THE P-ADIC INTEGERS, ANALYTICALLY AND ALGEBRAICALLY

ARUSHI GUPTA

Abstract. This paper discusses the power series, analytic, and algebraic formulations of the p-adic integers and the consequences of each of these. The analytic and algebraic viewpoints suggest two different proofs that the group of units (for $p \neq 2$) is isomorphic to $\mathbb{Z}_p \times (\mathbb{Z}/p\mathbb{Z})^\times$. The paper concludes with further discussion of the algebraic perspective, including the exactness of completion.

Contents

1. An Introduction to p-adic Integers

p-adic numbers show up in seemingly unexpected places, including cryptography, string theory, and more. The p-adics allow us to better understand and locally approximate the integers. In particular, solving equations in the p-adics gives information about their corresponding equations in the integers; in fact, equations without solutions in the p-adic integers cannot have integer solutions. This concept is especially relevant in number theory, where the Hasse-Minkowski theorem says that quadratic forms are equivalent over $\mathbb{Q}$ if and only if they are equivalent in the p-adics for all primes p. The p-adics have applications in many areas of mathematics, from number theory and topology to mathematical physics, dynamics, and even geology. [4]

This paper discusses different constructions of the p-adic numbers and their consequences. We will study how the p-adics can be seen as a special case of formal power series, Cauchy completion, or the completion of a ring with respect to an

Date: August 26, 2018.

ideal. Through considering each of these methods, we gain more insight into the structure of the p-adics; here, we will see how each formulation helps us construct the group of units. Finally, we will see how the general theory developed for completions of rings with respect to ideals can provide insight on p-adic completion.

2. The Power Series Definition of the p-adic Integers

The most concrete way to think of p-adic integers is as formal power series with base p. This idea is motivated by the unique decomposition of positive integers as sums of powers of p. For example, if we take $p = 3$, we can write 10 as $1+0\cdot 3+1\cdot 3^2$. Taking $p = 2$, we have $10 = 0+1\cdot 2+0\cdot 2^2+1\cdot 2^3$. We can do this for any nonnegative integer and any prime, and this type of construction gives us an explicit definition of the p-adic integers as formal power series. We can also come up with a formal power series to represent any negative integer, but these have infinitely many terms, so they are harder to describe.

Definition 2.1. The p-adic integers are the set of formal power series

$$a_0 + a_1 p + a_2 p^2 + \ldots + a_n p^n + \ldots$$

where p is a prime and the a_i are integers from $\{0, 1, \ldots, p-1\}$.

This set of power series is actually a ring; as a set, it is bijective with $\mathbb{Z}/p\mathbb{Z}[x]$, but the ring structure is different. The disadvantage of this definition of the p-adic integers is that defining addition and multiplication explicitly is difficult. It is possible to do so, but because we must deal with "carrying" when a digit is greater than $p-1$, it involves more complicated constructions than, say, those for $\mathbb{Z}/p\mathbb{Z}[x]$.

For example, if $\alpha = a_0 + a_1 p + a_2 p^2 + \ldots$ and $\beta = b_0 + b_1 p + b_2 p^2 + \ldots$, and $\alpha + \beta = \gamma = c_0 + c_1 p + c_2 p^2 + \ldots$, then $c_0 = a_0 + b_0 \mod p$. To find c_1, we have to solve $c_0 + c_1 p = a_0 + b_0 + +a_1 p + b_1 p \mod p^2$. Since we are going from mod p to mod p^2, there is not an easy way to express c_1 without a_0 and b_0. To find each subsequent term, we similarly have to consider all previous a_i and b_i, as well as c_i. Multiplication has a similar flavor; if $\alpha \cdot \beta = \mu = v_0 + v_1 p + v_2 p^2 + \ldots$, then $v_0 = a_0 b_0 \mod p$. To find subsequent terms, we have to consider previous terms. For example, to find v_1, we must solve $v_0 + v_1 p = (a_0 + a_1 p)(b_0 + b_1 p) \mod p^2$.

3. The Analytic Definition of the p-adic Integers

The p-adic integers can also be seen as the completion of the integers with respect to a p-adic metric. Let us introduce a p-adic valuation on the integers, which we will extend to $\mathbb{Z}_p$.

Definition 3.1. For any integer a, we can write $a = p^n r$ where p and r are relatively prime. The p-adic absolute value is

$$|a|_p = p^{-n}.$$

It is natural to wonder how the p-adic norm behaves with addition and multiplication.

Lemma 3.2. *For all integers a, b,*

1. $|a + b|_p \leq \max\{|a|_p, |b|_p\}$
2. $|a \cdot b|_p = |a|_p |b|_p$

Proof. Let $a = p^n r$ and $b = p^m s$. Then, $|a|_p = p^{-n}$ and $|b|_p = p^{-m}$.

1. Without loss of generality, say $n \leq m$. Then, $a + b = p^n r + p^m s = p^n(r + p^{m-n}s)$. Since $a + b$ is at least divisible by p^n (it is divisible by higher powers of p if $r + p^{m-n}s$ is divisible by p), the absolute value cannot be larger than p^{-n}. Thus, $|a + b|_p \leq \max\{|a|_p, |b|_p\}$ as desired.
2. We have $a \cdot b = p^{n+m}(r \cdot s)$. Since r and s are relatively prime with p, $r \cdot s$ cannot be divisible by p, and $|a \cdot b|_p = |a|_p|b|_p$, as desired.

