second property tells us that the p-adic absolute value satisfies an inequality stronger than the usual triangle inequality. Norms satisfying this inequality are called *non-archimedean* or *ultrametric*. It turns out that non-archimedean metric spaces have some truly fascinating properties, but we will not have time to discuss them in depth here.

We know that $\mathbb{Q}$ is not complete with respect to the usual absolute value, and so we introduce $\mathbb{R}$ as its completion. However, we now have an entirely new absolute value function, and an entirely new set of Cauchy sequences. For example, the sequence

$$1,\ p,\ p^2,\ p^3,\ \cdots$$

is Cauchy with respect to the p-adic metric, and it can easily be shown that this sequences converges to zero. However, consider the sequence

$$p,\ p+p^2,\ p+p^2+p^3,\ \cdots.$$

Clearly, this is also a Cauchy sequence, though it certainly does not converge to anything in $\mathbb{Q}$. In fact, it converges to the series $\sum_{i\geq 0} p^i$, which we know as a p-adic integer. This "convergence" of course suggests a solution to our problem and a way to complete $\mathbb{Q}$ with respect to the p-adic metic. However, we will certainly need something more than the p-adic integers, since we have already seen that $\mathbb{Z}_p$ is not a field.

3.3. The p-adic Numbers.

Definition 3.3.1. We define the field of p-adic *numbers* to be the set $\mathbb{Q}_p = \mathrm{Frac}(\mathbb{Z}_p)$ along with the operations $+$ and $\cdot$ as they were defined for a general quotient field.

Note that $\mathbb{Z}_p$ is a subset of $\mathbb{Q}_p$, and since $\mathbb{Z} \subset \mathbb{Z}_p$, we get that $\mathbb{Q} \subset \mathbb{Q}_p$. We might hope that there is some simple relationship between the p-adic *numbers* and the series expansions that we used for the p-adic integers, and as it turns out, there is.

Proposition 3.3.2. *Any $x \in \mathbb{Q}_p$ can be represented as a series of the form*

$$\sum_{i=m}^{\infty} a_i p^i = a_m p^m + a_{m+1}p^{m+1} + \cdots + a_0 + a_1 p + \cdots,$$

where m is an integer and we have integral coefficients $a_i \in [0, p-1]$.

Proof. We are trying to prove the equality

$$\left\{ \sum_{i\geq m} a_i p^i \colon m, a_i \in \mathbb{Z},\ \ 0 \leq a_i \leq p-1 \right\} = \mathrm{Frac}(\mathbb{Z}_p).$$

Suppose we have a series of the above form, and more specifically, one for which $m < 0$ (i.e., not a p-adic integer). Then we can rewrite the series as a sum of several terms:

$$\begin{aligned} &a_m p^m + a_{m+1}p^{m+1} + \cdots + a_0 + a_1 p + \cdots \\ &= a_m \frac{1}{p^{-m}} + a_{m+1}\frac{1}{p^{-(m+1)}} + \cdots + \sum_{i\geq 0} a_i p^i, \end{aligned}$$

where each $a_i \in \mathbb{Z}$ and $p^{-m} \in \mathbb{Z}_p$ since $m < 0$. It follows that every term of the sum that is *not* part of the infinite series term is of the form a/b where $a, b \in \mathbb{Z}_p$, and

the infinite series is just a p-adic integer which is of the form $a/1$, where $a \in \mathbb{Z}_p$. Now we just have a sum of elements of $\mathrm{Frac}(\mathbb{Z}_p)$, and of course if the first index m is greater than or equal to zero, then the series will just be that of a p-adic integer, which is also an element of $\mathrm{Frac}(\mathbb{Z}_p)$, so we see that $\{\sum_{i\geq m} a_i p^i \colon m, a_i \in \mathbb{Z},\ 0 \leq a_i \leq p-1\} \subset \mathrm{Frac}(\mathbb{Z}_p)$. Note that given a p-adic integer of order k, we can always decompose it into the form $p^k u$, where $u \in \mathbb{Z}_p^\times$. Given any $a/b \in \mathrm{Frac}(\mathbb{Z}_p)$ with $v(a) = n$ and $v(b) = k$, we can express the quotient as

$$\frac{a}{b} = ab^{-1} = cp^n(dp^k)^{-1} = (cd)p^{n-k}.$$

Since c and d are p-adic units, $v(cd) = v(c)+v(d) = 0$ and the product $cd \cdot p^{n-k}$ will be a series of the form $\sum_{i\geq n-k} a_i p^i$, which is identical to the series representation of the p-adic unit cd with coefficients "shifted" so that the series starts with index $n-k$. If we have $n < k$, then the series will start with negative indices and negative powers of p, and thus $\{\sum_{i\geq m} a_i p^i \colon m, a_i \in \mathbb{Z},\ 0 \leq a_i \leq p-1\} \supset \mathrm{Frac}(\mathbb{Z}_p)$. □

Now we can extend our definitions of the p-adic valuation and norm to $\mathbb{Q}_p$. Since the p-adic valuation of a rational number x is equal to the highest power of p that divides x, it follows that the p-adic valuation $v(a)$ for some $a \in \mathbb{Q}_p$ is just the power of p corresponding to the first nonzero coefficient in the series expansion. This number is also referred to as the *order* of a. We will now proceed to show that $\mathbb{Q}_p$ is a completion of $\mathbb{Q}$ with respect to the metric $|\cdot|_p$.

