The Artin-Hasse Exponential and p-adic Numbers

Faculty Mentor: Shiang Tang
Ph.D. Mentor: Ravi Donepudi
Xiaojian Li, Jay Reiter, Napoleon Wang, Hyunjin Yi

15 May, 2021

1 Introduction

In this project, we provide an original, combinatorial proof that the Artin-Hasse exponential, $AH_p(x)$, when written as a formal power series has coefficients in a subring of p-adic integers, $\mathbb{Z}_{(p)} = \{r \in \mathbb{Q} : |x|_p \leq 1\}$. Our proof of this result begins with a counting argument on the number of continuous homomorphisms between a topological group and S_n and includes a proof of a more general result which shows the number of such continuous homomorphisms can be counted using the complete Bell polynomials.

We then use this result about coefficients of $AH_p(x)$ to construct a new, direct proof of a known fact in p-adic number theory: for every p^k root of unity ζ in $\mathbb{C}_p$, there exists α in $\mathbb{C}_p$ such that $AH_p(\alpha) = \zeta$.

This fact provides a p-adic analogue for the way we express roots of unity in the complex numbers using the ordinary exponential, e.g. $e^{2\pi ik}$. Disappointingly, in the p-adic complex numbers, the only root of unity in the image of exp is 1 [1]; however, since we show each p^k root of unity is in the image of AH_p, we have a convenient and familiar way to represent them.

1.1 Review of Relevant Topics in p-adic Number Theory

We begin with a review of relevant properties of the p-adic numbers that we will use in the proofs of our results.

Notation. *For the duration of this paper, fix p to be any prime number.*

Definition 1.1. *[2, p.11] Let x be a nonzero rational number. There exists unique integers n, s, and t with s and t not divisible by p such that*

$$x = p^n \frac{s}{t}.$$

*We define the p-**adic norm** of x to be $|x|_p := p^{-n}$.*

Notation. *For notational simplicity when it is obvious what we mean by context, we may denote the p-adic norm of a p-adic number x simply by $|x|$.*

From this definition of the p-adic norm arises a construction of the p-adic numbers, $\mathbb{Q}_p$, that we will take as a definition. We use this definition of $\mathbb{Q}_p$ to define the p-adic integers and the p-adic complex numbers.

Definition 1.2. *[2, p.12,45] Let the p-**adic numbers**, $\mathbb{Q}_p$, be the completion of $\mathbb{Q}$ with respect to the metric induced on $\mathbb{Q}$ by the p-adic norm.*

*Let the p-**adic integers**, $\mathbb{Z}_p$, be the following subset of p-adic numbers:*

$$\mathbb{Z}_p := \{x \in \mathbb{Q}_p : |x|_p \leq 1\}.$$

*Let the p-**adic complex numbers**, $\mathbb{C}_p$, be the completion of the algebraic closure of $\mathbb{Q}_p$.*

We assume that the reader is familiar with elementary properties of the p-adic numbers and p-adic complex numbers. As such, we will only outline a few theorems here which will be directly applied in our proofs below.

The first is a fundamental, though initially somewhat surprising theorem which gives us criteria for the convergence of sequences and series in the p-adic numbers:

Theorem 1.3. *[2, p.61] Let $\{a_i\}$ be a sequence in $\mathbb{Q}_p$. Then*

(i) If $\lim_{n\to\infty} a_n$ is some nonzero $a \in \mathbb{Q}_p$, there exists some $M \in \mathbb{N}$ such that $m > M$ implies $|a_m|_p = |a|_p$.

(ii) The series $\sum_{i=0}^{\infty} a_i$ converges if and only if $\lim_{n\to\infty} a_n = 0$.

Next, we note a very powerful theorem for p-adic functions which is reminiscent of the method of Newton approximation for real-valued functions.

Theorem 1.4. *[2, p.79] Let K be either $\mathbb{Q}_p$ or $\mathbb{C}_p$. Let f be a K-valued function defined on the disc $B_a(r) := \{x \in K : |x-a| < r\}$ in K. Suppose there is some $s \in K$ such that*

$$\sup\left\{\left|\frac{f(x)-f(y)}{x-y} - s\right| : x, y \in B_a(r),\, x \neq y\right\} < |s|.$$

Then $s^{-1}f$ is an isometry, and f maps discs onto discs. More precisely, for each $b \in B_a(r)$ and $r_1 \in (0, r]$, f maps the disc $B_b(r_1)$ onto the disc $B_{f(b)}(|s|r_1)$.

