The Artin-Hasse Exponential Function

Derek Gao, Henry Greenwold, Leonna Wang, & Niyathi Kukkapalli

July-August 2023

Mentored by Bernie Luan

Thank you to John Sim and Bernie Luan for providing guidance throughout the course of our project.

Abstract

In 1928, the Artin-Hasse Exponential was created as an analogy to the exponential function that comes from infinite products, as discussed in the paper. A introductory discussion of formal power series and their connection to the p-adic numbers is given. The fact that $\mathbb{Q}_p$ is the completion of $\mathbb{Q}$ is proven, laying the grounds for a discussion of radius of convergence (for power series), where the mutual inverse isomorphism between the exponential and logarithmic functions in the p-adic number system is proven. Dwork's Lemma is proven via methods of induction, and is applied to prove the Integrality of the Artin Hasse Function, $E(x)$, which is essential for further research. Extensions regarding $E(x)$ are discussed, such as the radius of convergence and generalized images of the p-adics.

1 Formal Power Series

Definition 1: Let R be a ring and $R[[x]] = \{a_0 + a_1x + a_2x^2 + \ldots | a_i \in R\}$. It is easy to show that $R[[x]]$ is a ring and that $1 \in R[[x]]$ is the multiplicative identity.

Lemma 1: $f = a_0 + a_1x + a_2x^2 + \ldots \in R[[x]]$ is a unit $\iff$ $a_0 \in R$ is a unit.

Proof. For the forward direction, we have that $fg = 1$ for some $g = b_0+b_1x+b_2x^2+\ldots \in R[[x]]$. This means that the constant terms of the left and right hand sides must be equal, so $a_0b_0 = 1 \implies a_0$ is a unit.

For the reverse direction, we want to construct $g = b_0 + b_1x + b_2x^2 + \ldots$ such that $fg = 1$ We know that we can find a b_0 such that $a_0b_0 = 1$ because a_0 is a unit. Then, $\forall n \geq 1$, we want:

$$\sum_{k=0}^{n} a_k b_{n-k} = 0$$

We can do this inductively:

$$a_0 b_n + \sum_{k=1}^{n} a_k b_{n-k} = 0$$

$$\implies a_0 b_n = -\sum_{k=1}^{n} a_k b_{n-k}$$

$$\implies b_n = -b_0 \sum_{k=1}^{n} a_k b_{n-k}$$

Thus we have constructed every coefficient of b to make $ab = 1$ $\forall a$ where a_0 is a unit. □

2 The p-adic Numbers

Definition 2: Let p be a prime number. Define $\mathbb{Z}_p = \{(a_1, a_2, a_3, \ldots)|a_i \in \mathbb{Z}/p\mathbb{Z}\}$ to be the set of p-adic integers. Equivalently, one can write an element $a \in \mathbb{Z}_p$ as the power series $a = a_0 + a_1p + a_2p^2 + \ldots$ with $a_i \in \{0, 1, \ldots, p-1\}$.

Proposition 2.1: The p-adic numbers form a ring under termwise addition and multiplication. Additionally, if $ab = 0$ in $\mathbb{Z}_p$, then either $a = 0$ or $b = 0$.

Proof. Consider the three p-adic numbers $(a_1, a_2, a_3, \ldots)$, $(b_1, b_2, b_3, \ldots)$, and $(c_1, c_2, c_3, \ldots)$. Since we are adding these numbers term by term we only need to consider each individual column, or each a_i, b_i and c_i at a time for each i. Addition and multiplication on these terms act the same way as they do in the integers: $a_i + b_i = b_i + a_i$ (commutativity), $(a_i + b_i) + c_i = a_i + (b_i + c_i)$ and $(a_i \cdot b_i) \cdot c_i = a_i \cdot (b_i \cdot c_i)$ (associativity).

Thus each corresponding term in the sum or product of two or three p-adic numbers will remain the same regardless of the presence of parentheses or order of the terms being summed or multiplied. Distributivity applies in a similar manner: $a_i \cdot (b_i + c_i) = a_i \cdot b_i + a_i \cdot c_i$

The additive identity in the integers is 0, so in the same way the additive identity in the p-adics is the number $(0, 0, 0, \ldots)$, an infinite string of zeros. Adding this to some other p-adic number $(a_1, a_2, a_3, \ldots)$ term by term gives $(a_1 + 0, a_2 + 0, a_3 + 0, \ldots) = (0 + a_1, 0 + a_2, 0 + a_3, \ldots) = (a_1, a_2, a_3, \ldots)$.

For every p-adic integer $(a_1, a_2, a_3, \ldots)$, its additive inverse is the p-adic integer $(p-a_1, p-a_2, p-a_3, \ldots)$. Again, adding these two values term by term gives $(a_1+p-a_1, a_2+p-a_2, a_3+p-a_3, \ldots) = (p - a_1 + a_1, p - a_2 + a_2, p - a_3 + a_3, \ldots) = (p, p, p, \ldots) = (0, 0, 0 \ldots)$, which is the additive identity as shown above.

The multiplicative identity in the p-adics is also represented by the value $1 = (1, 0, 0, \ldots)$. $(a_1, a_2, a_3, \ldots) \cdot (1, 0, 0, \ldots) = (a_1 \cdot 1, a_2 \cdot 1, a_3 \cdot 1, \ldots) = (a_1, a_2, a_3, \ldots)$.

Thus the p-adics satisfy commutativity, associativity, and distributivity. There exists both an additive and multiplicative identity, and every element has an additive inverse, so $\mathbb{Z}_p$ is a ring. □

Theorem 1: $ab = 0$ in $\mathbb{Z}_p \implies a = 0$ or $b = 0$

Proof. Assume that $a = (a_1, a_2, a_3, \ldots) \neq 0$ and $b = (b_1, b_2, b_3, \ldots)$. Then, $\exists k \in \mathbb{N}$ *s.t.* $a_k \neq 0$.

Let us consider each b_i separately. $b_i \cdot a = 0 \implies b_i \cdot a_k = 0$. Since we know that $\mathbb{Z}/p\mathbb{Z}$ contains no zero divisors, b_i must be $0 \implies b_i = 0 \ \forall i \in \mathbb{N} \implies b = (0, 0, 0 \ldots)$, an infinite string of zeros, which we showed is equal to the integer zero. □

Theorem 2 (Hensel's Lemma): Let $f(x) \in \mathbb{Z}_p[x]$ and $a_1 \in \mathbb{Z}_p$. Assume that $f(a_1) \equiv 0 \pmod{p}$ and $f'(a_1) \not\equiv 0 \pmod{p}$. Then there is a unique $a \in \mathbb{Z}_p$ such that $f(a) = 0$ and $a \equiv a_1 \pmod{p}$.

Before we begin this proof let us consider an example in $\mathbb{Z}$. Consider the equation $x^2 \equiv 2 \pmod{7^n}$. It can be easily verified that the solutions taken mod 7 are $x \equiv \pm 3$. Then, $x = 7k \pm 3$ for some integer k. Now let us consider the equation mod 49. Then, $x^2 = (7k+3)^2 = 49k^2 \pm 42k + 9 \equiv \pm 7k + 9 \equiv 2 \pmod{49} \implies \pm 7k \equiv -7 \pmod{49} \implies k \equiv \pm 1 \pmod{7} \implies n \equiv 7(7k \pm 1) \pm 3 \equiv \pm 10 \pmod{49}$.

Proof. Using this example, let us assume a_1 exists and show that a unique a exists. We know that $f(a_1) \equiv 0 \pmod{p}$ and $a_1 \equiv a \pmod{p}$. Let $a = bp + a_1$ for some $b \in \mathbb{Z}$. Let us create a function f. Then, $f(a) = f(bp+a_1)$. We already know that a_1 exists, so we want to show that a does.