Proposition 3.3.3. *$\mathbb{Q}_p$ is complete with respect to $|\cdot|_p$.*

Proof. Suppose we have a Cauchy sequence $(x_n) \in \mathbb{Q}_p$. In other words, given $\epsilon > 0$, we can make $|x_i - x_j| < \epsilon$ by making i and j large enough. But that means that we can make the p-adic order of the difference between two terms of the sequence as large as we want. To make this idea more explicit, let $\epsilon = 1/p^k$. Then since (x_n) is Cauchy, we can ensure that $v(x_i - x_j) > k$. But this means that the first k terms of x_i and x_j are the same, and clearly, that is the same as making the terms of the sequence arbitrarily close to some p-adic number. Thus any sequence in $\mathbb{Q}_p$ that is Cauchy with respect to the p-adic metric will converge, and $\mathbb{Q}_p$ is complete. □

Of course, it only remains to show that $\mathbb{Q}$ is dense in $\mathbb{Q}_p$, and the proof of this fact will be left to the reader. It can also be shown (Ostrowski's theorem) that the p-adic absolute value (for all primes p) and the regular absolute value are the only nontrivial absolute values that can be defined on $\mathbb{Q}$.

4. Limits

Now that we have introduced the p-adic numbers, we will leave them behind for a time and focus on just the p-adic integers, though we will return to $\mathbb{Q}_p$ in the section on polynomials. The definition of p-adic integers given above in terms of infinite series is only one possible definition, and, as it turns out, of limited utility. We can completely reformulate our definition of the p-adic integers using *projective limits*, which will be referred to as simply "limits," but once again we will have to introduce several other new definitions before we can get to the central idea of this section.

Definition 4.0.1. Let x be some p-adic integer, $x = \sum_{i\geq 0} a_i p^i$. We define reduction modulo p^n as we defined reduction mod p:

$$\varepsilon_n(x) = \sum_{i<n} a_i p^i \bmod p^n.$$

Since $\varepsilon_n(x) \in \mathbb{Z}/p^n\mathbb{Z}$, we have a mapping $\varepsilon_n \colon \mathbb{Z}_p \to \mathbb{Z}/p^n\mathbb{Z}$, and using arithmetic in $\mathbb{Z}_p$, we see that this is actually a homomorphism.

Now, $\varepsilon_n(x)$ approaches x as n tends to infinity, and likewise we can see that in some sense the quotient rings $\mathbb{Z}/p^n\mathbb{Z}$ approach $\mathbb{Z}_p$.

Definition 4.0.2. We define a sequence (E_n, φ_n) of sets E_n and maps $\varphi_n \colon E_{n+1} \to E_n$ $(n \geq 0)$ as a *projective system*. We define the set E along with maps $\psi_n \colon E \to E_n$ as the *limit* of the projective system (E_n, φ_n) if: For each set X and maps $f_n \colon X \to E_n$ such that $f_n = \varphi_n \circ f_{n+1}$ there exists a unique factorization f of f_n through the set E:

$$f_n = \psi_n \circ f \colon X \to E \to E_n \ \ (n \geq 0)$$

Proposition 4.0.3. *For every projective system (E_n, φ_n) there exists a limit*

$$E = \varprojlim E_n = \{(x_n) \colon \varphi_n(x_{n+1}) = x_n \ \ \forall n \geq 0\} \subset \prod_{n\geq 0} E_n$$

together with maps $\psi_n \colon E \to E_n$. If (E', ψ_n') is a limit of the same sequence, then there exists a unique *bijection $f \colon E' \to E$ such that $\psi_n' = \psi_n \circ f$.*

Proof. Omitted. □

Proposition 4.0.4. *A limit of nonempty compact spaces is nonempty and compact.*

Proof. By Tychonoff's theorem, the product of any collection of compact topological spaces is compact. If we have a projective system (E_n, φ_n), where each E_n is compact, then their product will be compact as well, and by definition, we have $E = \varprojlim E_n \subset \prod_{n\geq 0} E_n$, so the limit must also be compact. The proof that the limit is nonempty is left to the reader. □

Proposition 4.0.5. *If we have a commutative ring A together with a sequence of decreasing ideals I_n in A which form a projective system $(A/I_n, \varphi_n)$ of quotient rings and maps $\varphi_n \colon A/I_{n+1} \to A/I_n$ then the limit $\widehat{A} = \varprojlim A/I_n$ is a topological ring with continuous homomorphisms $\psi_n \colon \widehat{A} \to A/I_n$.*