1.2 The Artin-Hasse Exponential, AH_p

The usual exponential function, exp, is defined the same way in the p-adic numbers as it is in the reals:

$$\exp(x) = \sum_{n\geq 0} \frac{x^n}{n!}.$$

The difference between the real exponential and p-adic exponential is that latter has a relatively small domain of convergence. Indeed, the power series $\exp(x)$ converges with respect to the p-adic norm only for x in $E := \{x \in \mathbb{C}_p : |x|_p \leq p^{1/(1-p)}\}$ [1, p.1].

This motivates the study of a more apt exponential function for the p-adic numbers:

Definition 1.5. *[1, p.1] The* ***Artin-Hasse Exponential****, AH_p, is defined as the formal power series obtained through the composition of two power series:*

$$AH_p(x) := \exp\left(\sum_{n\geq 0} \frac{x^{p^n}}{p^n}\right)$$

As we will show, when treated as a function on $\mathbb{C}_p$, the domain of convergence of AH_p is exactly $m_p := \{x \in \mathbb{C}_p : |x| < 1\}$. This disc is of course strictly larger than E.

2 Coefficients of $AH_p(x)$ are $\mathbb{Z}_p$ Integral

In this section we show that the coefficients of $AH_p(x)$ written as a formal power series are all $\mathbb{Z}_p$ integral. We will also be dealing with the notion of topological groups, so we offer a definition here:

Definition 2.1. *[3, p.16] A* ***topological group*** *is a set G with two structures:*

(i) G is a group

(ii) G is a topological space

such that the two structures are compatible, that is, both the multiplication map $\mu : G \times G \to G$ and the inversion map $\nu : G \to G$ are continuous.

With this is mind, we introduce the notation we will use when discussing topological groups in this section:

Notation. *Let G be a topological group; let S_n be the symmetric group on n letters equipped with the discrete topology. Let t_n denote the number of continuous homomorphisms φ from G to S_n. Let s_n be the number of such continuous homomorphisms where $\varphi(G)$ is a transitive subgroup of S_n. Finally, let M_n be the number of open subgroups of G with index n.*

2.1 Counting Continuous Homomorphisms from G to S_n

We begin with the following lemma which gives us a recursive formula for t_n, the number of continuous homomorphisms from G to S_n. The lemma also describes a relationship between the t_i's and s_i's, the number of homomorphisms φ from G to S_i where $\varphi(G)$ is a transitive subgroup:

Lemma 2.2.

$$t_n = s_1 t_{n-1} + \binom{n-1}{1} s_2 t_{n-2} + \ldots + \binom{n-1}{n-2} s_{n-1} t_1 + s_n t_0.$$

Proof. Suppose $\varphi : G \to S_n$ is a continuous homomorphism and $\mathcal{O}(1) = \{1, i_2, \ldots, i_k\}$ is an orbit under the action of $\varphi(G)$ on $\{1, 2, \ldots, n\}$ where $1 \leq k \leq n$. Then $\varphi(G)$ acts transitively on $\mathcal{O}(1)$ and acts as a subgroup of S_{n-k} on the other $n-k$ letters in $\{1, 2, \ldots, n\} \setminus \mathcal{O}(1)$. We can pick the $(k-1)$ letters $\{i_2, i_3, \ldots, i_k\}$ from $\{2, 3, \ldots, n\}$ in $\binom{n-1}{k-1}$ ways, so for each k, there are $\binom{n-1}{k-1} s_k t_{n-k}$ such homomorphisms φ where $|\mathcal{O}(1)| = k$. Note that for some k, there may not be any such homomorphism φ where $\varphi(G)$ acts transitively on some $\{1, i_2, \ldots, i_k\}$; in this case $s_k = 0$. The result follows by taking a sum of the number of continuous homomorphisms for $k = 1, 2, \ldots, n$. □

This recurrence can be used to compute t_n for any topological group G since we always have $t_0 = 1$ and $s_1 = 1$.