Taking the Taylor Series of f centered at a_1 gives:

$$f(x) = f(a_1) + f'(a_1)(x - a_1) + \frac{f''(a_1)(x - a_1)^2}{2} + \ldots + \frac{f^{(n)}(a_1)(x - a_1)^n}{n!} + \ldots$$

Then,

$$f(a) = f(bp + a_1) = f(a_1) + f'(a_1)(bp) + \frac{f''(a_1)(bp)^2}{2} + \ldots + \frac{f^{(n)}(a_1)(bp)^n}{n!} + \ldots \equiv 0 \pmod{p}$$

.

Thus we know $f(a) \equiv 0 \pmod{p} \implies f(a) = pk$ for some $k \in \mathbb{Z}$. Like our above example, now let us consider mod p^2:

$$f(a) \equiv f(a_1) + f'(a_1)(bp) \equiv f(a) + f'(a_1)(bp) \equiv pk + f'(a_1)(bp) \equiv 0 \pmod{p^2}$$

Dividing everything through by p gives

$$k + f'(a_1)b \equiv 0 \pmod{p}$$

Since $f'(a_1) \not\equiv 0 \pmod{p}$, we know that it has an inverse. Thus we can take

$$b = (-k)(f'(a_1))^{-1} \pmod{p}$$

Since k is unique and $f'(a_1)$ is unique, b must be unique. Thus we have shown that we can construct a unique a that satisfies $f(a) = 0$ and $a \equiv a_1 \pmod{p}$.

□

Example 1 Make sense of $\sqrt{p}$ as a p-adic number, regarding it's size.

Let's try $p = 3$, and then let's try $\sqrt{3}$ as a 7-adic number. We want to solve $x^2 \equiv 3(mod 7^k)$ with Hensel's Lemma. Using Hensel's Lemma, we find that the solutions are

$$x^2 \equiv 3 \mod 7$$
$$x^2 \equiv 3 + 7 \mod 7^2$$
$$x^2 \equiv 3 + 7 + 2 \cdot 7^2 \mod 7^3$$
$$x^2 \equiv 3 + 7 + 2 \cdot 7^2 + 6 \cdot 7^3 \mod 7^4$$
$$\ldots$$

We notice that $\sqrt{3}$ has no pattern, but there is a simple way to fix this. Let's use the Binomial Theorem, where we can calculate $(7a+1)^{\frac{1}{2}}$. Then, if we let $a = -\frac{1}{9}$ we get $\frac{\sqrt{2}}{\sqrt{9}}$. If we multiply the final power series by 3, then we get the expansion of $\sqrt{2}$.

First notice that not every $\sqrt{p}$ can be written as a p-adic number. Every rational number that is a quadratic residue mod p_1 can be a square root in $\mathbb{Q}_p$. In the example above, we see $(\frac{2}{7}) = 1$, so 2 is a square in the p-adics. A 2-adic unit α is a square in $\mathbb{Z}_2$ if and only if $\alpha \equiv 1 \mod 8$.

Let's consider a general p-adic number, $a = p^k(a_0 + a_1 p + a_2 p^2 \ldots)$. If $a = b^2$, then $\mid a \mid_p = (\mid b \mid_p)^2$ so that $\mid b \mid_p = \sqrt{\mid a \mid_p} = p^{-\frac{k}{2}}$. If k is even there is no problem, but if k is odd then $b \notin \mathbb{Q}_p$.

We see that the p-adic size of $\sqrt{p}$ is 0, unless the b_0 term in the p-adic expansion $(b_0 + b_1 p + b_2 p^2 + \ldots)$ is 0. The p-adic size of $p^{\frac{a}{b}}$ if $a > b$ would be just $\frac{1}{p^{\lfloor \frac{a}{b} \rfloor}}$. Although, if $a < b$ then we have to look at the congruence $p^a \equiv c \mod p$.

Definition 3: $\mathbb{Q}_p = \mathbb{Z}_p[\frac{1}{p}]$ where $\mathbb{Q}_p$ is the field of p-adic rationals. Moreover, we have two p-adic numbers, $\frac{a}{p^k}$ and $\frac{b}{p^m}$ equal only if $ap^m = bp^k$.

For example, note that we have $\frac{(1,4,13..)}{1} + \frac{(3,3,3..)}{3} + \frac{(2,5,14...)}{9} \in \mathbb{Z}_3$.

But, the above is not equal to $(1,4,13...) + (1,1,1...) + (\frac{2}{9}, \frac{5}{9}, \frac{14}{9}...)$. The division above is merely used as notation and does not directly translate to above. More generally, any element of $\mathbb{Q}_p$ is $a_0 + \frac{a_1}{p} + \frac{a_2}{p^2} + \frac{a_3}{p^3} + ...$ and taking p^k as the common denominator we get $\frac{a_0+a_1p+a_2p^2+...}{p^k} = \frac{a}{p^k}$.

Definition 4: We define the p-adic valuation, $v_p(a)$ of an integer $a \in \mathbb{Z}$ to be the greatest $n \in \mathbb{Z}$ such that $p^n | a$. We extend this definition to $\mathbb{Q}$ such that if $q = \frac{a}{b} \in \mathbb{Q}$, $v_p(q) = v_p(a) - v_p(b)$. Moreover, we define $v_p(0) = \infty$

Definition 5: We define the p-adic absolute value (or norm) to be the function $|\,.\,|_p\colon\ \mathbb{Q} \to \mathbb{R}$, such that for $q \in \mathbb{Q}$, $|q|_p = p^{-v_p(q)}$

Lemma 2: $\mathbb{Q}$ is contained in $\mathbb{Q}_p$

Proof. Before tackling $\mathbb{Q}_p$, let's start by considering the localization of $\mathbb{Z}$ at p the set:

$$\mathbb{Z}_{(p)} := \{(\frac{a}{b}) \in \mathbb{Q} \mid (a,b) = 1,\ p \not| b\}$$

We claim that $\mathbb{Z}_{(p)}$ is contained within $\mathbb{Z}_p$. We note that $\forall \frac{a}{b} \in \mathbb{Z}_{(p)}$, $\frac{a}{b} \in \mathbb{Z}_p$, as $\forall k \in \mathbb{N}$ there exists an inverse element of b, $b_k^{-1} \in \mathbb{Z}/p^k\mathbb{Z}$ such that $bb_k^{-1} = 1$ in $\mathbb{Z}/p^k\mathbb{Z}$, and thus there exists an element $ab_k^{-1} \in \mathbb{Z}/p^k\mathbb{Z}$ such that $bab_k^{-1} = a$ in $\mathbb{Z}/p^k\mathbb{Z}$. Considering the sequence ab_k^{-1} for $k = 1, 2, \ldots$ in $\mathbb{Z}_p$, we see that it is equivalent to some $x \in \mathbb{Z}_p$ such that $bx = a$, i.e. $x = \frac{a}{b}$

So $\mathbb{Z}_{(p)}$ is contained within $\mathbb{Z}_p$. We wish to use this fact to show that $\mathbb{Q}$ is contained within $\mathbb{Q}_p$. For all $\frac{c}{d} \in \mathbb{Q}$, let $\frac{c}{d} = p^k(\frac{a}{b})$, for $k \in \mathbb{Z}$, and $\frac{a}{b} \in \mathbb{Z}_{(p)}$.

As $\frac{a}{b} \in \mathbb{Z}_{(p)}$, we have shown that $\frac{a}{b} \in \mathbb{Z}_p$, and can write it's p-adic expansion as $a_0+a_1p+a_2p^2+\ldots$, where each $a_i \in \{0, 1, \ldots, p-1\}$.