Proof. Omitted. □

4.1. **Limits and the p-adic Integers.** We can now make use of the idea of limits to formalize our thoughts about the quotient rings $\mathbb{Z}/p^n\mathbb{Z}$ converging to $\mathbb{Z}_p$. To apply (4.0.5) to the p-adic integers, we need a decreasing sequence of ideals, which we already have, since $p^{n+1}\mathbb{Z} \subset p^n\mathbb{Z}$. Moreover, $\mathbb{Z}$ is clearly a commutative ring. We now have a projective system $(\mathbb{Z}/p^n\mathbb{Z}, \varphi_n)$, with maps $\varphi_n \colon \mathbb{Z}/p^{n+1}\mathbb{Z} \to \mathbb{Z}/p^n\mathbb{Z}$.

Theorem 4.1.1. *The mapping $\mathbb{Z}_p \to \varprojlim \mathbb{Z}/p^n\mathbb{Z}$ that maps the p-adic integer $x = \sum_{i\geq 0} a_i p^i$ to the sequence (x_n) of sums $x_n = \sum_{i<n} a_i p^i \bmod p^n$ is an isomorphism.*

Proof. Referring to (4.0.3) we see that the limit of a projective system is the set of sequences $(x_n) \in \prod \mathbb{Z}/p^n\mathbb{Z}$ that satisfy $\varphi_n(x_{n+1}) = x_n$. In this case, the map $\varphi\colon \mathbb{Z}_p \to \mathbb{Z}/p^n\mathbb{Z}$ is given by:

$$\sum_{i<n+1} a_i p^i \bmod p^{n+1} \mapsto \sum_{i<n} a_i p^i \bmod p^n.$$

Thus the sequences (x_n) that we are looking for are just p-adic integers reduced mod p^n, in other words, the partial sums of the series $\sum_{i\geq 0} a_i p^i$. We still need to show that we have an isomorphism. Given some p-adic integer $x = \sum_{i\geq 0} a_i p^i \in \mathbb{Z}_p$, the obvious choice is to map x to the corresponding sequence $(x_n) \in \varprojlim \mathbb{Z}/p^n\mathbb{Z}$. Thus we have a map $f\colon \mathbb{Z}_p \to \mathbb{Z}/p^n\mathbb{Z}$:

$$x_1 = a_0, \;\; x_2 = a_0 + a_1 p, \;\; x_3 = a_0 + a_1 p + a_2 p^2$$

as well as a map $g\colon \mathbb{Z}/p^n\mathbb{Z} \to \mathbb{Z}_p$:

$$a_0 = x_1, \;\; a_2 = \frac{x_2 - x_1}{p}, \;\; a_3 = \frac{x_3 - x2}{p^2}, \;\; \cdots.$$

We see that we have a continuous bijection between two rings, so we have an isomorphism of topological rings. □

5. Polynomials in $\mathbb{Z}_p$ and $\mathbb{Q}_p$

We have begun to explore the relationship between $\mathbb{Z}_p$ and $\mathbb{Z}/p^n\mathbb{Z}$. Now we will consider the relationship between polynomials and their solutions over these rings, and we will see how a solution in $\mathbb{Z}/p^n\mathbb{Z}$ is an "approximate" solution to the same polynomial over $\mathbb{Z}_p$. Once we have spent some time studying polynomials over $\mathbb{Z}_p$, we will move on to polynomials over all of the p-adic numbers.

Proposition 5.0.1. *Let $P(X, Y) \in \mathbb{Z}[X, Y]$ be a polynomial in two variables with integral coefficients. The equation $P = 0$ has a solution in $\mathbb{Z}_p$ if and only if for all $n \geq 0$, $P = 0$ has a solution in $\mathbb{Z}/p^n\mathbb{Z}$.*

Proof. First, note that when we say that $P(X, Y) = 0$ has a solution in some ring A, we mean that there exists some pair $(x, y) \in A \times A$ such that $P(x, y) = 0$. Suppose that we have a solution for $P = 0$ in $\mathbb{Z}_p$. Then there exists some $x = \sum_{i\geq 0} a_i p^i$, $y = \sum_{i\geq 0} b_i p^i \in \mathbb{Z}_p$ such that $P(x, y) = 0$. But if we define $x_n = \sum_{i<n} a_i p^i \bmod p^n$ and y_n similarly, we see that $P(x_n, y_n) = P(x, y) \bmod p^n$. So if we have a solution in $\mathbb{Z}_p$, we have a solution in $\mathbb{Z}/p^n\mathbb{Z}$.