We also derive the following relationship between M_n, the number of open subgroups of G with index n and s_n, the number of continuous homomorphisms from G to S_n:

Lemma 2.3. $s_n = M_n \cdot (n-1)!$.

Proof. Let $\varphi : G \to S_n$ be a continuous homomorphism so $\varphi(G)$ acts transitively on $\{1, 2, \ldots, n\}$. Let H be the stabilizer of 1. Note that H is open in G since $\varphi(H)$ is open in S_n under its discrete topology and φ is continuous. By the Orbit-Stabilizer theorem [4, p.116], $|\mathcal{O}(1)| = n = [G : H]$, so there are M_n choices for H. The action of $\varphi(G)$ is then determined by the images of the other $n-1$ right cosets of H under φ which each send 1 to a unique element of $\{2, 3, \ldots, n\}$. This can be done in $(n-1)!$ ways, so we conclude that there are $M_n \cdot (n-1)!$ choices for φ. □

Now, we use the results of Lemma 2.2 and Lemma 2.3 to build another recursive formula for t_n, this time using the M_i's:

Lemma 2.4. *Let G be a topological group such that for every integer n, there are finitely many open subgroups of index n. Then*

$$\frac{t_n}{(n-1)!} = t_0 M_n + t_1 \frac{M_{n-1}}{1!} + t_2 \frac{M_{n-2}}{2!} + \ldots + t_{n-1} \frac{M_1}{(n-1)!}.$$

Proof. By the result of Lemma 2.2, we have

$$t_n = \sum_{k=1}^{n} \binom{n-1}{k-1} s_k t_{n-k}.$$

We apply Lemma 2.3 to see

$$= \sum_{k=1}^{n} \binom{n-1}{k-1} M_k (k-1)! t_{n-k}.$$

Finally, rearrange to get the result:

$$\begin{aligned} &= \sum_{k=1}^{n} \frac{(n-1)!}{(n-k)!} M_k t_{n-k} \\ \frac{t_n}{(n-1)!} &= \sum_{k=1}^{n} \frac{M_k}{(n-k)!} t_{n-k}. \end{aligned} \qquad \square$$

We are now ready to present our first general theorem which allows us to write the composition of $\exp(x)$ with another power series as a single power series with closed-form coefficients:

Theorem 2.5. *Let G be a topological group so that for every integer n, there are finitely many open subgroups of index n. Then*

$$\exp\left(\sum_{H \le G} \frac{x^{[G:H]}}{[G:H]} \right) = \sum_{n \ge 0} \frac{t_n}{n!} x^n$$

where H runs over the open subgroups of G with finite index.

The proof of this theorem uses a standard tool in combinatorics, typically used for counting partitions: the complete Bell polynomials. Before proceeding with the proof, we provide a pair of relevant definitions.

Definition 2.6. *[5, p.205] Given $B_0 = 1$, the* ***complete Bell polynomial****, $B_{n+1} \in \mathbb{Z}[x]$, can be defined for all non-negative integers n by the following recurrence relation:*

$$B_{n+1}(x_1, \dots, x_{n+1}) = \sum_{k=1}^{n} \binom{n}{k} B_{n-k}(x_1, \dots, x_{n-k}) x_{+1}.$$

As we will see, this recurrence is perfectly suited to our needs for this proof. We will also use the following:

Definition 2.7. *[5, p.205] The* ***complete exponential Bell polynomial*** *is defined by the generating function for the complete Bell polynomials, $\mathcal{B}(u)$:*

$$\mathcal{B}(u) = \exp\left(\sum_{n \ge 1} x_n \frac{u^n}{n!} \right) = \sum_{n \ge 0} B_n(x_1, \dots, x_n) \frac{u^n}{n!}$$

The use of Bell polynomials, often used for counting partitions, lends a combinatoric flavor to this theorem and to this whole discussion of counting continuous homomorphisms from G to S_n. Indeed, we show below that t_n is related to the M_i's exactly by the nth Bell polynomial. This is not altogether surprising, though, since our recurrence for t_n in Lemma 2.2 involves partitioning the image of a homomorphism $\varphi : G \to S_n$ into transitive and non-transitive subgroups.

