The Artin Hasse Exponential and the p-adics

Niyathi Kukkapalli[1]

[1]Charter School of Wilmington, Delaware, USA

August 15th, 2023

Abstract

In 1928, the Artin-Hasse Exponential $E(x)$ was created and it's considered an analogue of the exponential function that comes from infinite products. It also has applications in formal group schemes and is studied in the p-adic number system. In this paper, fundamental results about the field of the p-adic rationals, Q_p, like completion, are proven while smaller propositions are left to the reader. The integrality of E(x) is shown using Dwork's Lemma and extensions of the Artin Hasse exponential are further discussed.

1 Introduction

$$E(x) = \exp\left(\sum_{n\geq 0} \frac{x^{p^n}}{p^n}\right) = \exp\left(x + \frac{x^p}{p} + \frac{x^{p^2}}{p^2} + \dots\right)$$

The exponential above is the Artin-Hasse Exponetial discovered by Artin and Hasse in 1928. It's a function that is a composition of two functions with p-adically large coefficents, where those coefficents are bounded. We define exp(x) as the formal power series $\sum_{n\geq 0} \frac{x^n}{n!}$ in the ring, $\mathbb{Q}_p[[x]]$. There are many interesting results regarding this exponential. For example, despite all the fractions in the exp(x) function, we can prove the integrality of the coefficents of E(x). We build up to Dwork's Lemma is proven using induction from which various corollaries arise. To lay out some groundwork, first, the p-adics have to be introduced.

2 The p-adic number system

We have to show the properties of the exp(x) and log(x) still hold in the p-adics. We define the p-adic number system as below.

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

We can write a number n as a formal power series, or as in base p in the p-adics. Notice that we cannot rigidly define the p-adics like we can do for $\mathbb{Z}$ or $\mathbb{Q}$. To write a number in the p-adics, we need to be able to find solutions to congruences mod p, p^2, p^3 and so on. Hensel's Lemma states this explicitly.

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 $a \equiv a_1 \pmod{p}$

Example 1: Consider the equation $x^2 \equiv 2 \pmod{7^n}$ in $\mathbb{Z}$. 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, $x^2 = (7k+3)^2 = 49k^2 \pm 42k + 9 \equiv \pm 7k + 9 \equiv 2 \pmod{49} \implies \pm 7k \equiv -7 \pmod{49} \implies k \equiv \pm 1 \pmod{7} \implies n \equiv 7(7k \pm 1) \pm 3 \equiv \pm 10 \pmod{49}$. Notice how the exponent is building.

Proof. 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 $a \equiv a_1 \pmod{p}$.

□

Definition 2: $\mathbb{Q}_p = \mathbb{Z}_p[\frac{1}{p}]$ 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 3: We define the p-adic absolute value (or norm) to be the function $|\,.\,|_p$: $\mathbb{Q} \to \mathbb{R}$, such that for $q \in \mathbb{Q}$, $|q|_p = p^{-v_p(q)}$, where $v_p(q)$ is the exponent of the largest power of p that divides q. This is the analogue of the absolute value in Z for the p-adics.

Proposition 1: $\mathbb{Q}_p$ is the completion of $\mathbb{Q}$ with respect to $|\cdot|$.

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 $\forall n > N$:

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

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 $\mathbb{Q}$. □

3 Radius of Convergence

We want to examine all properties of E(x), and this logically includes the radius of convergence since we are dealing with a polynomial.

Proposition 2: 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. We start by dividing our proof into three cases: $r = 0$, $r = \infty$, and $r \in (0, \infty)$

Case 1: $r = 0$. 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.