Now, suppose we have a solution in $\mathbb{Z}/p^n\mathbb{Z}$. We can always construct a solution in $\mathbb{Z}/p^{n+1}\mathbb{Z}$, so we can construct a sequence of finite sets

$$X_n = \{(x, y) \in \mathbb{Z}/p^n\mathbb{Z} \times \mathbb{Z}/p^n\mathbb{Z}\colon P(x, y) = 0\}$$

along with maps $\varphi\colon X_{n+1} \to X_n$ given by:

$$\left(\sum_{i\leq n} a_i p^i, \;\; \sum_{i\leq n} b_i p^i\right) \mapsto \left(\sum_{i<n} a_i p^i \bmod p^n, \;\; \sum_{i<n} b_i p^i \bmod p^n\right).$$

We have a sequence of sets and maps (X_n, φ_n), which must therefore have a limit $X = \varprojlim X_n \subset \mathbb{Z}_p \times \mathbb{Z}_p$. Since the limit of nonempty finite sets in nonempty, we will have solutions for $P = 0$ in $\mathbb{Z}_p$. □

There is one more fact that we will need to make use of later on.

Proposition 5.0.2. *Let $P(X)$ be a polynomial over some ring A. Then there exist polynomials $P_1(X,Y)$ and $P_2(X,Y)$, also over A, such that*

$$P(X+h) = P(X) + h \cdot P_1(X,h) = P(X) + h \cdot P'(X) + h^2 \cdot P_2(X,h).$$

Proof. We will need to express the polynomial $P(X)$ as a series with coefficients a_n and a finite number of terms: $P(X) = \sum a_n X^n$. Now we have

$$P(X+h) = \sum a_n (X+h)^n.$$

Using the binomial theorem, we get

$$\begin{aligned} P(X+h) &= \sum a_n (X^n + nX^{n-1}h + h^2(\cdots)) \\ &= \sum X^n a_n + h \cdot \sum n a_n X^{n-1} + h^2 \cdot P_2(X,h) \\ &= P(X) + h \cdot P'(X) + h^2 \cdot P_2(X,h) \end{aligned}$$

□

5.1. **The Newtonian Algorithm.** As mentioned earlier, a solution x to the polynomial $P \in \mathbb{Z}/p^n\mathbb{Z}[X]$ is also an approximate solution for the same polynomial over $\mathbb{Z}_p$, since we will still have $P(x) \equiv 0 \bmod p^n$. Now we want to be able to improve our solution. In other words, we want to be able to construct some new number x' such that $P(x') \equiv 0 \bmod p^{n+1}$.

Suppose we have some polynomial $P \in \mathbb{Z}[X]$ and some $x \in \mathbb{Z}$ such that $P(x) \equiv 0 \bmod p$. Since we only care that x is a solution modulo p, we can assume without loss of generality that x is some integer a_0 that satisfies $0 \leq a_0 \leq p-1$. As before, we want to construct some integer $\hat{x}$ such that $P(\hat{x}) \equiv 0 \bmod p^2$. Since we are looking for solutions modulo p^2, we can express $\hat{x}$ as some integer $\hat{x} = a_0 + a_1 p$ (again, $0 \leq a_1 \leq p-1$). Now, we must have $P(\hat{x}) \equiv 0 \bmod p^2$. Here we can apply (5.0.2):

$$P(\hat{x}) = P(a_0 + a_1 p) = P(a_0) + a_1 p \cdot P'(a_0) + (a_1 p)^2 \cdot b$$

where b is some integer. Since $P(x) \equiv 0 \bmod p$, we can write $P(a_0) = P(x) = pt$ for some $t \in \mathbb{Z}$, so now we have:

$$P(\hat{x}) \equiv 0 \bmod p^2 \iff pt + a_1 p \cdot P'(a_0) \equiv 0 \bmod p^2$$

Dividing through by p, we see that the congruence relation holds if $t + a_1 P'(a_0) \equiv 0 \bmod p$. Assuming $P'(a_0) \not\equiv 0 \bmod p$, we can let $a_1 \equiv -t/P'(a_0) \bmod p$, which gives us

$$\hat{x} = a_0 + a_1 p = a_0 - \frac{pt}{P'(a_0)} = x - \frac{P(x)}{P'(x)} = N_p(x)$$

which satisfies $P(\hat{x}) \equiv 0 \bmod p^2$. This formula may look familiar: it is the same as Newton's formula for approximating the roots of a real function.

Proposition 5.1.1. *Let $P \in \mathbb{Z}_p[X]$ and $x \in \mathbb{Z}_p$ be such that $P(x) \equiv 0 \bmod p^n$. If $v(P'(x)) = k < n/2$, we can use Newton's algorithm to construct $\hat{x} = N_p(x) = x - P(x)/P'(x)$. We claim that $\hat{x}$ satisfies*

(1) $P(\hat{x}) \equiv 0 \bmod p^{n+1}$
(2) $\hat{x} \equiv x \bmod p^{n-k}$
(3) $v(P'(\hat{x})) = v(P'(x))$