We now proceed with the proof of the theorem.

Proof of Theorem 2.5. Since M_k is finite for all $k \geq 1$, we may rewrite the left hand side as follows using the definition of the complete exponential Bell polynomial as in Definition 2.7:

$$\begin{aligned}\exp\left(\sum_{H\leq G}\frac{x^{[G:H]}}{[G:H]}\right) &= \exp\left(\sum_{k\geq 1}\frac{M_k}{k}x^k\right)\\ &= \exp\left(\sum_{k\geq 1}M_k(k-1)!\frac{x^k}{k!}\right)\\ &= \sum_{n\geq 0}B_n\big(M_1(0!), M_2(1!), \ldots, M_n(n-1)!\big)\frac{x^k}{k!}.\end{aligned}$$

where B_n is the nth complete Bell polynomial. It therefore suffices to show $t_n = B_n\big(M_1(0!), M_2(1!), \ldots, M_n(n-1)!\big)$ for all $n \geq 0$. We proceed by induction.

The base case is trivial since $t_0 = B_0 = 1$. Suppose the equation holds for all $n = 1, 2, \ldots, k$. By the recurrence definition of complete Bell polynomials (Definition 2.6), we have

$$B_{k+1}\big(M_1, \ldots, M_{k+1}(k!)\big) = \sum_{\ell=0}^{k}\binom{k}{\ell}\big(M_{\ell+1}\ell!\big)B_{k-\ell}\big(M_1, \ldots, M_{k-\ell}(k-\ell-1)!\big)$$

and so, by our inductive hypothesis,

$$\begin{aligned}&= \sum_{\ell=0}^{k}\binom{k}{\ell}(M_{\ell+1}\ell!)t_{k-\ell}\\ &= k!\sum_{\ell=0}^{k}t_{k-\ell}\frac{M_{\ell+1}}{(k-\ell)!}\end{aligned}$$

but this is exactly the form of the recurrence for t_{k+1} of Lemma 2.4. The claim is therefore true by induction, and the proof follows. □

It is also worth mentioning that though the use of topological groups in this section is important for our purposes, the results here are still true if we only consider ordinary homomorphisms between groups without topology and omit the restrictions to open subgroups. One can see this by simply equipping a non-topological group G with the discrete topology so any subgroup is open and any homomorphism $\varphi : G \to S_n$ is automatically continuous (when S_n has the discrete topology).

2.2 Application to $\mathbb{Z}_p$ and $AH_p(x)$

We now apply the previous result by taking our topological group to be the p-adic integers $\mathbb{Z}_p$ to get a new expression for $AH_p(x)$ as a power series.

Theorem 2.8. *Let $t_{\mathbb{Z}_p,n}$ denote the number of continuous homomorphisms from $\mathbb{Z}_p$ to S_n. Then the coefficients of $AH_p(x)$ are of the form $t_{\mathbb{Z}_p,n}/n!$, so*

$$AH_p(x) = 1 + \sum_{n\geq 1} \frac{t_{\mathbb{Z}_p,n}}{n!} x^n.$$

Proof. Note that for all $k \geq 1$, there exists a unique (open) subgroup of $\mathbb{Z}_p$ of index p^k, and that there are no subgroups not of p-power index. From here, apply the result of Theorem 2.5 to see

$$\sum_{n\geq 0} \frac{t_{\mathbb{Z}_p,n}}{n!} x^n = \exp\left(\sum_{H \leq \mathbb{Z}_p} \frac{x^{[\mathbb{Z}_p:H]}}{[\mathbb{Z}_p : H]} \right) = \exp\left(\sum_{k\geq 0} \frac{x^{p^k}}{p^k} \right) = AH_p(x). \qquad \square$$

Finally, all that remains to show is that each coefficient of $AH_p(x)$ belongs to the p-adic integers.