Then $\frac{c}{d} = a_0p^k + a_1p^{k+1} + a_2p^{k+2} + \ldots$. As this expansion is an element of $\mathbb{Q}_p$, it follows that $\frac{c}{d} \in \mathbb{Q}_p$, and thus $\mathbb{Q}$ is contained within $\mathbb{Q}_p$. □

Proposition 2.2: $\mathbb{Q}_p$, is a field given the fact that $\mathbb{Q}$ is contained in $\mathbb{Q}_p$.

Proof. It can be easily checked by using the fact that $\mathbb{Q}_p$ is the completion of the rationals with respect to the p-adic norm. □

Question 2.3 What *do* p-adically small numbers look like? What do p-adically large numbers look like?

An example of a p-adically large number would be of the form 000...0001, for the absolute value of a p-adic number is the reciprocal of the largest power of p that divides it.

An example of a p-adically small number would be of the form 1000...000, as the larger the denominator, the smaller the fraction is (closer to 0).

Proposition 2.4.1: The following properties of $v_p(n)$ for any $a, b \in \mathbb{Z}$ hold true.

1. $v_p(ab) = v_p(a) + v_p(b)$
2. $v_p(a+b) \leq min(v_p(a), v_p(b))$
3. If $v_p(a) \neq v_p(b)$ then $v_p(a+b) = min(v_p(a), v_p(b)$.

Proof. Let $v_p(a) = k_1$ and $v_p(b) = k_2$. WLOG, assume that $k_1 \geq k_2$.

1. We have $ab = a'b'p^{k_1+k_2}$ where $(a'b', p) = 1$ since each of the a' and b' are co-prime to p. Hence $v_p(ab) = k_1 + k_2 = v_p(a) + v_p(b)$. □

2. We have $a + b = a'(p^{k_1}) + b'(p^{k_2})$ since $k_1 \geq k_2$. We can write that...

$$a + b = p^{k_2}(a'p^{k_1-k_2} + b')$$

. Hence, $v_p(a+b) = k_2 + v_p(a'p^{k_1-k_2})$. Clearly, the above is at least k_2. Hence $v_p(a+b) \geq k_2 = min(v_p(a), v_p(b))$ since we assumed that $v_p(a) \leq v_p(b)$. □

3. Since we have $v_p(a) \neq v_p(b)$ then we know that $k_1 > k_2$. Thus $a'({p_1}^{k_1-k_2}) + b' \equiv 0 + b' \equiv b'$ (mod p). Hence $p \nmid a'({p_1}^{k_1-k_2} + b'$ so we can write $v_p(a+b) = k_2 = v_p(b) = min(v_p(a), v_p(b)$ since we assumed that $v_p(a) \leq v_p(b)$. □

Proposition 2.4.2: The following properties regarding $| \cdot |_p$ are true.

1. $|a|_p \geq 0$
2. $|a+b|_p \leq \max(|a|, |b|)$
3. $|ab|_p = |a|_p|b|_p$

Proof. 1. We have $| a |_p = p^{-v_p(a)}$. We have $p^{-v_p(a)} = 0$ only when $v_p(a) = \infty$ which only happens when $a = 0$. □

2. We have $| a + b |_p = p^{-v_p(a+b)} \leq p^{-min(v_p(a), v_p(b)} = p^{max(-v_p(a), -v_p(b))}$ since $v_p(a+b) \geq min(v_p(a), v_p(b)$. Thus, $| a + b |_p \leq max(| a |)$. □

3. We have...

$$| ab |_p = p^{-v_p(ab)} = p^{-v_p(a)-v_p(b)} = p^{-v_p(a)}p^{v_p(b)} = | a |_p | b |_p$$

□

Proposition 2.5: Show that $\mathbb{Q}$ is a metric space over d_p where d_p is defined as $\mathbb{Q} \times \mathbb{Q} \to \mathbb{R}$: $d(x, y) =\mid x - y \mid_p$.

Proof. In order to prove this, we must prove it for all the properties of a metric space.

1. $d_p(x, y) =\mid x - x \mid_p=\mid 0 \mid_p= 0$.

2. $d_p(x, y) =\mid x - y \mid_p> 0$ from above.

3. $d_p(x, z) =\mid x - z \mid_p=\mid (x - y) + (y - z) \mid_p$. By property 2 in Proposition 2.4.2 above, $\mid (x-y)+(y-z) \mid_p\leq max(\mid x-y \mid_p, \mid y-z \mid_p) \leq\mid x-y \mid_p + \mid y-z \mid_p$. Hence $d(x, z) \leq d(x, y)+d(y, z)$.

4. $d_p(x, y) =\mid x - y \mid_p=\mid y - x \mid_p$.

Thus, $\mathbb{Q}$ is a metric space over d_p. □

Remark 1: In fact we can prove a stronger statement about the metric space d_p over $\mathbb{Q}$, namely that it is "ultrametric", i.e. it satisfies the Strong Triangle Inequality that $d_p(x, z) \leq \max(d_p(x, y), d_p(y, z))$:

This follows directly from $|a+b|_p \leq \max(|a|, |b|)$, as we have $|(x-y)+(y-z)| \leq \max(|x-y|, |y-z|)$, and thus $|x - z| \leq \max(|x - y|, |y - z|) \implies d_p(x, z) \leq \max(d_p(x, y), d_p(y, z))$.

As the p-adics exhibit this Strong Triangle Inequality, we call our metric d_p a "non-Archimedian" metric, and $| \,.\, |_p$ a "non-Archimedian" norm.

Definition 6: A sequence is called Cauchy if for any $\epsilon > 0$, there exists $N \in \mathbb{N}$ such that $n, m \geq N \to\mid a_n - a_m \mid< \epsilon$.

An example of such a sequence is the harmonic series where it's represented by $\sum_{n=1}^{\infty} \frac{1}{n}$.

Remark 2: If a_n is a Cauchy sequence, then a_n is bounded.

Proposition 2.6: Show that $\mathbb{Q}_p$ is the completion of $\mathbb{Q}$ with respect to $| \,.\, |_p$.

Proof. To show that $\mathbb{Q}_p$ is the completion of $\mathbb{Q}$, we must show that all Cauchy sequences of rationals converge to some value in $\mathbb{Q}_p$, and that for all $a \in \mathbb{Q}_p$, there exists a Cauchy sequence of rationals which converges to a.

Claim 1: For all $a \in \mathbb{Q}_p$, there exists a Cauchy sequence of rationals which converges to a.

Fix $a \in \mathbb{Q}_p$. For some $k \in \mathbb{Z}$, we may write the p-adic expansion of a to be:

$$a = p_k a^k + p_{k+1} a^{k+1} + p_{k+2} a^{k+2} + \ldots = \sum_{i=0}^{\infty} p^{k+i} a_i$$

.

Define the partial sums $S_n = \sum_{i=0}^{n} p^{k+i} a_i$, and note that $\forall n \in \mathbb{Z}_{\geq 0}$, $S_n \in \mathbb{Q}$.

Consider the sequence $(S_0, S_1, S_2, \ldots)$ in $\mathbb{Q}$. We claim that this sequence is Cauchy, and converges to a. To see that it is Cauchy, we note that $\forall \epsilon > 0$, $\exists N \in \mathbb{N}$ such that $0 < \frac{1}{p^N} < \epsilon$.

Note that $\forall m, n \in \mathbb{N}$ such that $m \geq n > N - k$, we have:

$$\begin{aligned} S_m - S_n = \sum_{i=n}^{m} p^{k+i} a_i &\implies \\ p^{k+n} | (S_m - S_n) &\implies \\ p^N | (S_m - S_n) &\implies \\ |S_m - S_n|_p \leq \frac{1}{p^N} < \epsilon \end{aligned}$$

It follows that our sequence $(S_0, S_1, S_2, \ldots)$ is Cauchy. Moreover, we claim that this sequence converges to a in $\mathbb{Q}_p$. $\forall \epsilon > 0$, $\exists N \in \mathbb{N}$ such that $0 < \frac{1}{p^N} < \epsilon$. $\forall n > N - k$, note that:

$$\begin{aligned} a - S_n = \sum_{i=n}^{\infty} p^{k+n} a_n &\implies \\ p^{k+n} | (a - S_n) &\implies \\ p^N | (a - S_n) &\implies \\ |a - S_n|_p \leq \frac{1}{p^N} < \epsilon \end{aligned}$$

Thus $(S_0, S_1, S_2, \ldots)$ is a Cauchy sequence converging to a in $\mathbb{Q}_p$.
Claim 2: Every Cauchy sequence of $\mathbb{Q}_p$ converges to some a in $\mathbb{Q}_p$.