□

We can also look at analysis in the p-adics; unlike in standard calculus, a series $\sum a_n$ in the p-adic metric converges if and only if $\lim_{n\to\infty} |a_n|_p = 0$. This condition is obviously necessary, just as in standard calculus. It is sufficient because $|x+y|_p \leq \max(|x|_p, |y|_p)$; adding numbers with smaller valuations does not have any affect on the overall valuation.

Another concept that makes sense is that of a p-adic order. The p-adic order, denoted ord_p, of the integer $a = p^n r$ would be n. Many computations, like some we will see later, are easier when working with orders instead of absolute values.

Recall that a Cauchy sequence is a sequence (a_n) such that for any $\epsilon > 0$, there exists some $N \in \mathbb{N}$ such that for all $n, m \geq N$, $|a_n - a_m| < \epsilon$. Let us consider Cauchy sequences in $\mathbb{Z}$ with respect to the p-adic norm. These are sequences (a_n) such that above some N, $|a_n - a_m|_p < \epsilon$, so the difference between terms can by divided by higher powers of p.

Definition 3.3. The ring $\mathbb{Z}_p$ is the completion of $\mathbb{Z}$ with respect to the p-adic norm. That is, $\mathbb{Z}_p$ is the set of all equivalence classes of Cauchy sequences (a_n) where (a_n) and (b_n) are equivalent if $\lim_{n\to\infty} |a_n - b_n|_p = 0$.

There is a natural ring structure given by component-wise addition and multiplication. Let (a_n) and (b_n) be representatives in two equivalence classes. Define $(a_n) + (b_n)$ to be $(a_n + b_n)$. This must be a Cauchy sequence. For any ϵ, there exist some N_1 and N_2 such that for all $n, m > N_1$ and $p, q > N_2$, $|a_n - a_m|_p \leq \epsilon$ and $|b_p - b_q|_p \leq \epsilon$. Take N to be the maximum of N_1 and N_2. Then, for any $n, m > N$, we have $|a_n + b_n - a_m - b_m|_p \leq \max\{|a_n - a_m|_p, |b_n - b_m|_p\} \leq \epsilon$. So, $(a_n + b_n)$ is a Cauchy sequence. Addition does not depend on choice of representative. If we have (a'_n) and (b'_n), two other representatives, then we know $\lim_{n\to\infty} a_n - a'_n = 0$ and $\lim_{n\to\infty} b_n - b'_n = 0$, so $\lim_{n\to\infty} a_n + b_n - a'_n - b'_n = 0$.

Let us also define multiplication to be $(a_n) \cdot (b_n) = (a_n \cdot b_n)$. We know that multiplication is well defined since

$$\begin{aligned} |a_n b_n - a_m b_m|_p &= |a_n b_n - a_n b_m + a_n b_m - a_m b_m|_p \\ &\leq \max\{|a_n|_p \cdot |b_n - b_m|_p, |b_m|_p \cdot |a_n - a_m|\} \end{aligned}$$

Since $|a_n|_p$ and $|b_n|_p$ are both bounded by 1, we know that $(a_n b_n)$ is a Cauchy sequence. The same equation shows that multiplication does not depend on choice of representative. If we take the same equation above and substitute a_m for a'_n and b_m for b'_n and take the limit as $n \to \infty$, we get that the absolute value approaches 0.

Remarks 3.4. This definition yields two facts. Firstly, the integers are contained in the p-adic integers. For any integer n, we can consider the Cauchy sequence (a_m) where each of the $a_m = n$. This sequence is constant, so it must be Cauchy. So, we know $\mathbb{Z} \subseteq \mathbb{Z}_p$. This fact implies that an equation can only have a solution in $\mathbb{Z}$

if it has a solution in $\mathbb{Z}_p$. Secondly, the p-adic norm can be uniquely extended to $\mathbb{Z}_p$. If (a_n) is a sequence in $\mathbb{Z}_p$, then we can define $|(a_n)|_p$ to be $\lim_{n\to\infty} |a_n|_p$. We know that $|a_n|_p$ must have a limit, as (a_n) is a Cauchy sequence with respect to this absolute value.

We now have two definitions of $\mathbb{Z}_p$, and we must show that they are equivalent.

Proposition 3.5. *Definitions 2.1 and 3.3 are equivalent.*

Proof. Let us define a map ϕ from the set from Definition 2.1 to the set described in Definition 3.3. Any p-adic integer of the form $a_0 + a_1 p + \ldots + a_n p^n + \ldots$ can be written as a sequence (s_n) by taking $s_n = \sum_{i=1}^{n} a_i p^i$. We will show that this sequence is Cauchy. For any $\epsilon > 0$, there is some N such that $\epsilon < p^{-N}$. For any $n > m > N$, we know $s_n - s_m = \sum_{i=m+1}^{n} a_i p^i$. Since each of these terms must be divisible by p^m, we know $|s_n - s_m|_p \leq p^{-m} < \epsilon$. Thus, the sequence (s_n) is Cauchy, and all elements of the set from Definition 2.1 can be written as some element from that in Definition 3.3.

We can also define an inverse map ψ from the set in Definition 3.3 to that in Definition 2.1. First, let us pick a representative of an equivalence class in $\mathbb{Z}_p$. Since the sequence (s_n) is Cauchy, for any k, there must exist some N above which taking the residue mod p^k is stable. Take T_k to be this residue, that is, the representative of $\lim_{n\to\infty} s_n \mod p^k$ taken from $1, 2, \ldots, p^k - 1$. Then, we can write $a_0 = T_0$ and $a_i = (T_i - T_{i-1})/p^i$ for $i \geq 1$. This map is independent of choice of representative. If we have two representatives (s_n) and (s'_n), then $\lim_{n\to\infty} |s_n - s'_n|_p = 0$. Taking the residue mod p^k must be invariant under choice of representative.