Notation. *For the following proof, let v_p denote the p-adic valuation on $\mathbb{Q}$. Let $\mathbb{Z}_{(p)}$ be the subring of the p-adic integers $\mathbb{Z}_p$ given by*

$$\mathbb{Z}_{(p)} = \{r \in \mathbb{Q} : |r|_p \leq 1\} = \{r/s \in \mathbb{Q} : (r, s) = 1,\ p \nmid s\}.$$

Theorem 2.9. *The coefficients of $AH_p(x)$ are $\mathbb{Z}_{(p)}$ integral. That is, $AH_p(x)$ belongs to the ring of formal power series with coefficients in $\mathbb{Z}_{(p)}$:*

$$AH_p(x) \in \mathbb{Z}_{(p)}[[x]].$$

Proof. Let $m \in \mathbb{Z}$ be such that $n! = p^{v_p(n!)}m$ and $(p, m) = 1$. We will show that for each $n \geq 0$, there exists an integer ℓ so $p^{v_p(n!)}\ell = t_{\mathbb{Z}_p,n}$, and therefore

$$\frac{t_{\mathbb{Z}_p,n}}{n!} = \frac{\ell}{m} \in \mathbb{Z}_{(p)}.$$

Let $T = \{\sigma \in S_n : \sigma^{p^k} = 1,\ k \in \mathbb{N}\}$ be the elements of S_n with p-power order. Note that $t_{\mathbb{Z}_p,n} = |T|$. By a theorem of Frobenius [6, p.136], $p^{v_p(n!)}$ divides the size of $A := \{\sigma \in S_n : \sigma^{p^{v_p(n!)}} = 1\}$. Clearly $A \subseteq T$. To see that $T \subseteq A$, consider an element $\tau \in T$. There exists $k \geq 0$ so $\tau^{p^k} = 1$ and $p^k \leq n$. Thus, $p^k \mid n!$, and moreover, since $(p, m) = 1$ and $m \mid n!$, we have $mp^k \mid n!$, so $p^k \mid p^{v_p(n!)}$. Hence $\tau^{p^{v_p(n!)}} = 1$, so $\tau \in A$. We conclude that $p^{v_p(n!)} \mid |T| = t_{\mathbb{Z}_p,n}$, so such an ℓ exists.

The coefficients of $AH_p(x)$ are therefore in $\mathbb{Z}_{(p)}$, so $AH_p(x) \in \mathbb{Z}_{(p)}[[x]]$. $\square$

3 AH_p and Roots of Unity in $\mathbb{C}_p$

In this section, we apply some results from the previous section to construct a new proof of the well-known but not well-document fact in p-adic analysis that all the p^k roots of unity in $\mathbb{C}_p$ are contained in the image of AH_p when AH_p is considered as a function on $\mathbb{C}_p$. We begin by proving some analytic properties of AH_p.

3.1 Analytic Properties of AH_p on $\mathbb{C}_p$

Our result that the coefficients of $AH_p(x)$ have p-adic norm bounded by 1 is very useful fro examining its analytic properties. We present a proof AH_p converges on the interior of the unit disc in $\mathbb{C}_p$ which is made simple given the result of Theorem 2.9.

Notation. *Let $m_p := \{x \in \mathbb{C}_p : |x|_p < 1\}$. We will show the domain of convergence of AH_p is exactly m_p.*

Lemma 3.1. *If $x \in m_p$, then $AH_p(x)$ converges.*

Proof. Let $AH_p(x)$ be written as the power series

$$AH_p(x) = \sum_{k \geq 0} c_k x^k.$$

By Theorem 2.9, the coefficients $\{c_k\}$ are in $\mathbb{Z}_p$, so for all k, $|c_k|_p \leq 1$. Since $|x|_p < 1$, it is clear that $|c_k x^k|_p = |c_k|_p |x|_p^k \to 0$ as $k \to \infty$. Thus $AH_p(x)$ converges at x with respect to the p-adic norm by Theorem 1.3. □

Even with the result of Theorem 2.9, proving that the disc of convergence of AH_p is exactly m_p takes work. To see this, we complete a proof that AH_p diverges on ∂m_p provided in Keith Conrad's notes [1].

Lemma 3.2. *$AH_p(x)$ diverges everywhere on $\partial m_p = \{\alpha \in \mathbb{C}_p : |\alpha|_p = 1\}$. Thus, the disc of convergence for $AH_p(x)$ is exactly m_p.*

Proof. (A completion of a proof in Conrad's notes [1, p.6]) It suffices to show $AH_p(x)$ diverges at 1, i.e. the coefficients of $AH_p(x)$ do not tend to 0. We do this by showing $AH_p(x)$ has infinitely many coefficients in $\mathbb{Z}_p^\times$ (note $u \in \mathbb{Z}_p^\times$ implies $|u|_p = 1$).