Case 2; $R = \infty$. 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 $\Sigma a_n x^n$

Case 3: $r \in [0, \infty]$. 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 $\mathbb{Q}_p$. □

3.1 The p-adic exponential and logarithm

Definition 4: We define $exp(x) = \sum_{n\geq 0} \frac{(x)^n}{n!}$ and $log(x) = \sum_{n\geq 1} \frac{(x)^n}{n}$ in the ring $\mathbb{Q}_p[[x]]$

Proposition 3: The properties listed below are true in the p-adics.
1. exp(x+y) = exp(x)exp(y)
2. exp(nx) = $exp(x)^n$
3. $|exp(x-y)|_p = |x-y|_p$

We can prove the first part of Proposition 1.

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 $\sum_{n\geq 0} \sum_{k=0}^{l} \frac{a^{n-k}}{(n-k)!} \cdot \frac{b^k}{k!}$ which is what we desire. □

Exercise 1: Prove statements 2 and 3 in Proposition 1.

Proposition 4: The radius of convergence of exp(x) is $p^{\frac{-1}{p-1}}$.

Proof. Now we continue by using Proposition 3, which states the radius of convergence for a power series. We are working in the p-adics so we will use the p-adic norm. 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 Legendre's Theorem, 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, $p^{\frac{v_p(n!)}{n}} < p^{\frac{1}{p-1}}$. □

We also want to talk about log(x), given it's not as important for our purposes. We notice that the logarithm is the inverse of the exponential, but we want to prove this.

Proposition 5: exp(x) and log(x) inverse functions of each other in the p-adics.

This means that we want to show $exp(log(x)) = x$ and $log(exp(x)) = x$. We will only prove one direction here, and the other is left as an exercise to the reader.

Proof. exp(log(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...

$$(1+x) \cdot \sum_{n=0}^{\infty} a_n \cdot n x^{n-1} = \sum_{n=0}^{\infty} a_n \cdot x^n$$

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 $(1+x)$. $\square$

4 Integrality of E(x)

Contrary to the form of E(x), the coefficents of the polynomial are integers and we can prove this fact with a powerful lemma that can be proved 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 $f(x) \in 1 + x\mathbb{Z}_p[[x]] \iff \frac{f(x^p)}{f(x)^p} \in 1 + px\mathbb{Z}_p[[x]]$.

Exercise 2: Prove the forward direction of this statement. (Hint: Utilize the generalization of Freshman's Dream)

Proof. 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 $f(x^p) = f(x)^p \cdot g(x)$.

Base Case: 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 $1 \in \mathbb{Z}_p$.

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: $p \nmid N$

Recall $f(x^p) = f(x)^p \cdot g(x)$. Note that if $p \nmid N$, 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 $a_{\frac{N}{p}} = a_{\frac{N}{p}}^p + pa_N + c$ 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 $a_{\frac{N}{p}}^p = a_{\frac{N}{p}}$ 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 6: $\exp(-px) \in 1 + px\mathbb{Z}_p[[x]]$

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

For $n \geq 1$, by Legendre's Theorem 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 7: $\frac{E(x^p)}{E(x)^p} = \exp(-px)$.

Proof. We will need to utilize some of the exponential properties listed in Proposition 3.

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

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

.

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

Corollary 1: $E(x) \in \mathbb{Z}_p[[x]]$

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 $E(x) \in \mathbb{Z}_p[[x]]$. □

4.1 Radius of Convergence of E(x)

We found that the radius of convergence of exp(x) is $p^{\frac{-1}{p-1}}$, but we can come up with a stricter radius for E(x). To do this, we will utilize a different definition of exp(x).

Definition 5: $\exp(x) = \prod_{n\geq 1}(1-x^n)^{\frac{-\mu(n)}{n}}$ then we get $E(x) = \prod_{(p,n)=1}(1-x^n)^{\frac{-\mu(n)}{n}}$

Thus, the radius of convergence of E(x) is 1 from above. We can see the above definition is true from taking the log of both sides of exp(x). From the formal power series of exp(x) we have that the radius of convergence is 1 for E(x), which is more tightly bounded then $p^{\frac{-1}{p-1}}$ (Proposition 3). To note, there are many more properties of the Artin Hasse Exponential, but many require advanced p-adic analysis to dig deeper into.

5 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).