The two maps described are inverses, and applying both maps is equal to the identity. Applying ϕ to the image of ψ (that is, taking $\phi \circ \psi$), we can take s'_n to be $\sum_{i=0}^{n} a_i p^i$ where the a_i are chosen as described, then $s'_n = \sum_{i=1}^{n} T_{i+1} - T_i = T_{n+1}$. We must show that (s_n) and (s'_n) are equivalent, or $|s_n - s'_n|_p = |s_n - T_{n+1}|_p$ approaches 0 as $n \to \infty$. Since (s_n) is Cauchy, for all $\epsilon > 0$, there exists some N_1 such that for all $n, m > N_1$, we have $|s_n - s_m|_p < \epsilon$. Note that there also exists some N_2 such that for all $n > N_2$, we have $p^{-(n+1)} < \epsilon$. Let N be the maximum of N_1, N_2. Then, for all fixed $n > N$, since $T_{n+1} = \lim_{m\to\infty} s_m \mod p^{n+1}$, there exists some $M > N$ such that $p^{n+1} | (T_{n+1} - s_M)$, which implies that $|T_{n+1} - s_M|_p < p^{-n+1} < \epsilon$. So, $|s_n - T_{n+1}|_p = |(s_n - s_m) + (s_m - T_{n+1})|_p \leq \max(|s_n - s_m|_p, |s_m - T_{n+1}|_p) = \epsilon$. The composition of the two maps is therefore the identity.

We have shown that ϕ is a bijection, so if we show that it is a ring homomorphism, we will know that the constructions from definitions 2.1 and 3.3 are isomorphic as rings. Let us check that it respects addition and multiplication.

$$\begin{aligned}
\phi(\sum a_n p^n + \sum b_n p^n) &= \sum_{n=0}^{\infty} a_n p^n + \sum_{n=0}^{\infty} b_n p^n \mod p^{n+1} \\
&= \sum a_n p^n \mod p^{n+1} + \sum b_n p^n \mod p^{n+1} \\
&= \phi(\sum a_n p^n) + \phi(\sum b_n p^n)
\end{aligned}$$

$$\begin{aligned}\phi(\sum a_n p^n \cdot \sum b_n p^n) &= \sum_{n=0}^{\infty} a_n p^n \cdot \sum_{n=0}^{\infty} b_n p^n \mod p^{n+1} \\ &= \sum a_n p^n \mod p^{n+1} \cdot \sum b_n p^n \mod p^{n+1} \\ &= \phi(\sum a_n p^n) \cdot \phi(\sum b_n p^n)\end{aligned}$$

The two definitions are therefore equivalent. □

Remark 3.6. The same valuation as we discussed in Definition 3.1 makes sense for p-adic integers. For any p-adic integer, $|a_0 + a_1 p + \ldots + a_n p^n + \ldots|_p$ is $\frac{1}{p^n}$ such that $a_n \neq 0$ and $a_i = 0$ for $i < n$. We also have $\text{ord}_p(a_0 + a_1 p + \ldots + a_n p^n + \ldots) = n$. This norm is equivalent to that defined in remark 3.4.

There is a third definition of the p-adic integers, but we must first introduce some notions from commutative algebra.

4. The Algebraic Definition of the p-adic Integers

There is also an algebraic definition of the completion of a group, which can also give us an equivalent definition of the p-adic integers as a completion of $\mathbb{Z}$.

Definition 4.1. Let us consider a family of groups $\{G_i\}$ with homomorphisms $\varphi_{ji} : G_j \to G_i$ for all $i \leq j$ such that φ_{ii} is the identity on G_i and $\varphi_{ki} = \varphi_{kj} \circ \varphi_{ji}$ for all $i \leq j \leq k$. The inverse limit, denoted $\varprojlim G_n$, is the set of all sequences (a_n) with the property $a_n \in G_n$ and $\varphi_{ji}(a_j) = a_i$ for all $i \leq j$.

Remark 4.2. The inverse limit $\varprojlim G_n$ has a natural group structure given by component-wise addition. Additionally, if the G_n are rings, then $\varprojlim G_n$ inherits a ring structure.

Remark 4.3. For all n, we have a natural projection $p_n : \varprojlim G_n \longrightarrow G_n$ defined by $(a_n) \mapsto a_n$. This map is a group homomorphism.

The completion of a group G with respect to a system of subgroups

$$G = G_0 \supseteq G_1 \supseteq \ldots \supseteq G_n \supseteq \ldots$$

with maps $\varphi_{n+1} : G/G_{n+1} \to G/G_n$ is denoted $\widehat{G}$ and defined as $\varprojlim G/G_n$. The inverse limit $\varprojlim G/G_n$ is the set of all sequences (a_n) with the property $a_n \in G/G_n$ and $\varphi_{n+1}(a_{n+1}) = a_n$ for all n. [1]

Note that this definition of completion is analogous to the topological definition of completion. The subgroups G_n provide a topology on G, as they define open neighborhoods of the identity on G. By translation, for an element g of G, we have a basis for open neighborhoods given by $g + G_n$. The Cauchy sequences (s_n) in this topology are sequences such that for any G_k, there is some N such that for all $n, m > N$, $s_n - s_m$ is in G_k.

