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. This paper is part of a bigger project on The Artin Hasse Exponential.

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. In this brief article, essential knowledge about the p-adics are assumed.

2 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 1: 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 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 $n \geq 1$, 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 2: $\frac{E(x^p)}{E(x)^p} = \exp(-px)$.

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 $E(x) \in \mathbb{Z}_p[[x]]$. □

2.1 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 1: $\exp(x) = \prod_{n\geq 1}(1-x^n)^{\frac{-\mu(n)}{n}}$ 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.

3 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).