Let $(x_1, x_2, x_3, \ldots)$ be an arbitrary Cauchy sequence of elements in $\mathbb{Q}_p$. We may write each x_i as a p-adic expansion. Let each $x_i = \sum_{j=k_i}^{\infty} p^j a_{ij}$, for some $k_i \in \mathbb{Z}$.

We note that for all $q \in \mathbb{Z}$, there exists $N_q \in \mathbb{N}$ such that the p^q coefficient of x_n for all $n > N_q$ is the same.

This is because as $(x_1, x_2, x_3, \ldots)$ is Cauchy, for all $q \in \mathbb{Z}$ there exists $N_q \in \mathbb{N}$ such that for all $m, n > N_q$:

$$\begin{aligned} |x_m - x_n|_p < \frac{1}{p^q} &\implies \\ p^q |\ x_m - x_n &\implies \\ \sum_{j \leq q} p^j(a_{mj} - a_{nj}) = 0 &\implies \\ a_{mj} = a_{nj}, \forall j \leq q & \end{aligned}$$

Specifically we obtain $a_{mq} = a_{nq}$, as desired. For each $q \in \mathbb{Z}$, let b_q be the unique coefficient of p^q for which there exists $N_q \in \mathbb{N}$ such that all x_n with $n > N_j$ have a p^q coefficient of b_j. Take $a \in \mathbb{Q}_p$ such that the p^q coefficient of a is b_q. We claim that a is the limit of $(x_1, x_2, x_3, \ldots)$.

$\forall \epsilon > 0$, $\exists M \in \mathbb{N}$ such that $0 < \frac{1}{p^M} < \epsilon$. Take $N \in \mathbb{N}$ to be the maximum of N_q, for all $q \leq M$. Note that $\forall n > N$, x_n has p^j coefficients of b_j for all $j \leq M$. It follows that $\forall n > N$:

$$\begin{aligned} p^M |\ (a - x_n) &\implies \\ |a - x_n|_p \leq \frac{1}{p^M} &< \epsilon \end{aligned}$$

Thus $(x_1, x_2, x_3, \ldots)$ converges to $a \in \mathbb{Q}_p$, as desired.

Combining our two claims, it follows that $\mathbb{Q}_p$ is the completion of $\mathbb{Q}$. □

Proposition 2.7: For $a \in \mathbb{Q}_p$, we may write a as $a_k p^k + a_{k+1} p^{k+1} + \ldots$, for some $k \in \mathbb{Z}$. Show that a is rational if and only if the sequence (a_i) is eventually periodic.

Proof. We start with the backwards direction. Suppose past some $j \in \mathbb{Z}$, (a_i) is periodic, repeating every q terms. Let $c = \sum_{i=k}^{j} a_i p^i$. We have that $a = c + a_{j+1}p^{j+1} + a_{j+2}p^{j+2} + \ldots + a_{j+q}p^{j+q} + \ldots$, and thus $a = c + p^{j+1}(a_{j+1}p^{j+1} + a_{j+2}p^{j+2} + \ldots + a_{j+q}p^{j+q})(\frac{1}{1-p^q})$. As this expression clearly evaluates to some rational number, it follows that $a \in \mathbb{Q}$.

For the forwards direction, consider some $a \in \mathbb{Q}$. Let $a = \frac{b}{c}$, for $b, c \in \mathbb{Z}$ such that $c \neq 0$, $(b, c) = 1$. Take $c = p^{v_p(c)}c'$. It suffices to show that $a' = \frac{b}{c'}$ is eventually periodic, as we may simply divide by $p^{v_p(c)}$ (i.e. shift our summation $v_p(c)$ places to the left) to obtain the expansion of a. We may write $a' = d + e$, for some $d \in \mathbb{Z}$, $e \in \mathbb{Q}$ such that $-1 \leq e < 0$. d has a finite p-adic expansion, and thus to show that a' is eventually periodic it suffices to show e is eventually periodic.

If $e = -1$, this claim is immediate. Otherwise, let $e = \frac{x}{y}$, for $x \in \mathbb{Z}$, $y \in \mathbb{N}$ such that $(x, y) = 1$. Note that $p \nmid y$, as we have extracted all factors of p from the denominator of a in defining a'.

Note that $p^{\phi(y)} \equiv 1 \bmod y \implies y|(p^{\phi(y)} - 1)$. Let $q \in \mathbb{N}$ be such that $yq = p^{\phi(y)} - 1$. Then we have that:

$$\frac{x}{y} = \frac{xq}{yq} = \frac{xq}{p^{\phi(y)} - 1} = \frac{-xq}{1 - p^{\phi(y)}} = (-xq)(1 + p^{\phi(y)} + p^{2\phi(y)} + \ldots)$$

.

Note that $-1 < \frac{x}{y} < 0 \implies 0 < -xq < yq \implies 0 < -xq < p^{\phi(y)} - 1$. Thus the p-adic expansion of $-xq$ has somewhere between 1 and $\phi(y) - 1$ digits, and it follows that our expression for $\frac{x}{y}$ is periodic every $\phi(y)$ terms. (It should be noted that, in fact, $\frac{x}{y}$ will be periodic every n terms, where n is the least natural number such that $p^n \equiv 1 \bmod y$.)

Thus e has a periodic p-adic expansion, which we have demonstrated suffices to show that a has a periodic p-adic expansion, as desired. □

3 Power Series in p-adics

Lemma 3: Let $(a_n)_{n\geq 0}$ be a sequence in $\mathbb{Q}_p$. Then if $|a_{n+1} - a_n|$ converges to 0 in $\mathbb{Q}_p$, $(a_n)_{n\geq 0}$ is a Cauchy sequence.

Proof. For all $\epsilon > 0$, $\exists N$ such that $\forall n > N$, $|a_{n+1} - a_n| < \epsilon$. Then $\forall m, n > N$ we have:

$$|a_m - a_n| = |(a_m - a_{m-1}) + (a_{m-1} - a_{m-2}) + \ldots + (a_{n+1} - a_n)|$$

$$\leq \max\left(|a_m - a_{m-1}|, |a_{m-1} - a_{m-2}|, \ldots, |a_{n+1} - a_n|\right) < \epsilon$$

by the Strong Triangle Inequality. Thus $(a_n)_{n\geq 0}$ is Cauchy, as desired. □

Note: This is an especially neat property of the p-adic numbers which interestingly does not hold for the absolute value we define over the reals. Consider the sequence $(a_n)_{n\geq 1}$ in $\mathbb{R}$ given by $a_n = \ln(n)$. We have that:

$$\lim_{n\to\infty} |a_{n+1} - a_n| = \lim_{n\to\infty} |\ln\left(\frac{n+1}{n}\right)| = \ln(1) = 0$$

.

However, we note that $(a_n)_{n\geq 1}$ is not Cauchy, as for all $n \in \mathbb{N}$, $|a_{2n} - a_n| = \ln(2)$, and thus there is no point past which our terms become arbitrarily close. □

Definition 7: Let $(a_n)_{n\geq 0}$ be a sequence in $\mathbb{Q}_p$. Define the sequence $(S_i)_{i\geq 0}$ of partial sums $S_i := \sum_{j\leq i} a_j$. We say that the series $\sum_{n\geq 0} a_n$ converges to $a \in \mathbb{Q}_p$ if $(S_i)_{i\geq 0}$ converges to a in $\mathbb{Q}_p$.