Any Cauchy sequence gives an element of the inverse limit. We can define p_k to be the projection $G \to G/G_k$. Then, $p_k(s_n) = p_k(s_m)$ for all $n, m > N$. If $a_k := p_m(s_n)$ for all $n > N$, then (a_k) is an element of $\varprojlim G/G_k$. We can show that the completion is the same as the inverse limit by showing that there is an inverse map, and every element in the inverse limit yields a Cauchy sequence. If we have $(a_k) \in \varprojlim G/G_k$, then we can choose a sequence of representatives $s_n \in G$ in the equivalence classes of $a_n \in G/G_n$. We can show that (s_n) is a Cauchy sequence,

which does not vary under choice of representative, and get that the inverse limit and completion are equivalent.

One common special case of completions of groups is the I-adic completion of a ring R for some ideal I. The sequence of subgroups we consider is $G = R$ and $G_n = I^n R$. We can apply this idea, with $R = \mathbb{Z}$ and $I = (p)$, to define the p-adic integers in a different way.

Remark 4.4. The p-adic integers are the (p)-adic completion of $\mathbb{Z}$, that is, $\varprojlim \mathbb{Z}/p^n\mathbb{Z}$. The p-adic integers are a special case of Definition 4.1.

The inverse limit definition of the p-adics is equivalent to the Cauchy completion of $\mathbb{Z}$ under the p-adic norm. All three definitions of the p-adics are therefore equivalent.

5. The Units of $\mathbb{Z}_p$, Analytically

The different ways of looking at the p-adic integers give us different ways to consider the group of units.

Lemma 5.1. *An element α of $\mathbb{Z}_p$ is invertible if and only if $a_0 \neq 0$, or equivalently, $|\alpha|_p \leq 1$.*

Proof. For α to be in $\mathbb{Z}_p^\times$, its multiplicative inverse $\frac{1}{\alpha}$ must be in $\mathbb{Z}_p$. All p-adic integers have norm less than or equal to 1, so $|\alpha|_p \leq 1$ and $|\frac{1}{\alpha}|_p = \frac{1}{|\alpha|_p} \leq 1$, which implies $|\alpha|_p = 1$. Similarly, if $|\alpha|_p = 1$, then $\frac{1}{\alpha}$ is also a p-adic integer and α must be invertible. If we write α as a formal power series $a_0 + a_1 p + \ldots + a_n p^n + \ldots$, the condition $a_0 \neq 0$ is necessary and sufficient for α to be a unit. We know that a_0 must be in $\mathbb{Z}/p\mathbb{Z}$, so for α to be a unit, we need it to be in $(\mathbb{Z}/p\mathbb{Z})^\times$. □

As sets, we therefore have $\mathbb{Z}_p^\times = (\mathbb{Z}/p\mathbb{Z})^\times \times (1 + p\mathbb{Z}_p)$.

We can show more than just equivalence of sets: we can show that $\mathbb{Z}_p^\times$ and $\mathbb{Z}/p\mathbb{Z}^\times \times (1+p\mathbb{Z}_p)$ are isomorphic as groups for $p \neq 2$. Let us start by looking at this case. For convenience, let us define $U_1 := 1+p\mathbb{Z}_p$. Note that the algebraic definition of the p-adic integers implies that there is a natural projection $\mathbb{Z}_p^\times \to (\mathbb{Z}/p\mathbb{Z})^\times$. There is an exact sequence

$$1 \longrightarrow U_1 \longrightarrow \mathbb{Z}_p^\times \longrightarrow (\mathbb{Z}/p\mathbb{Z})^\times \longrightarrow 0. \tag{5.2}$$

We want to show that this sequence splits, which is the same as saying that $\mathbb{Z}_p^\times$ is isomorphic to $\mathbb{Z}/p\mathbb{Z}^\times \times (1 + p\mathbb{Z}_p)$.

We can analytically demonstrate that the exact sequence splits by applying Hensel's lemma:

Lemma 5.3. *(Hensel) For any polynomial $f(x)$ with p-adic coefficients and p-adic integer a such that $f(a) \equiv 0 \mod p$ and $f'(a) \not\equiv 0 \mod p$, there is a unique p-adic integer α such that $f(\alpha) = 0$ and $\alpha \equiv a \mod p$.*

The proof of this lemma involves a version of Newton's formula, and can be found in [2]. The lemma says that you can uniquely lift a simple root of a polynomial in $\mathbb{F}_p$ to $\mathbb{Z}_p$, which implies that $\mathbb{Z}_p$ contains the $(p-1)$th roots of unity. Indeed, these roots of unity are the solutions of the equation $x^{p-1} - 1 = 0$. The derivative of this polynomial is $(p-1)x^{p-2}$, which is nonzero as long as x is nonzero in $\mathbb{F}_p$. Hensel's lemma tells us that there is a unique root in $\mathbb{Z}_p$ congruent to each of $1, 2, ..., p-1 \mod p$, which means that there is a subgroup of $\mathbb{Z}_p$ that is isomorphic to $(\mathbb{Z}/p\mathbb{Z})^\times$.

Looking at the map $\mathbb{Z}_p \to (\mathbb{Z}/p\mathbb{Z})^\times$ in the extension, we know that the subgroup isomorphic to $(\mathbb{Z}/p\mathbb{Z})^\times$ in $\mathbb{Z}_p$ intersects trivially with U_1, as every element of U_1 is congruent to 1 mod p. Recall the splitting lemma, which says that in abelian groups, short exact sequences $0 \to A \to B \xrightarrow{p} C \to 0$ are split if there is a map $q : C \to B$ such that pq is the identity on C. We therefore know that the sequence is split, and $\mathbb{Z}_p^\times \cong U_1 \times (\mathbb{Z}/p\mathbb{Z})^\times$.