Proof. First we show that $\hat{x} \equiv x \bmod p^{n-k}$. Since $P(x) \equiv 0 \bmod p^n$ we know that $P(x)$ is of order n, so we can let $P(x) = p^n y$ for some $y \in \mathbb{Z}_p^\times$, and likewise we let $P'(x) = p^k u$, where $u \in \mathbb{Z}_p^\times$. This is always possible if $P'(x) \neq 0$ because we know that $P'(x)$ is of order k. Substituting into Newton's algorithm and subtracting x, we get

$$\hat{x} - x = -\frac{P(x)}{P'(x)} = -p^{n-k} y u^{-1} \in p^{n-k}\mathbb{Z}_p.$$

Here we see when $P'(x)$ is of a small order, we get a "better" congruence relation. In other words, when the order of the derivative at x is small, x is very close to $\hat{x}$. This is reminiscent of Newton's approximation method for real functions. When a p-adic number is of a larger order, it is small, by the p-adic metric we defined earlier, and as a consequence the root obtained by the Newton algorithm is not very close to it: it is only congruent modulo p^{n-k}. Likewise, with real functions, when the derivative small, the root obtained using Newton's method can be quite far away. Now, we want to show that $P(\hat{x}) \equiv 0 \bmod p^{n+1}$. Here we use a Taylor expansion in $\hat{x}$ at the point x.

$$P(\hat{x}) = P(x) + (\hat{x} - x)P'(x) + (\hat{x} - x)^2 \cdot t$$

$$= P(x) - \frac{P(x)}{P'(x)} P'(x) + (\hat{x} - x)^2 \cdot t = (\hat{x} - x)^2 \cdot t$$

where t is some p-adic integer, since $P \in \mathbb{Z}_p[X]$. This gives us

$$P(\hat{x}) = (\hat{x} - x)^2 \in p^{2n-2k}\mathbb{Z}_p = p^n \cdot p^{n-2k}\mathbb{Z}_p$$

By our assumption that $k < n/2$, we get that $n - 2k \geq 1$, so $p^n \cdot p^{n-2k} \geq p^{n+1}$ and thus $P(\hat{x}) \in p^{n+1}\mathbb{Z}_p$, so $P(\hat{x}) \equiv 0 \bmod p^{n+1}$. Finally, we need to show that $v(P'(\hat{x})) = v(P'(x)) = k$. We will once again consider a Taylor expansion, this time of $P'(\hat{x})$ at the point x:

$$P'(\hat{x}) = P'(x + (\hat{x} - x)) = P'(x) + (\hat{x} - x) \cdot s$$

$$= p^k u + p^{n-k} z = p^k (u + p^{n-2k} z)$$

where $z = -su^{-1}y$. We will once again use the condition that $n - 2k > 0$, so $n - 2k \geq 1$, as well as the fact that $u \in \mathbb{Z}_p^\times$, to get:

$$u + p^{n-2k} z \in u + p\mathbb{Z}_p \subset \mathbb{Z}_p^\times \implies p^k(u + p^{n-2k} z) \in p^k\mathbb{Z}_p \implies v(P'(\hat{x})) = k$$

□

5.2. **Hensel's Lemma.** Using the Newtonian algorithm, we can take a solution x to $P \bmod p^n$ and construct $\hat{x}$ satisfying $P(\hat{x}) \equiv 0 \bmod p^{n+1}$. However, we want to be able to produce a true solution ξ to $P(X) \in \mathbb{Z}_p$ such that $P(\xi) = 0$.

Theorem 5.2.1 (Hensel's Lemma)**.** *Suppose we have a polynomial $P(X) \in \mathbb{Z}_p[X]$ and $x \in \mathbb{Z}_p$ satisfying $P(x) \equiv 0 \bmod p^n$ and $k = v(P'(x)) < n/2$. Then P has a unique root $\xi \in \mathbb{Z}_p$ with $\xi \equiv x \bmod p^{n-k}$ and $v(P'(\xi)) = v(P'(x)) = k$.*

Proof. First we need to show that such a root exists. Given such an x, which we will rename x_0, we can use the Newtonian algorithm described in (5.1.1) to generate a p-adic integer x_1 that satisfies $P(x_1) \equiv 0 \bmod p^{n+1}$, $x_1 \equiv x_0 \bmod p^{n-k}$, and $v(P'(x_1)) = v(P'(x_0)) = k$. We can continue this process indefinitely, generating an infinite sequence (x_m) of p-adic integers satisfying

$$P(x_0) \equiv 0 \bmod p^n$$
$$P(x_1) \equiv 0 \bmod p^{n+1}$$
$$P(x_2) \equiv 0 \bmod p^{n+2}$$
$$\vdots$$

as well as

$$x_1 \equiv x_0 \bmod p^{n-k}$$
$$x_2 \equiv x_1 \bmod p^{n-k+1}$$
$$\vdots$$

and finally, we have $v(P(x_m)) = v(P(x_0)) = k$ for all m. Note that this sequence is Cauchy with respect to the p-adic metric that we defined earlier. Let x_i and x_j be terms in the sequence and, without loss of generality, let $i < j$. Then we have

$$x_i \equiv x_j \bmod p^{n-k+i} \implies |x_i - x_j|_p \leq \frac{1}{p^{n-k+i}},$$

so by taking i sufficiently large, we can make the difference arbitrarily small, and we have a Cauchy sequence. Since $\mathbb{Z}_p$ is compact, the sequence converges to some limit $\xi \in \mathbb{Z}_p$ with $P(\xi) = 0$.