Proposition 3.1: Let $(a_n)_{n\geq 0}$ be a sequence in $\mathbb{Q}_p$. Show that $\sum_{n\geq 0} a_n$ converges in $\mathbb{Q}_p$ if and only if the sequence $(a_n)_{n\geq 0}$ converges to 0 in $\mathbb{Q}_p$.

Proof. We start with the forwards direction. Suppose $\sum_{n\geq 0} a_n$ converges to a in $\mathbb{Q}_p$. By definition, this implies that the sequence $(S_i)_{i\geq 0}$ converges to a in $\mathbb{Q}_p$. Thus for all $\epsilon > 0$, $\exists N$ such that $\forall n > N$, $|S_n - a| < \epsilon$. Then we obtain:

$$|a_{n+1} - 0| = |S_{n+1} - S_n| = |(S_{n+1} - a) - (S_n - a)| \leq \max\left(|S_{n+1} - a|, |S_n - a|\right)$$

Where the last step follows from the Strong Triangle Inequality. Noting that $|S_n - a| < \epsilon$, and $|S_{n+1} - a| < \epsilon$, it follows that $|a_{n+1} - 0| < \epsilon$, and thus $(a_n)_{n\geq 0}$ converges to 0 in $\mathbb{Q}_p$.

For the backwards direction, suppose $(a_n)_{n\geq 0}$ converges to 0 in $\mathbb{Q}_p$. We demonstrate that $(S_i)_{i\geq 0}$ is a Cauchy sequence.

We have that for all $\epsilon > 0$, $\exists N$ such that $\forall n > N$, $|a_n - 0| < \epsilon$. Noting that $S_{n+1} - S_n = a_{n+1}$, we have that $|S_{n+1} - S_n| < \epsilon$. Thus $|S_{n+1} - S_n|$ converges to 0 in $\mathbb{Q}_p$. By Lemma 1, it follows that $(S_i)_{i\geq 0}$ is Cauchy, and thus converges in $\mathbb{Q}_p$ by the notion of completion. □

Definition 8: We define the radius of convergence of $\sum_{n\geq 0} a^n x^n$ to be the value r so that the sequence $\mid a^n \mid_p c^n$ converges to 0 for all $c < r$ and does not converge for $c > r$. The following reuslt is fundamental.

Proposition 3.2: Show that the radius of convergence r of a power series $\Sigma_{n\geq 0} a_n x^n$, is equal to $(\limsup |a_n|^{\frac{1}{n}})^{-1}$

Proof. **Claim:** $\Sigma_{n\geq 0} a_n x^n$ converges if $|x| < r$

We start by dividing our proof into three cases: $r = 0$, $r = \infty$, and $r \in (0, \infty)$

Our first case is when $r = 0$. Our goal is to show that $f(x)$ doesn't converge for $x \neq 0$ in $\mathbb{Q}_p$. For $r = 0$, we have $\overline{\lim}_{n\to\infty} |a_n|^{\frac{1}{n}} = \infty$, so we know that some sub-sequence of $\sqrt[n]{|a_n|}$ approaches ∞. For $x \in \mathbb{Q}_p - \{0\}$, we want to prove that $f(x)$ isn't convergent.

If $x \neq 0$, then $|x| > 0 \Rightarrow \sqrt[n]{|a_n|} > \frac{1}{|x|}. \Rightarrow |a_n x^n| > 1$ for infinitely many n.
Therefore, since $\Sigma_{n\geq 0} a_n x^n$ doesn't converge because the general sum never approaches zero.

The second case is when $R = \infty$. Our goal for this case is to show that $f(x)$ converges $\forall x \in \mathbb{Q}_p$. $(\limsup |a_n|^{\frac{1}{n}})^{-1} = 0$ so $|a_n|^{\frac{1}{n}} = 0$. We know that the convergence $f(x), x = 0$ (Case 1) is obvious, so for $x \in \mathbb{Q}_p$, we have:

$$|a_n|^{\frac{1}{n}} < \frac{1}{2|x|} \text{ for } n \geq 0 \text{ implies } |a_n x^n| < \frac{1}{2^n} \text{ for sufficiently large}$$

Therefore, by the convergence of $\Sigma|\frac{1}{2n}|$ in $\mathbb{R}$ implies the convergence of $\Sigma a_n x^n$

The third case is when $r \in [0, \infty]$. Our goal is to show that $\forall\, r$ in the range $[0, \mathbb{R}]$, $|a_n|^{\frac{1}{n}}$ converges.

$$0 < |x| < \mathbb{R} \Rightarrow 0 < \frac{1}{r} = (\limsup{}_{n\to\infty} |a_n|^{\frac{1}{n}})$$

We know that there is a value ϵ, $0 < \epsilon < 1$, such that $\frac{1}{r} < \frac{1-\epsilon}{|x|}$. Therefore, $\limsup{}_{n\to\infty} |a_n|^{\frac{1}{n}} < \frac{1-e}{|x|} \Rightarrow |a_n x^n| < (1-\epsilon)^n$ for n sufficiently large. Because $\Sigma_{n\geq 0}(1-\epsilon)^n$ in r converges, by the comparison test, $\Sigma_{n\geq 0}|a_n x^n|$ converges in $\mathbb{Q}_p$. □

Proposition 3.3: Show that the function obtained above $f : D(0; r^-) \to \mathbb{Q}_p$ is continuous. Here $D(0; r^-)$ is the open disc of radius r centered at 0. That is, it contains all elements whose absolute value is less than r.

Proof. We first prove a lemma which states that if $f = \sum_{n\geq 0} a_n x^n$ converges on a closed disc of radius r nonzero, then it is uniformly continuous and bounded on such disc. Recall a function is uniformly continuous on some set A if for every $\epsilon > 0$, there exists a $\delta > 0$ such that for all $x, y \in A$ with $|x - y| \leq \delta$, we have $|f(x) - f(y)| \leq \epsilon$.

Suppose f converges at some x_0 such that $|x_0| = r$, then by Proposition 3.1, we have $|a_n x_0^n| = |a_n|r^n \to 0$ as $n \to \infty$. For x, y in the closed disc, we have $f(x) - f(y) = (x - y)\sum_{n\geq 1} a_n(x^{n-1} + x^{n-2}y + \cdots + y^{n-1})$. Using properties as an ultrametric, we obtain the bound $|\sum_{n\geq 0} a_n(x^{n-1} + x^{n-2}y + \cdots + xy^{n-2} + y^{n-1})| \leq \max_{n\geq 1} |a_n|r^{n-1} = C$, where the existence of maximum is implied by the convergence of $|a_n|r^n$.

If all coefficients except a_0 are zero, then f is constant, and obviously uniformly continuous. If some $a_n, n \geq 1$ is nonzero, then $C > 0$. Set $\delta = \frac{\epsilon}{C}$, and for all $|x - y| < \delta$, we have $|f(x) - f(y)| < \frac{\epsilon}{C}C = \epsilon$, and we are done.

If the series only converges at 0, then continuity is clear. Suppose it converges on an open disc of radius r, and let x_0 be an element in the open disc. Then $|x_0| = r_0 < r$, so f converges on the closed disc of radius r_0, so f is uniformly continuous on such closed disc, which implies continuity. Since $r_0 < r$ is arbitrary, this completes the proof. □

3.1 The p-adic exponential and logarithm

Definition 9: Let $\exp(x)$ be the formal power series, $\exp(x) = \sum_{n\geq 0} \frac{(x)^n}{n!}$ in the ring $\mathbb{Q}_p[[x]]$.