5.1. **More on U_1.** Let us now take a closer look at U_1. We can show that $1 + p\mathbb{Z}_p$ is isomorphic to $\mathbb{Z}_p$ (for $p \neq 2$) using analytical tools: exponential and logarithmic maps. In general, exponential and logarithmic maps allow us to switch between thinking additively and multiplicatively; here, we want to move between the multiplicative group $1 + p\mathbb{Z}_p$ and the additive group $\mathbb{Z}_p$. We can define a log map from $(1 + p\mathbb{Z}_p, \times)$ to $(\mathbb{Z}_p, +)$ by $x \to \log(x)$; the inverse of this map is an exponential.

Lemma 5.4. *The logarithmic map converges for all elements of $1 + p\mathbb{Z}_p$.*

Proof. The Taylor series for a logarithmic map $\log(1 + x)$ is $\sum(-1)^{n+1}\frac{x^n}{n}$. For this series to converge, we need $\lim_{n\to\infty}(-1)^n\frac{x^n}{n} = 0$, which means $\lim_{n\to\infty}\frac{x^n}{n}$ must equal 0. Saying that the absolute value must approach 0 is the same as saying that the order must approach ∞. Note that $\mathrm{ord}(x/y) = \mathrm{ord}(x) - \mathrm{ord}(y)$, so $\mathrm{ord}(x^n/n) = \mathrm{ord}(x^n) - \mathrm{ord}(n)$, which equals $n\ \mathrm{ord}(x) - \mathrm{ord}(n)$. This expression obviously converges if $\mathrm{ord}_p(x) \geq 1$. It cannot converge if $\mathrm{ord}_p(x) = 0$, so in $\mathbb{Z}_p$, we have that $\mathrm{ord}_p(x) \geq 1$, or equivalently, $|x|_p \leq \frac{1}{p}$. The logarithmic map $\log(1 + x)$ therefore converges for every element of $p\mathbb{Z}_p$, so the map $\log(x)$ converges for every element of $1 + p\mathbb{Z}_p$. □

Let us now look at the inverse map, $\exp(x)$.

Lemma 5.5. *If $ord_p(x) > \frac{1}{p-1}$, then $\exp(x)$ converges.*

Proof. The Taylor series for $\exp(x)$ is $\sum\frac{x^n}{n!}$. The order of $n!$ is $\sum_{i=1}^{\infty}\lfloor\frac{n}{p^i}\rfloor$, as each $\lfloor\frac{n}{p^i}\rfloor$ counts how many integers less than or equal to n are divisible by p^i, and the sum of all of these gives the multiplicity of p in the prime factorization of $n!$. Since $\lfloor\frac{n}{p^i}\rfloor \leq \frac{n}{p^i}$, we know $\sum_{i=1}^{\infty}\lfloor\frac{n}{p^i}\rfloor \leq \sum_{i=1}^{\infty}\frac{n}{p^i}$, which equals $\frac{n}{p-1}$ by the usual formula for geometric series. Since $\mathrm{ord}(\frac{x^n}{n!}) = \mathrm{ord}(x^n) - \mathrm{ord}(n!)$, we have $\mathrm{ord}(\frac{x^n}{n!}) \geq n \cdot \mathrm{ord}(x) - \frac{n}{p-1}$. The series therefore converges for any p-adic number α where $\mathrm{ord}(\alpha) > \frac{1}{p-1}$, or equivalently, where $|\alpha|_p < p^{-1/(p-1)}$. For $p \neq 2$, the exponential map converges for all elements of $p\mathbb{Z}_p$. □

We also want to show that the image of each map is in the radius of convergence of the other. For an element of $p\mathbb{Z}_p$, the sum $\sum\frac{x^n}{n!}$ always has a positive order, so the image under the exponential map must be in the radius of convergence of the logarithmic map. Note that when we take $\log(\exp(x))$, we are really applying $\log(1+x)$ to $\exp(x)-1$, but since the order of $\sum\frac{x^n}{n!}$ is greater than the order of -1, the order of $\exp(x) - 1$ equals the order of $\exp(x)$. To show that the image of the logarithm is in the domain of the exponential, note that $|\frac{(-1)^{n+1}x^n}{n}| < |x|$. We can see this by manipulating the difference of the orders. We have that $|\log(x)| = |x|$, so it is in the radius of convergence of the exponential map.

We have now defined a logarithmic map and its exponential inverse from the multiplicative group $1 + p\mathbb{Z}_p$ to the additive group $p\mathbb{Z}_p$, so these are isomorphic.

Since the additive groups $p\mathbb{Z}_p$ and $\mathbb{Z}_p$ are isomorphic, we have $1 + p\mathbb{Z}_p \cong \mathbb{Z}_p$, and so $\mathbb{Z}_p^\times \cong \mathbb{Z}_p \times (\mathbb{Z}/p\mathbb{Z})^\times$ as desired.

5.2. **The Case of $p = 2$.** If $p = 2$, then $\mathbb{Z}_2^\times$ is actually ismorphic to $\mathbb{Z}/2\mathbb{Z}\times(1+4\mathbb{Z}_2)$.

For $p = 2$, there are more roots of unity than Hensel's lemma implies. Using Hensel's lemma only gives us the obvious result of a single first root of unity. $\mathbb{Z}_2$ actually contains two second roots of unity, the equivalents of ± 1. From direct computation, we can see that both 1 and $1 + 1 \cdot 2 + 1 \cdot 2^2 + \ldots$ are equal to 1 when squared.