Equivalently, we show $AH_p(x) \mod p \in \mathbb{F}_p[[x]]$ is not in $\mathbb{F}_p[x]$ (where $\mathbb{F}_p$ is the field of p elements). From the definition of $AH_p(x)$, we have

$$x\frac{AH_p(x)}{AH_p'(x)} = \sum_{k=0}^{\infty} x^{p^k} := f(x)$$

This is an equation in $\mathbb{Z}_p[[x]]$, so we can reduce modulo p, and it will also be true in $\mathbb{F}_p[[x]]$. Since $\text{char}(\mathbb{F}_p) = p$, we have $(f(x)^p) = f(x) - x$, so $f(x) \bmod p$ must be a root of $t^p - t + x$ in $\mathbb{F}_p(x)$. We derive a contradiction by showing $t^p - t + x$ has no roots in $\mathbb{F}_p(x)$:

Consider $t^p = t - x$; we have $p \deg(t) = \deg(t - x) \in \{\deg(t), 1, 0\}$. All three possibilities for $\deg(t - x)$ lead to contradiction: If $p\deg(t) = \deg(g)$, $p = 1$. If $p\deg(t) = 1$, $p \mid 1$. Finally, $p\deg(t) = 0$ implies $\deg(t) = 0$, so we can write $t = f/g$ for $f, g \in \mathbb{F}_p[x]$ with $\deg(f) = \deg(g)$. This forces $\deg(f^p/g^p - f/g) = 1$, which is impossible. Thus $t^p - t + x$ has no roots in $\mathbb{F}_p(x)$, and in particular $AH_p(x) \bmod p \notin \mathbb{F}_p[x]$.

We conclude that $AH_p(x)$ diverges on ∂m_p and hence the disc of convergence of AH_p is exactly m_p. □

For the proof that the p^k roots of unity in $\mathbb{C}_p$ are contained in the image of AH_p, we need one more result:

Lemma 3.3. *$AH_p : m_p \to m_p + 1$ is a surjective isometry.*

Proof. By Theorem 1.4, it suffices to show that for all $x, y \in m_p$,

$$\left| \frac{AH_p(x) - AH_p(y)}{x - y} - 1 \right| < 1.$$

Writing $AH_p(x)$ and $AH_p(y)$ as a power series (by Theorem 2.9), this inequality can be rewritten as

$$\begin{aligned} 1 &> \left| \frac{1}{x-y} \left(\sum_{n \geq 2} \frac{t_n}{n!} x^n - \sum_{n \geq 2} \frac{t_n}{n!} y^n \right) \right| \\ &= \left| \frac{1}{x-y} \sum_{n \geq 2} \frac{t_n}{n!} (x^n - y^n) \right| \end{aligned}$$

We use the fact that m_p is an ideal of $\mathbb{C}_p$ [2, p.25]. Since $x, y \in m_p$, both x^n and y^n are in m_p for all n, and therefore each term $t_n(x^n - y^n)/n!$ of the sum is in m_p. We conclude that the whole expression inside the norm is in m_p, so the inequality is satisfied. The result follows. □

3.2 $AH_p(m_p)$ Contains all p^k Roots of Unity

Finally, we present our proof that the p^k roots of unity in $\mathbb{C}_p$ are contained in the image of AH_p:

Theorem 3.4. *For every p^k root of unity $\zeta \in \mathbb{C}_p$, there exists $\alpha \in m_p$ for which $AH_p(\alpha) = \zeta$.*

Proof. Let ζ be a primitive p^k root of unity for $k \geq 1$. Let $f \in \mathbb{C}_p[x]$ be given by

$$f(x) = \frac{x^{p^k} - 1}{x^{p^{k-1}} - 1} = 1 + x^{p^{k-1}} + \ldots + x^{(p-1)p^{k-1}}.$$