Definition 10: We define a closed disc of radius r and center a to be the set $D(a; r) := z \in \mathbb{Q}_p :| z - a |_p \leq r$ and an open disc of radius r, centered at a to be the set $D(a; r^-) := z \in \mathbb{Q}_p :| z - a |_p < r$.

Now consider $f(x) = \sum_{n=0}^{\infty} a_n x^n \in \mathbb{Q}_p[[x]]$. Therefore, we can define a function $f : D(0; r^-) \to \mathbb{Q}_p$ so that for any $t \in D(0; r^-)$ we have...

$$f(t) = \sum_{n=0}^{\infty} a_n t^n$$

Definition 11: We say that a function is continuous $f : S \to \mathbb{Q}_p$ at a point $x \in S$, if for all $\epsilon \in R^+$, there exists some positive δ, where $| x - y |_p < \delta$ and $| f(x) - f(y) |_p < \epsilon$.

Definition 12: We define $\exp(x)$ to be the formal power series $\sum_{i\geq 0} \frac{x^i}{i!}$ in the ring $\mathbb{Q}_p[[x]]$.

Proposition 3.1.1: For $a, b \in D(0; p^{\frac{-1}{p-1}})$ we have that $a + b \in D(0; p^{\frac{-1}{p-1}})$ and furthermore $exp(a + b) = exp(a) \cdot exp(b)$.

Proof. So we need to use formal power series to prove this p-adically. We know that $\sum_{i=0}^{l} \frac{(a+b)^n}{n!}$, so we can use the binomial theorem where we have $(a + b)^n$, so we $\sum n \sum_{k=0}^{l} \binom{n}{k} \cdot a^{n-k}b^k$ which is true from the Binomial Theorem, and we know that the binomial coefficients are $\binom{n}{k} = \frac{n!}{(n-k)!k!}$.

So the n!'s cancel, and then we get $\sum_{n\geq 0}\sum_{k=0}^{l}\frac{a^{n-k}b^k}{k!(n-k)!}$, where it's $\sum_{n\geq 1}\sum_{k=0}^{l}\frac{a^{n-k}}{(n-k)!}\cdot\frac{b^k}{k!}$ which is what we desired. □

Corollary 1: $exp(na) = (exp(a))^n$ for all integers n and $a \in D(0; p^{\frac{-1}{p-1}})$.

Proof. This follows directly from the previous proposition by induction. □

Proposition 3.5b: Show that the radius of convergence of $\exp(x)$ is $p^{\frac{-1}{p-1}}$.

Lemma 4: $v_p(n!)$ is equivalent to $\frac{n-s_p(n)}{p-1}$ where $s_p(n)$ is the sum of the digits of n in base p.

Proof. So we can write that $v_p(n!) = \sum_{i=0}^{l}\lfloor\frac{n}{p^i}\rfloor$. Let $n = n_lp^l + n_{l-1}p^{l-1} + \ldots n_{i+1}p + n_i$ be the base p representation of n. We know that $\frac{n}{p^i}$ is the same as $\sum_{i=1}^{l}(n_lp^{l-i} + \ldots + n_{i+1}p + n_i)$ as we just apply a factor of p^{-i} to the base p representation. This sum can be turned into a double summation. $\sum_{j=1}^{l}\sum_{i=1}^{j}n_j(p^{j-i}) = \sum_{j=1}^{l}n_j(\frac{p^j-1}{p-1})$. Since $\frac{1}{p-1}$ is a constant, we can write our sum as...

$\frac{1}{p-1}\sum_{j=1}^{l}n_j(p^j - 1)$ which is equivalent to $\frac{1}{p-1}\sum_{j=1}^{l}n_j(p^j) - \frac{1}{p-1}\sum_{j=1}^{l}n_j = \frac{n-s_p(n)}{p-1}$ where $s_p(n) = \sum_{j=1}^{l}n_j$ is the sum of the digits of n in base p. □

Now we continue by using Proposition 3.2, which states the radius of convergence for a power series. We want to find that $\lim_{n\to\infty}p^{\frac{v_p(n!)}{n}}$ just plugging in $n!$ into the radius of convergence formula.

We need to know $v_p(n!)$. From Lemma 2, we can say that $v_p(n!) = \frac{n-s_p(n)}{p-1}$. So, $v_p(n!) < \frac{n}{p-1}$. So $\frac{v_p(n!)}{n} < \frac{1}{p-1}$. Thus, $p^{\frac{v_p(n!)}{n}} < p^{\frac{1}{p-1}}$. □

Proposition 3.1.2: Show that $\mid exp(a) - exp(b) \mid = \mid a - b \mid$ for all $a, b \in D(0; p^{\frac{-1}{p-1}})$.

Proof. So we can write $\mid exp(x) - exp(y) \mid$ as $\mid \sum_{n=1}^{\infty}\frac{a^i}{i!} - \sum_{n=1}^{\infty}\frac{b^i}{i!} \mid$. If we write out all the terms then we have...

$$\mid \sum_{n=1}^{\infty}(\frac{a}{1} + \frac{a^2}{2!} + \frac{a^3}{3!}...) - \sum_{n=1}^{\infty}(\frac{b}{1} + \frac{b^2}{2!} + \frac{b^3}{3!}...) \mid$$

We can group the terms together and we get...

$$\mid \sum_{n=1}^{\infty}(\frac{a-b}{1} + \frac{a^2-b^2}{2!} + \frac{a^3-b^3}{3!} + ...) \mid$$

We know that $a^n - b^n$ can be factored as $(a-b)(a^{n-1} + a^{n-2}b + ...)$, so we can factor out $(a-b)$ as the GCD of all the factors. That means the p-adic evaluation of the whole summation is the p-adic evaluation of the GCD, which in this case is $(a-b)$ so we are done. □

Definition 10: We have the formal power series as follows, $log(1-x) = -\sum_{n=1}^{\infty} \frac{x^n}{n}$ and $log(1+x) = \sum_{n=1}^{\infty}(-1)^{n+1}\frac{x^n}{n}$

Theorem 3: Let $\lim_{x\to\infty} \mid \frac{a_{n+1}}{a_n} \mid =$ L. If $L < 1$, then $\sum_{n=1}^{\infty} \mid a_n \mid$ is absolutely convergent.

Proof. Let's assume that there is some r, where $L < r < 1$, where $\mid \frac{a_{n+1}}{a_n} \mid < r$, so we have that $\mid a_{n+1} \mid = r \mid a_n \mid$. Let's consider the following.

$$\mid a_{n+1} \mid < r \mid a_n \mid$$

$$\mid a_{n+1} \mid < r \mid a_n < r^2 a_n$$

$$\mid a_{n+2} \mid < r \mid a_{n+1} < r^3 a_n$$

$$...$$

$$\mid a_{n+k} \mid < r \mid a_{n+k-1} \mid < r^k \mid a_n \mid$$

So this means that we can just look at the following series, $\sum_{n=1}^{\infty} \mid a_n \mid r^k$ and use a comparison test. This is a geometric series because $0 < r < 1$ and since we know that $\mid a_{n+k} \mid < r^k \mid a_n \mid$.

As we stated above, $\sum_{n=1}^{\infty} \mid a_n \mid$ is convergent to L, and we can truncate the series so it's equivalent to $\sum_{n=N+1}^{\infty} \mid a_n \mid$ which means that this is convergent. So by comparison test, we have that $\lim_{x\to\infty} \mid \frac{a_{n+1}}{a_n} \mid < 1$ means the series converges. □

Proposition 3.1.3: The radius of convergence of $log(x+1)$ is 1. In particular, log defines a continuous function: $1 + p(\mathbb{Z})$ to the evaluation of the power series x $\in 1 + p\mathbb{Z}$.