For $p = 2$, the exponential map converges for $4\mathbb{Z}_2$, as these are the elements for which $\mathrm{ord}_2(x) > 1$. By applying the logarithmic and exponential maps, we therefore know that $(1 + 4\mathbb{Z}_2, \times)$ is isomorphic to $(4\mathbb{Z}_2, +)$, and thus to $(\mathbb{Z}_2, +)$.

Let us consider the exact sequence

$$1 \longrightarrow (1 + 4\mathbb{Z}_2) \longrightarrow \mathbb{Z}_2^\times \longrightarrow \{\pm 1\} \longrightarrow 0 \tag{5.6}$$

There is a natural projection from $\mathbb{Z}_2^\times$ to $\longrightarrow \{\pm 1\}$, as each unit of $\mathbb{Z}_2$ is either isomorphic to 1 or -1 mod 4. The image of $1 + 4\mathbb{Z}_2$ under the inclusion map must intersect trivially with the preimage of $\{\pm 1\}$, which is isomorphic to $\mathbb{Z}/4\mathbb{Z}^\times$ and $\mathbb{Z}/2\mathbb{Z}$. The sequence therefore splits, and $\mathbb{Z}_2^\times \cong \mathbb{Z}/2\mathbb{Z} \times (1 + 4\mathbb{Z}_2)$, as desired.

6. The Units of $\mathbb{Z}_p$, Algebraically

We can use the inverse limit definition of the p-adic integers to find the group of units in a somewhat different manner, without using Hensel's lemma. Let U denote the units of $\mathbb{Z}_p^\times$, and let us define U_n to be $1 + p^n\mathbb{Z}_p$. We can use algebraic methods to show that $U \cong \mathbb{F}_p^\times \times U_1$ and, for $p \neq 2$, U_1 is isomorphic to $\mathbb{Z}_p$.

Lemma 6.1. *If we have an exact sequence of commutative groups $0 \to A \to E \to B \to 0$, where A and B are finite and have relatively prime orders, then $E \cong A \times B'$, where B' is the (unique) subgroup of E isomorphic to B.*

Proof. Let a denote the order of A and b the order of B. Since a and b are relatively prime, there must be some integers r and s such that $ra + sb = 1$. Let B' be the set of elements in E with order dividing b, that is, elements x such that $bx = 0$. If an element x is in $A \cap B'$, then $ax = 0$ and $bx = 0$, so $x = (ra + sb)x = 0$. The intersection is trivial. All elements x of E can be written as $x = rax + sbx$, so $rax \in B'$ and $sbx \in A$. So, E is the direct sum of A and B', and the projection from E to B is an isomorphism when restricted to B'. Any subgroup of E isomorphic to B would be contained in B', as all elements would have to have order divisible by b. Since the group would have have to have the same order as B', the groups would have to be equal. [6] □

For all n, U_n is a subgroup of U.

Lemma 6.2. *U is $\varprojlim U/U_n$.*

Proof. We know that $\mathbb{Z}_p = \varprojlim \mathbb{Z}/p^n\mathbb{Z}$ and there exist projections $p_n : \mathbb{Z}_p \to \mathbb{Z}/p^n\mathbb{Z}$. The kernel of any projection p_n is $p^n\mathbb{Z}_p$. Then, $\mathbb{Z}_p = \varprojlim \mathbb{Z}/p^n\mathbb{Z} = \varprojlim Z_p/\ker(p_n)$. We also know $\mathbb{Z}_p^\times$ is $(\varprojlim \mathbb{Z}/p^n\mathbb{Z})^\times = \varprojlim(\mathbb{Z}/p^n\mathbb{Z})^\times$. We know $\mathbb{Z}_p^\times$ is a subgroup of $\mathbb{Z}_p$, so p_n restricted to $\mathbb{Z}_p^\times$ is a group homomorphism. Each p_n gives us a surjective map from $\mathbb{Z}_p$ to $(\mathbb{Z}/p^n\mathbb{Z})^\times$. The kernel of each p_n is $1 + p^n\mathbb{Z}_p$, which equals U_n. So, $\mathbb{Z}_p^\times = \varprojlim U/U_n$. □

Lemma 6.3. *U_n/U_{n+1} is isomorphic to $\mathbb{Z}/p\mathbb{Z}$.*

Proof. Let us define a map $h : (U_n, \cdot) \to (\mathbb{Z}/p\mathbb{Z}, +)$ by $1 + p^n x + \ldots \mapsto x \mod p$. This map is a group homomorphism, as $(1 + p^n x)(1 + p^n y) \equiv 1 + p^n(x + y) \mod p^{n+1}$, and so $h(1+p^n x)(1+p^n y) = (x+y) \mod p = h(1+p^n x) + h(1+p^n y)$. The map is surjective, as x can be any of $0, 1, 2, \ldots, p-1$. The kernel is U_{n+1}, as the elements of U_n where $x = 0$ are in U_{n+1} as well. Thus, $U_n/U_{n+1} \cong \mathbb{Z}/p\mathbb{Z}$. □

Because we know U_n/U_{n+1} has order p, we can use induction on n to find that U_1/U_n has order p^{n-1}.