It remains to show that the root ξ is unique in $\mathbb{Z}_p$. Suppose that for a given x satisfying $P(x) \equiv 0 \bmod p^n$ as well as the other conditions given in the hypothesis, the polynomial had two roots in $\mathbb{Z}_p$, say ξ and η. We will certainly have

$$\xi \equiv \eta \bmod p^{n-k}.$$

Since $n > 2k$, we have that $n - k \geq k + 1$ because n and k are integers, so it is also true that

$$\xi \equiv \eta \bmod p^{k+1}.$$

Here will use a Taylor expansion of P in η at ξ:

$$P(\eta) = P(\xi) + P'(\xi)(\eta - \xi) + (\eta - \xi)^2 a.$$

But by definition $P(\eta) = P(\xi) = 0$, so we have

$$(\eta - \xi)\Big(P'(\xi) + (\eta - \xi)a\Big) = 0.$$

Furthermore, $v(P'(\xi) = k$ and since $\eta \equiv \xi \bmod p^{n-k}$ we have $v(\eta - \xi) \geq n - k \geq k + 1$. This gives us $v((\eta - \xi)a) > v(P'(\xi))$. Now we have

$$P'(\xi) + (\eta - \xi)a \neq 0 \implies (\eta - \xi) = 0 \implies \eta = \xi$$

so the root not only exists, but is unique. □

It is worth noting that if a polynomial has multiple solutions mod p^n, then it may have multiple solutions in $\mathbb{Z}_p$. For example, we could consider which numbers have square roots in $\mathbb{Z}_p$.

5.3. **Square Roots in $\mathbb{Z}_p$.** Consider solutions to polynomials of the form $P(X) = X^2 - a$, with $P \in \mathbb{Z}_p[X]$. If for a given a we can find some x satisfying $P(x) \equiv 0 \bmod p^n$ (as well as the other conditions we imposed on x), then we will be able to find a solution to the polynomial in $\mathbb{Z}_p$ and thus a will have a square root in $\mathbb{Z}_p$. As an example, let us try to find the square root of 2 in $\mathbb{Z}_7$. Since we are trying to find a solution $x \in \mathbb{Z}_7$ to $x^2 - 2 = 0$, we can use Hensel's lemma, provided we can find a suitable solution modulo 7^n for some n. Now, we know that $3^2 = 9 \equiv 2 \bmod 7^1$. Note that $v(P'(3)) = 0 < 1/2$, so we can apply the Newtonian algorithm from Hensel's lemma, which gives us

$$N_7(3) = 3 - \frac{7}{6} = \frac{11}{6} \equiv 10 \bmod 7^2.$$

By (5.1.1), this should be a solution to P modulo 7^2: $P(10) = 98 \equiv 0 \bmod 7^2$, and by part (3) of (5.1.1), we can continue this process indefinitely. If we repeated it one more time, we would get

$$N_7(10) = 10 - \frac{98}{20} = \frac{51}{10} \equiv 108 \bmod 7^3.$$

As expected, $P(108) = 11602 \equiv 0 \bmod 7^3$. Continuing this process, we have a Cauchy sequence that converges to $\sqrt{2}$ in $\mathbb{Z}_p$. Furthermore, we can express $\sqrt{2}$ directly as a 7-adic integer by expressing the terms of the sequence in base 7:

$$3 = 3, \;\; 10 = 3 + 1 \cdot 7, \;\; 108 = 3 + 1 \cdot 7 + 2 \cdot 49, \;\; \cdots$$

so we see that the terms of the sequence are actually just giving us successive coefficients of the 7-adic representation of the square root of 2. In other words, $\ldots 213_7 = \sqrt{2}$. Notice that we could just as easily have started with 4, since $4^2 = 16 \equiv 2 \bmod 7$. Using the same procedure as we did before, we would obtain another, distinct square root in $\mathbb{Z}_p$. It is important to remember that the uniqueness condition in Hensel's lemma applies only when considering one "seed." A polynomial may certainly have multiple roots in $\mathbb{Z}_p$.

5.4. **Newton Polygons.** Hensel's lemma gives us a method for finding roots to a polynomial over $\mathbb{Z}_p$, and it is indeed a useful tool. However, we will now begin to expand our horizons and consider polynomials over all of $\mathbb{Q}_p$.

Definition 5.4.1. Given a set X of points in two dimensional Euclidean space, we define the convex hull as the minimal convex set containing X. The *lower* convex hull is simply the lower section of the convex hull bounded on the left by the point having the least x-value and on the right by the point having the greatest x-value.