The roots of f are then all the primitive p^k roots of unity ζ^r such that $1 \leq r < p^k$ and $(r, p) = 1$. Therefore,

$$f(1) = p = \prod_{\substack{1 \leq r < p^k \\ (r,p)=1}} (1 - \zeta^r). \qquad (*)$$

Note that for all such r in the product above, by the strong triangle inequality $u := (\zeta^r - 1)/(\zeta - 1)$ in $\mathbb{C}_p$ has p-adic norm bounded by 1:

$$|u| = \left| \frac{\zeta^r - 1}{\zeta - 1} \right| = |1 + \zeta + \zeta^2 + \ldots + \zeta^{r-1}| \leq \max_{0 \leq k < r} \{|\zeta^k|\} = 1.$$

Since $(r, p^k) = 1$, there exist $s, t \in \mathbb{Z}$ so that $1 = sr + tp^k$. Using this, we obtain the following formula for u^{-1}:

$$u^{-1} = \frac{\zeta - 1}{\zeta^r - 1} = \frac{\zeta^{sr+tp^k} - 1}{\zeta^r - 1} = \frac{(\zeta^r)^s - 1}{\zeta^r - 1} = 1 + \zeta^r + \zeta^{2r} + \ldots + \zeta^{(s-1)r}.$$

Likewise by the strong triangle inequality, $|u^{-1}| \leq 1$. But since $uu^{-1} = 1$, this forces $|u| = |u^{-1}| = 1$. In particular, we get $|\zeta^r - 1| = |\zeta - 1|$.

Taking norms of $(*)$ above, we can use this to see

$$|p| = \prod_{\substack{1 \leq r < p^k \\ (r,p)=1}} |1 - \zeta^r| = |1 - \zeta|^{\varphi(p^k)} = |1 - \zeta|^{(p-1)p^{k-1}}$$

so, by evaluating the norms,

$$|1 - \zeta| = \left(p^{\frac{1}{1-p}}\right)^{p^{1-k}} < 1$$

and thus $\zeta - 1 \in m_p$, so $\zeta \in m_p + 1$. By Lemma 3.3, $AH_p(x)$ is an isometry which takes m_p onto $m_p + 1$, so there exists a unique $\alpha \in m_p$ for which $AH_p(\alpha) = \zeta$. □

4 Conclusion and Further Research

We started study the p-adic numbers, and explore Artin-Hasse exponential on $\mathbb{Z}_p$, $\mathbb{Q}_p$ and $\mathbb{C}_p$. From these process, we found that coefficients of AH_p are in $\mathbb{Z}_p$ with algebraic way. Besides, we could explore this expression with analytic ways, and we found relationship between AH_p and Unity.

- We discussed and handle the Artin-Hasse exponential on specific field like $\mathbb{Z}_p$, $\mathbb{Q}_p$ and $\mathbb{C}_p$, but we could discuss about this exponential within general fields like K (non-archimedean valued complete field), and could find some properties like above.
- Until now, we just check the existence of α such that $AH_p(\alpha) = \zeta$, but we curious about the construction of α.

5 Acknowledgements

We would like to thank the Illinois Geometry Lab at the University of Illinois at Urbana Champaign for proceeding with this project this semester. Thank you to our faculty member, Professor Shiang Tang, and to our Ph.D. mentor Ravi Donepudi. Without their support and guidance throughout the semester, the results would have never been possible.

References

[1] K. Conrad. Artin-hasse-type series and roots of unity. University of Connecticut, 2020. `https://kconrad.math.uconn.edu/blurbs/gradnumthy/AHrootofunity.pdf`.

[2] W. H. Schikhof. *Ultrametric Calculus: an Introduction to p-adic Analysis*. Cambridge Studies in Advanced Mathematics. Cambridge University Press, 2006.

[3] P. J. Higgins. *An Introduction to Topological Groups*. London Mathematical Society lecture note series; 15. Cambridge University Press, 1974.

[4] F. M. Goodman. *Algebra: Abstract and Concrete*. Prentice Hall, 1998.

[5] G. E. Andrews. *The Theory of Partitions*. Encyclopedia of Mathematics and its Applications. Cambridge University Press, 1984.

[6] M. Hall. *The Theory of Groups*. Dover Books on Mathematics. Dover, reprint edition, 2018.