Let us consider the exact sequence

$$1 \longrightarrow U_1/U_n \longrightarrow U/U_n \longrightarrow \mathbb{F}_p^\times \longrightarrow 1 \tag{6.4}$$

The order of $\mathbb{F}_p^\times$ is $p-1$, while the order of U_1/U_n is p^{n-1}, so we can apply the lemma: we know $U/U_n \cong \mathbb{F}_p^\times \times U_1/U_n$. Let us define V_n to be the unique subgroup of U/U_n isomorphic to $\mathbb{F}_p^\times$. If we have a map $\theta_n : U/U_n \to U/U_{n-1}$, then $\ker(\theta_n) = U_{n-1}/U_n \cong \mathbb{Z}/p\mathbb{Z}$. We can restrict θ_n to V_n, and the kernel is $V_n \cap \ker(\theta_n)$. Since the kernel would have to have an order dividing both that of V_n (which is $p-1$), and that of $\ker(\theta_n)$ (which is p), it must be trivial; θ_n is an isomorphism when restricted to V_n. Thus, the image of V_n under θ_n is a group of order $p-1$ in U/U_{n-1}, and is therefore the unique subgroup V_{n-1}. Since θ_n carries V_n isomorphically onto V_{n+1}, when we take inverse limits, while $U = \varprojlim U/U_n$, $V = \varprojlim V_n \cong \mathbb{F}_p^\times$. Thus, U has a subgroup isomorphic to $\mathbb{F}_p^\times$, and $U \cong U_1 \times \mathbb{F}_p^\times$. Note that we have shown that $\mathbb{Z}_p$ contains the $(p-1)$-th roots of unity without directly using Hensel's lemma.

We can also show that U_1 is isomorphic to $\mathbb{Z}_p$ for the case of $p \neq 2$, or to $\{\pm 1\} \times U_2$ for the case $p = 2$. First, let us note that if α is in $U_n - U_{n+1}$, then α^p is in $U_{n+1} - U_{n+2}$. We can write α as $1 + kp^n$ for some k in $\mathbb{F}_p^\times$. Raising α to the p-th power, we get that the only terms that are not congruent to 0 mod $n+2$ are $1 + kp^{n+1}$.

For the case $p \neq 2$, let us consider an element α of $U_1 - U_2$. Then, α^{p^i} is in $U_{i+1} - U_{i+2}$. Let us define α_n to be the image of α in U_1/U_n. Then, $(\alpha_n)^{p^{n-2}}$ is not 1, but $(\alpha_n)^{p^{n-1}}$ is; α_n has order p^{n-1}, which means that it is a generator for U_1/U_n. We can define an isomorphism θ_n from $\mathbb{Z}/p^{n-1}\mathbb{Z}$ to U_1/U_n by $z \mapsto \alpha_n^z$. By taking the inverse limits, we get an isomorphism θ from $\varprojlim \mathbb{Z}/p^{n-1}\mathbb{Z} = \mathbb{Z}_p$ to $\varprojlim U_1/U_n = U_1$. We have $U_1 \cong \mathbb{Z}_p$, as desired. So, $U \cong \mathbb{F}_p^\times \times \mathbb{Z}_p$.

For the case $p = 2$, let us consider an element α of $U_2 - U_3$, that is, α is congruent to 5 mod 8. Using the same isomorphism θ_n as above, except from $\mathbb{Z}/2^{n-2}\mathbb{Z}$ to U_2/U_n. Again, we can take the inverse limits to get an isomorphism from $\mathbb{Z}_2$ to U_2. Since $U_1 \cong \mathbb{Z}/2\mathbb{Z} \times U_2$, and $\mathbb{Z}/2\mathbb{Z}$ is isomorphic to $\{\pm 1\}$, we have $U_1 \cong \{\pm 1\} \times \mathbb{Z}_2$. Since $\mathbb{F}_2^\times$ is trivial, for $p = 2$, we know $U \cong \{\pm 1\} \times \mathbb{Z}_2$. [6]

7. The Exactness of Completion

The algebraic definition of the p-adic integers has another interesting consequence. For an ideal I and R-module M, we can extend an I-adic completion of R to an I-adic completion of M. The I-adic completion of a module M is defined similarly to the I-adic completion of a ring: $\widehat{M_I} = \varprojlim M/I^n M$. This construction allows us to take the p-adic completion of any $\mathbb{Z}$-module, that is, any abelian group.

Completions are an important concept in algebraic topology, and one useful lemma about completions is the Artin-Rees lemma. The Artin-Rees lemma states that for any Noetherian ring R with ideal I and finitely generated R-module M and submodule M', there is some sufficiently large k so that $I^nM \cap M' = I^{n-k}(I^kM \cap M')$ [1]. The left hand side of this construction gives the subspace topology on M' induced by intersecting it with $\{I^nM\}$. The right hand side is the I-adic topology induced on M'. After a certain point, it does not matter if we intersect the two modules first, then apply I more times, or apply I first, then intersect the modules.

This lemma can be used to prove the exactness property of completion, which can be applied to p-adic numbers to tell us that for finitely generated abelian groups, p-adic completion preserves exact sequences.

Theorem 7.1. *If we have an exact sequence of finitely-generated R-modules*

$$0 \longrightarrow M_1 \longrightarrow M_2 \longrightarrow M_3 \longrightarrow 0 \tag{7.2}$$

then the I-adic completion

$$0 \longrightarrow \widehat{M_1} \longrightarrow \widehat{M_2} \longrightarrow \widehat{M_3} \longrightarrow 0 \tag{7.3}$$

is also exact.