Definition 5.4.2. Let $f(x) = a_0 + a_1x + \cdots + a_nx^n$ be a polynomial over $\mathbb{Q}_p$ such that $a_0a_n \neq 0$. Now we make pairs $(i, v(a_i)) \in \mathbb{R}^2$ for each term in the polynomial, which gives us the set

$$\{(1, v(a_1)), \;\; , (2, v(a_2)), \;\; \cdots , (n, v(a_n))\}$$

If we take the lower convex hull of this set of points, we will have a polygonal chain made of a sequence of line segments with increasing slopes. This is called the Newton Polygon of the polynomial $f(x)$.

Proposition 5.4.3. *Again, let $f(x) = a_0 + a_1x + \cdots + a_nx^n$ be a polynomial over $\mathbb{Q}_p$ such that $a_0a_n \neq 0$, and let w be an extension of the p-adic valuation to L, the splitting field of the polynomial f. If the line segment $(r, v(a_r)) \leftrightarrow (s, v(a_s))$ of slope*

$-m$ appears in the Newton polygon of f, then $f(x)$ has $s-r$ roots $(\alpha_1, \cdots, \alpha_{s-r})$ with valuations $w(\alpha_1) = w(\alpha_2) = \cdots = w(\alpha_{s-r}) = m$.

Proof. Since we are studying the Newton polygon of f, we can assume $a_n = 1$. If it is not, we can always divide through by a_n, which will only translate the polygon up or down. Now, we will number the roots of the polynomial as follows:

$$\begin{gathered} w(\alpha_1) = \cdots = w(\alpha_{s_1}) = m_1 \\ w(\alpha_{s_1+1}) = \cdots = w(\alpha_{s_2}) = m_2 \\ \vdots \\ w(\alpha_{s_t+1}) = \cdots = w(\alpha_n) = m_{t+1}. \end{gathered}$$

We split up the roots into groups which have the same valuation, so the roots of the given polynomial can take on any one of $t+1$ valuations. We also require that $m_1 < m_2 < \cdots < m_{t+1}$. The ith coefficient of any polynomial will be a function of its roots, and moreover, they follow a certain pattern. This is easy enough to see when we are dealing with a polynomial of a low degree. For example, consider an arbitrary third degree polynomial in its fully factored form:

$$(x-\alpha_1)(x-\alpha_2)(x-\alpha_3) = 0.$$

If we multiply the expression out fully, we obtain the standard form of the polynomial:

$$\begin{gathered} -(\alpha_1\alpha_2a_3) + (\alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3)x - (\alpha_1 + \alpha_2 + \alpha_3)x^2 + x^3 \\ = a_0 + a_1x + a_2x^2 + a_3x^3 \end{gathered}$$

There is an important pattern here. Notice that the constant term a_0 is a product of all three roots of the polynomial. a_1 is a sum of products of two roots, and so on. In an nth degree polynomial, the ith coefficient is always a sum of products of $n-i$ roots. Recalling the definition of a valuation, we can derive the following:

$$\begin{gathered} v(a_n) = v(1) = 0 \\ v(a_{n-1}) \geq \min_i\{w(\alpha_i)\} = m_1 \\ v(a_{n-2}) \geq \min_{i,j}\{w(\alpha_i\alpha_j)\} = 2m_1 \\ \vdots \\ v(a_{n-s_1}) = \min_{i_1,\cdots,i_{s_1}}\{w(\alpha_{i_1}\cdots\alpha_{i_{s_1}})\} = s_1m_1, \end{gathered}$$

making special note of the final equality, which comes from (3.1.2). Continuing this process, we have:

$$\begin{gathered} v(a_{n-s_1-1}) \geq \min_{i_1,\cdots,i_{s_1+1}}\{w(\alpha_{i_1}\cdots\alpha_{i_{s_1+1}})\} = s_1m_1 + m_2 \\ v(a_{n-s_1-2}) \geq \min_{i_1,\cdots,i_{s_1+2}}\{w(\alpha_{i_1}\cdots\alpha_{i_{s_1+2}})\} = s_1m_1 + 2m_2 \\ \vdots \\ v(a_{n-s_2}) = \min_{i_1,\cdots,i_{s_2}}\{w(\alpha_{i_1}\cdots\alpha_{i_{s_2}})\} = s_1m_1 + (s_2-s_1)m_2. \end{gathered}$$