We can use Theorem 1, where we have that $\lim_{x\to\infty} \mid \frac{a_{n+1}}{a_n} \mid$ is $\lim_{x\to\infty} \mid \frac{x^{n+1}}{n+1} \cdot \frac{n}{x^n} \mid$, and since the coefficients of $n+1$ and n are the same, then we have that the limit is 1. Formally, $\mid x \mid < 1$ because $\mid x \mid$ is a constant. □

Proposition 3.1.4: *$log(ab) = log(a) + log(b)$.*

Proof. The partial derivative of log(ab) with respect to a is $\frac{1}{ab} \cdot b = \frac{1}{a}$, by chain rule. The RHS derivative is also $\frac{1}{a}$, thus since the derivatives are equal then the functions differ by some constant.

Thus, we have $log(ab) = log(a) + log(b) + C$ for some constant C. Utilizing Definition 2, we know that $log(ab) = -\sum_{n=1}^{\infty} \frac{(ab-1)^n}{n}$. If we factor out b^n, then we get $\sum_{n=1}^{\infty}(-1)^{n+1}\frac{b^n(a-\frac{1}{b})^n}{n}$. We have $log(a) + log(b) = log(b) + \sum_{n=1}^{\infty}(-1)^{n+1}\frac{(a-1)^n}{n}$. So we notice that one series is centered at 1 and the other at $\frac{1}{b}$. We treat b as a constant since we considered it so when we took the partial derivative. □

Lemma 5: If two power series on a disc of positive radius in K have the same derivative differ by a constant on that disc.

Proof. If $f(x) = \sum_{n=1}^{\infty} a_n x^n$ and $g(x) = \sum_{n=1}^{\infty} b_n x^n$ and $f'(x) = g'(x)$ and so $f^n(x) = g^n(x)$ which means that $\frac{f^n(x)}{n!} = \frac{g^n(x)}{n!}$ so the only difference between their power series are their constant terms. □

From Lemma 5, the centers on the series don't matter, and then we can say that $log(xy)$ and $log(x) + log(y)$ only differ by a constant. □

Proposition 3.1.5: $exp(a) \in D(0; p^{\frac{-1}{p-1}})$ and that exp(x) and log(x) are mutually inverse isomorphisms of groups between the group $D(0; p^{\frac{-1}{p-1}})$ under addition and the multiplicative group $D(1; p^{\frac{-1}{p-1}})$.

This means that we want to show $exp(log(1 + x)) = 1 + x$ and $log(exp(x)) = x$. We see that $\frac{d}{dx}(e^{log(1+x}) = \frac{1}{1+x} \cdot e^{log(1+x}$. Generally, we see that $(1+x) \cdot \frac{d}{dx}(f(x)) = f(x)$. Let's make a function $f(x) = \sum_{n=1}^{\infty} a_n x^n$. We can write...

$$(1 + x) \cdot \sum_{n=1}^{\infty} a_n \cdot nx^{n-1} = \sum_{n=1}^{\infty} a_n \cdot x^n$$

On the LHS, we have $a_1 + (a_1 + a_2)x + (2a_2 + 3a_3)x^2 + ...$ On the RHS, we have that $a_0 + a_1 x + (a_2)^2 x^2$... Equating coefficients we get that...

$$a_0 = a_1$$
$$a_1 + 2a_2 = a_1$$
$$2a_2 + 3a_3 = (a_2)^2$$
$$...$$

This means, $a_2 = a_3 = a_4 = ... = 0$. Only the constant terms are equal, which is what we want. This implies that any expression satisfying $f(x)$ is a constant multiple $(1 + x)$.

Now, we prove the other way, that $log(exp(a)) = a$. The proof is analogous. □

4 The Artin Hasse Exponential

Definition 11: We define the Artin-Hasse exponential $E(x) = \exp\left(\sum_{n\geq 0} \frac{x^{p^n}}{p^n}\right) = \exp\left(x + \frac{x^p}{p} + \frac{x^{p^2}}{p^2} + \dots\right)$

4.1 Integrality of $E(x)$

The goal is to prove that $E(x) \in \mathbb{Z}_p[[x]]$ or that the coefficients of the Artin Hasse Exponential are contained in $\mathbb{Z}_p$. Although, we need an essential lemma, and we will show a novel proof for it using induction.

Dwork's Lemma: Let $f(x) \in 1 + x\mathbb{Q}_p[[x]]$ be a power series with p-adic rational coefficients. Then $f(x) \in 1 + x\mathbb{Z}_p[[x]] \iff \frac{f(x^p)}{f(x)^p} \in 1 + px\mathbb{Z}_p[[x]]$.

Proof. For the forward direction, note that due to the multinomial theorem we have that for $f(x) \in 1 + x\mathbb{Z}_p[[x]]$, $f(x)^p \equiv f(x^p) \bmod p$. As $f(x^p)$ has a constant coefficient of 1, we note that $f(x^p)$ is invertible, and thus it follows that $\frac{f(x^p)}{f(x)^p} \in 1 + px\mathbb{Z}_p[[x]]$, as we note that the quotient of these power series is 1 mod p, and has constant term 1.

For the other direction, we proceed by induction. Suppose for some $f(x) \in 1 + x\mathbb{Q}_p[[x]]$, we have that $\frac{f(x^p)}{f(x)^p} \in 1 + x\mathbb{Z}_p[[x]]$, and thus there exists $g(x) \in 1 + px\mathbb{Z}_p[[x]]$ such that $f(x^p) = f(x)^p \cdot g(x)$.

For the base case of our induction, we note that the constant term of our polynomial must be 1 by the assumption that $f(x) \in 1 + x\mathbb{Q}_p[[x]]$. Note that $1 \in \mathbb{Z}_p$.

For the inductive step, suppose for some $N > 1$, we have that for all $n \in \mathbb{N}$ such that $n < N$, the x^n coefficient of $f(x)$ is in $\mathbb{Z}_p$.

Firstly, we claim that the Nth coefficient of $f(x)^p \cdot g(x)$ is congruent to the Nth coefficient of $(\sum_{n \leq N} a_n x^n)^p$ in $\mathbb{Z}_p$. We note that as $f(x)$ has no coefficients of negative x powers, we can truncate $f(x)$ up to the Nth term when we are considering just the coefficient of x^N. So the Nth coefficient of $f(x)^p \cdot g(x)$ is congruent to that of $(\sum_{n \leq N} a_n x^n)^p \cdot g(x)$. As $g(x) \in 1 + px\mathbb{Z}_p[[x]]$, it follows that the Nth coefficient of $f(x)^p \cdot g(x)$ is congruent to that of $(\sum_{n \leq N} a_n x^n)^p$ in $\mathbb{Z}_p$, as desired.

Now we show that a_N is in $\mathbb{Z}_p$, considering two cases:

Case 1: $p \not| N$

Recall $f(x^p) = f(x)^p \cdot g(x)$. Note that if $p \not| N$, the coefficient of x^N on the LHS is 0. Thus we have that 0 is equivalent to the x^N coefficient of $(\sum_{n \leq N} a_n x^n)^p$ in $\mathbb{Z}_p$. To form a term of x^N from $(\sum_{n \leq N} a_n x^n)^p$, we can combine the $a_N x^N$ term in $(\sum_{n \leq N} a_n x^n)$ with $p - 1$ other constant terms $a_0 = 1$, in p ways.

All other ways to combine terms of $(\sum_{n \leq N} a_n x^n)^p$ to yield an x^N coefficient do not involve a term of $a_N x^N$, and by our inductive hypothesis are comprised only of a product of coefficients in $\mathbb{Z}_p$. By the multinomial theorem, each of these terms occurs with a coefficient divisible by p, and thus we may equate coefficients on the left and right hand sides to write that $0 = pa_N + c$ in $\mathbb{Z}_p$, for some $c \in p\mathbb{Z}_p$. Thus it must be that $a_N \in \mathbb{Z}_p$, completing our inductive hypothesis in this case.