Proof. If $0 \to M_1 \to M_2 \to M_3 \to 0$ is exact, then we can also show that

$$0 \longrightarrow M_1/(M_1 \cap I^kM_2) \longrightarrow M_2/I^kM_2 \longrightarrow M_3/I^kM_3 \longrightarrow 0 \tag{7.4}$$

is exact. The exactness of (7.2) implies that $M_2 \to M_3$ is surjective, which implies that $I^kM_2 \to I^kM_3$ is surjective, and therefore that $M_2/I^kM_2 \to M_3/I^kM_3$ is surjective. The kernel of this map is $(M_1 + I^kM_2)/I^kM_2$, which is isomorphic to $M_1/(M_1 \cap I^kM_2)$. Since we have an injective map followed by a surjective map, sequence (7.4) is exact.

Let us now take the inverse limits of each of these modules. We get the sequence

$$0 \longrightarrow \varprojlim M_1/(M_1 \cap I^kM_2) \longrightarrow \varprojlim M_2/I^kM_2 \longrightarrow \varprojlim M_3/I^kM_3 \longrightarrow 0 \tag{7.5}$$

Taking an inverse limit always preserves left exactness, and if we have a surjective system, then it preserves exactness.

Lemma 7.6. *Given an exact sequence*

$$0 \longrightarrow A_n \longrightarrow B_n \longrightarrow C_n \longrightarrow 0$$

and systems $\{A_n\}, \{B_n\}, \{C_n\}$, if for all n, $A_{n+1} \to A_n$ is surjective, then there is an exact sequence

$$0 \longrightarrow \varprojlim A_n \longrightarrow \varprojlim B_n \longrightarrow \varprojlim C_n \longrightarrow 0.$$

Proof. Recall the snake lemma, which says that given a commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A & \longrightarrow & B & \longrightarrow & C & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle a} & & \downarrow{\scriptstyle b} & & \downarrow{\scriptstyle c} & & \\ 0 & \longrightarrow & A' & \longrightarrow & B' & \longrightarrow & C' & \longrightarrow & 0 \end{array}$$

where the rows are exact sequences, there exists an exact sequence

$$0 \longrightarrow \ker a \longrightarrow \ker b \longrightarrow \ker c \longrightarrow \operatorname{coker} a \longrightarrow \operatorname{coker} b \longrightarrow \operatorname{coker} c \longrightarrow 0.$$

We can apply this lemma with $A = \prod A_n$ and $a : A \to A$ where a is defined as $a((a)_n) = (x_n)$ with $x_n = a_n - \theta_{n+1}(a_{n+1})$ and θ_{n+1} is the projection from

A_{n+1} to A_n; define B and C similarly. The kernel of a is $\varprojlim A_n$, so if we apply the snake lemma, we get an exact sequence $0 \to \varprojlim A_n \to \varprojlim B_n \to \varprojlim C_n$. If $A_{n+1} \to A_n$ is surjective, then a is also surjective, so we have an exact sequence $0 \to \varprojlim A_n \to \varprojlim B_n \to \varprojlim C_n \to 0$. □

We know that $\{M_1/(M_1 \cap I^k M_2)\}$ is surjective because $M_1/(M_1 \cap I^{k+1}M_2) \to M_1/(M_1 \cap I^k M_2)$ is surjective, so sequence (7.5) is exact. The completion of M_2 is $\varprojlim M_2/I^k M_2$, and that of M_3 is $\varprojlim M_3/I^k M_3$. By the Artin-Rees lemma, we know that for some k, $M_1/(M_1 \cap I^k M_2)$ is equal to $M_1/I^{n-k}(I^k M \cap M_1)$, which is equal to $\widehat{M_1}$ (as n increases, $I^{n-k}(I^k M \cap M_1)$ approaches $I^n M_1$). We therefore have that (7.3) is exact, as desired. □

If we apply this theorem to the p-adic integers, we find that the p-adic completion of finitely generated $\mathbb{Z}$-modules, that is, abelian groups, preserves exact sequences. p-adic completion is an exact functor when restricted to finitely generated abelian groups.

The p-adic numbers may seem strange upon first glance, but they are more than a mere mathematical curiosity. Why would we define closeness by divisibility by p, so that numbers that would usually be considered far apart are close in the p-adic metric? The metric allows us to equate formal power series and completions; taking additional terms of the power series provides a closer approximation to the number. Furthermore, we were able to connect the analytical Cauchy completion and solving equations to algebraic completion, both of the ring and of its modules. The p-adics lie at the intersection of analysis, algebra, and number theory.

Acknowledgments. It is a pleasure to thank my mentor, Bingjin Liu, for all of her help and guidance on this paper; I would not have been successful without her valuable suggestions and patient explanations. I would also like to thank Aygul Galimova for her additional mentorship and assistance. Finally, I would like to thank Professor Peter May for his support and for organizing the UChicago REU program.

References

[1] Michael F. Atiyah and Ian G. Macdonald. Introduction to Commutative Algebra. Addison-Wesley Publishing Company. 1969.
[2] Keith Conrad. Hensel's Lemma. http://www.math.uconn.edu/ kconrad/blurbs/gradnumthy/hensel.pdf
[3] Fernando Q. Gouvea. p-adic Numbers: An Introduction. Springer. 1997.
[4] A. Khrennikov, K. Oleschko, and M. de Jesus Correa Lopez. Applications of p-adic numbers?: from physics to geology. ADVANCES IN NON-ARCHIMEDEAN ANALYSIS (pp. 121?131). https://doi.org/10.1090/conm/665/13363. 2016.
[5] Frederique Oggier. p-adic numbers. http://web.spms.ntu.edu.sg/ frederique/antchap5.pdf
[6] Jean-Pierre Serre. A Course in Arithmetic. Springer. 1973.