We can continue this process until we have written out the valuations of all $n+1$ coefficients, and now that we know the valuations of all of the coefficients (or at least have lower bounds for them) we can say something about the Newton polygon of the

polynomial. Clearly, the rightmost vertex will be the point $(n, 0)$. Moving leftward, we have a set of $s_1 + 1$ points which all lie on or above a line with slope $-m_1$, so we know that the points $(n, 0)$ and $(n - s_1, v(n - s_1))$ will definitely be vertices in the polygon. Moving farther to the left, we encounter a new line segment of slope $-m_2$. Consider the $(j+1)$th line segment in the Newton polygon, punctuated on the right side by the point $(n-s_j, v(n-s_j)) = (n-s_j, s_1m_1+(s_2-s_1)m_2+\cdots+(s_j-s_{j-1})m_j)$. Its slope can be calculated quite easily:

$$\frac{(s_1m_1 + \cdots + (s_j - s_{j-1})m_j) - (s_1m_1 + \cdots + (s_{j+1} - s_j)m_{j+1})}{(n - s_j) - (n - s_{j+1})} = -m_{j+1},$$

so we see that the result holds for all faces of the polygon. Since $m_1 < m_2$, we know for sure that we will have a distinct line segment between $(n - s_1, v(n - s_1))$ and $(n - s_2, v(n - s_2))$ with $s_2 - s_1 + 1$ points lying on or above it, and this result can also be generalized to any line segment in the polygon. Furthermore, notice that because of the way we labelled our coefficients and roots we can easily see that for each ordered pair $(i, v(a_i))$ there is a root whose valuation is equal to minus the slope of the segment that contains (or lies beneath) the point, and hence the proposition. □

5.5. **Factoring Polynomials in $\mathbb{Q}_p$ with Newton Polygons.** We will now introduce one final result, concerning Newton polygons, to conclude our discussion of polynomials. We have shown how Newton polygons can be used to investigate the valuations of roots. They can also be used to investigate the way a polynomial factors over its field. As it turns out, given some polynomial over $\mathbb{Q}_p$, it's factorization in $\mathbb{Q}_p$ corresponds to the slopes of its Newton polygon.

Proposition 5.5.1. *Suppose $f(x)$ is a polynomial over $\mathbb{Q}_p$ whose Newton polygon has slopes $-m_r < \cdots < -m_1$. If the p-adic valuation v has a unique extension w to the splitting field L of f, then we have the factorization*

$$f(x) = a_n \prod_{j=1}^{r} f_j(x),$$

where each factor is an element of $\mathbb{Q}_p$ as follows:

$$f_j(x) = \prod_{w(\alpha_i)=m_j} (x - \alpha_i) \in \mathbb{Q}_p[x].$$

Proof. As in the previous proof, we can let $a_n = 1$. If $f(x)$ is irreducible, the proposition clearly holds. Given a root $\alpha_i \in L$ we have $\alpha_i = \sigma_i\alpha_1$ for some $\sigma_i \in G(L|K)$. Since the extension w to L is unique, and since $w \circ \sigma_i$ is another extension, we have $w(\alpha_i) = w(\sigma_i\alpha_1) = m_1$, so $f_1(x) = f(x)$ and thus the polygon has only one segment, corresponding to its one factor. We will now proceed to treat the general case by way of induction on the degree n of f. The case where $n = 1$ is trivial. Let $p(x)$ be the minimal polynomial of α_1 over $\mathbb{Q}_p$ and $g(x) = f(x)/p(x) \in \mathbb{Q}_p$. All of the roots of $p(x)$ will have valuation m_1, so by definition of $f_j(x)$, $p(x)$ divides $f_1(x)$. Let $g_1(x) = f_1(x)/p(x)$. Now we can factor $g(x)$ by its slopes as we did with $f(x)$:

$$g(x) = g_1(x) \prod_{j=2}^{r} f_j(x).$$

Now, by our definitions of $f_1(x)$ and $g_1(x)$, the degree of $g(x)$ is smaller than the degree of $f(x)$, and we have that $f_j(x) \in \mathbb{Q}_p$ for all $j \in 1, \cdots, r$. □

This gives us a powerful tool: we can now look at a Newton polygon for any given polynomial over $\mathbb{Q}_p$ and learn quite a bit about how it factors. In short, if its Newton polygon contains r line segments, it will factor into r pieces, which may or may not themselves be irreducible.

Acknowledgements. I would like to express my sincere gratitude toward my mentor, Daniel Johnstone, for guiding me in my research, having the patience to read and edit my paper, and, most important, helping to illuminate for me the mathematics that I was studying. I would also like to thank the University of Chicago, and especially the Department of Mathematics, for providing this opportunity for me to study and funding my research project. Finally, I would like to thank my family for supporting me in my academic endeavors, this summer and always.

References

[1] Jürgen Neukirch. Algebraische Zahlentheorie. Springer-Verlag, 1992.
[2] Alain Robert. A Course in p-adic Analysis. Springer-Verlag, 2000.
[3] David Dummit and Richard Foote. Abstract Algebra. John Wiley and Sons, Inc., 2004.
[4] Tom Aposotl. Introduction to Analytic Number Theory. Springer-Verlag, 1976.
[5] David Madore. A First Introduction to p-adic Numbers. http://www.madore.org/ david/math/padics.pdf
[6] F. Crivelli. Absolute Values, Valuations, and Completion. http://www.math.ethz.ch/education/bachelor/seminars/fs2008/algebra/Crivelli.pdf
[7] Paul Sally. Tools of the Trade. American Mathematical Society, 2008.