Case 2: $p|N$

Once again, consider $f(x^p) = f(x)^p \cdot g(x)$. Note that the x^N coefficient on the LHS is $a_{\frac{N}{p}}$. On the right hand side, the x^N coefficient is equivalent to that of $(\sum_{n \leq N} a_n x^n)^p$ in $\mathbb{Z}_p$. We note that we can form an x^N term by combining n terms of $a_{\frac{N}{p}} x^{\frac{N}{p}}$.

We can also form such a term by taking the $a_N x^N$ term in $(\sum_{n \leq N} a_n x^n)$ with $p-1$ other constant terms $a_0 = 1$, in p ways. By our inductive hypothesis, we note that all other terms of x^N are comprised only of a product of coefficients in $\mathbb{Z}_p$. By the multinomial theorem, each of these terms occurs with a coefficient divisible by p. Equating coefficients on the left and right, we have $a_{\frac{N}{p}} = a^p_{\frac{N}{p}} + pa_N + c$ in $\mathbb{Z}_p$, for some $c \in p\mathbb{Z}_p$.

By our inductive hypothesis we have that $a_{\frac{N}{p}} \in \mathbb{Z}_p$, and thus $a^p_{\frac{N}{p}} = a_{\frac{N}{p}}$ in $\mathbb{Z}_p$ by Fermat's Little Theorem in $\mathbb{Z}_p$. So we have that $a_{\frac{N}{p}} = a_{\frac{N}{p}} + pa_N + c$ in $\mathbb{Z}_p$, and thus $0 = pa_N + c$ in $\mathbb{Z}_p$, which implies $a_N \in \mathbb{Z}_p$, as $c \in p\mathbb{Z}_p$. This completes our inductive hypothesis in this case.

Combining cases 1 and 2, we have completed our inductive step, and thus we have that for all $n \in \mathbb{N}$, $a_n \in \mathbb{Z}_p$. As $a_0 = 1$, it follows that $f(x) \in 1 + x\mathbb{Z}_p[[x]]$, completing our backwards direction. □

Proposition 4.1: $\exp(-px) \in 1 + px\mathbb{Z}_p[[x]]$

Proof. We have that $\exp(-px) = \sum_{n \geq 0} \frac{(-px)^n}{n!} = 1 + \sum_{n \geq 1} \frac{(-px)^n}{n!}$.

For $n \geq 1$, recall that $v_p(n!) = \left(\frac{n - s_p(n)}{p-1}\right)$, where $s_p(n)$ is the sum of the digits of n in base p. Thus, $v_p(\frac{(-p)^n)}{n!}) = n - \left(\frac{n - s_p(n)}{p-1}\right) > n - \left(\frac{n}{p-1}\right) = \frac{n(p-2)}{(p-1)} \geq 0$, and so $v_p(\frac{(-p)^n)}{n!}) \geq 1$, from which we obtain $\sum_{n \geq 1} \frac{(-px)^n}{n!} \in px\mathbb{Z}_p[[x]]$. Thus $\sum_{n \geq 0} \frac{(-px)^n}{n!} \in 1 + px\mathbb{Z}_p[[x]] \implies \exp(-px) \in 1 + px\mathbb{Z}_p[[x]]$ □

Proposition 4.2: $\frac{E(x^p)}{E(x)^p} = \exp(-px)$.

Proof.

$$E(x)^p = \left(\exp\left(\sum_{n \geq 0} \frac{x^{p^n}}{p^n}\right)\right)^p = \exp\left(p \sum_{n \geq 0} \frac{x^{p^n}}{p^n}\right) = \exp\left(px + p \sum_{n \geq 1} \frac{x^{p^n}}{p^n}\right) = \exp(px) \cdot \exp\left(\sum_{n \geq 1} \frac{x^{p^n}}{p^{(n-1)}}\right)$$

$$= \exp(px) \cdot \exp\left(\sum_{n \geq 0} \frac{x^{p^{(n+1)}}}{p^n}\right) = \exp(px) \cdot \exp\left(\sum_{n \geq 0} \frac{(x^p)^{p^n}}{p^n}\right) = \exp(px) \cdot E(x^p)$$

.

It follows that $\frac{E(x^p)}{E(x)^p} = \frac{1}{\exp(px)} = \exp(-px)$, as desired. □

Corollary: $E(x) \in \mathbb{Z}_p[[x]]$

As we have shown that $\exp(-px) \in 1 + px\mathbb{Z}_p[x]$, it follows that:

$$\frac{E(x^p)}{E(x)^p} = \exp(-px) \implies \frac{E(x^p)}{E(x)^p} \in 1 + px\mathbb{Z}_p[[x]]$$

. By Dwork's Lemma we have that $E(x) \in 1 + x\mathbb{Z}_p[[x]]$, and thus $E(x) \in \mathbb{Z}_p[[x]]$. □

4.2 Radius of Convergence

Proposition 4.3: The radius of convergence of $E(x)$ is 1.

Lemma 6: We can write $e^x = \prod_{n\geq 1}(1-x^n)^{\frac{\mu(n)}{n}}$ where $\mu(n)$ is the mobius function.

Proof. Let's write...

$$log \prod_{n=1}^{\infty}(1-x^n)^{\frac{-\mu(n)}{n}} = \sum_{n=1}^{\infty} \frac{-\mu(n)}{n} log(1-x^n) = \sum_{n=1}^{\infty} \frac{\mu(n)}{n} \sum_{k=1}^{\infty} log(1-x^k) =$$

$$\sum_{n=1}^{\infty} \frac{\mu(n)}{n} \sum_{k=1}^{\infty} \frac{x^{nk}}{k} = \sum_{m=1}^{\infty} x^m \sum_{n=0}^{\infty} \frac{\mu(n)}{m} = \sum_{m=1}^{\infty} \frac{x^m}{m} \sum_{d|m} \mu(d)$$

.

The reason the bounds are from 1 onwards, is because we have $\frac{1}{n}$ in some of our expressions which means that it would be undefined if we included 0. We know that $\sum_{d|m} \mu(d) = 1$ and so the final sum is equivalent to $-log(1-x)$. □

So we can write the below from Lemma 6.

$$e^x = \prod_{n\geq 0}(1-x^n)^{\frac{-\mu(n)}{n}}$$

$$E_p(x) = \prod_{n\geq 0, p\nmid n}(1-x^n)^{\frac{-\mu(n)}{n}}$$

The above is the representation as a formal power series. The radius of convergence of the above series is 1 from the definition of a radius of convergence. □

Remark 2: This is a stronger radius than $p^{-\frac{1}{p-1}}$, the general radius of convergence for $\exp(x)$ demonstrated in Proposition 3.5.

5 Further Research

Using all this groundwork and various proofs that were discussed in the paper, we can look into $E(\sqrt{p})$ or if $E(\sqrt{p^{\frac{a}{b}}})$ converges, which would lead into finding whether $E(\sqrt{p})$ or even just $E(p)$ is rational or irrational. For finding whether $E(\sqrt{p})$ converges or not, a new definition of the p-adic norm would have to be adapted because the regular definition is not sufficent for fractional exponents that are less than 1. Overall, this is a very interesting topic that can definitely be explored more.

6 Acknowledgements

Thank you to the PROMYS Program, Emma Knight, Abhishek Oswal, Ananth Shankar, and David Fried for providing us with this project and to Bernie Luan and John Sim for mentoring us throughout the process. We also thank the Clay Mathematical Institute for providing us with advanced seminars to broaden our knowledge and scope of the project.

7 References

[1] “p-adic Numbers: An Introduction”. Fernando Q Gouvea (1991).

[2] “p-adic Numbers, p-adic Analysis, and Zeta Functions” Second Edition. Neal Koblitz (1991).

[3] “A Course in p-adic analysis” Graduate Texts in Mathematics. Alain M Robert (2000).