The Artin-Hasse Exponential and p-adic Numbers

Faculty Mentor: Shaing Tang; Graduate Mentor: Ravi Donepudi; Xiaojian Li, Jay Reiter, Napoleon Wang, Hyunjin Yi

Illinois Geometry Lab, University of Illinois at Urbana Champaign

Introduction & Project Goals

In this project, we provide an original, combinatorial proof that the Artin Hasse exponential, $AH_p(x)$, as a formal power series has coefficients in the subring of p-adic integers: $\mathbb{Z}_{(p)} = \{r \in \mathbb{Q} : |x|_p\}$. Our proof of this result begins with a counting argument on the number homomorphisms, and makes stops in topological group theory, the combinatorics of counting integer partitions.

We then use this result 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 $AH_p(\alpha) = \zeta$.

The p-adic Numbers

In this section, we provide some definitions and theorems which have been useful to us in gaining intuition for the p-adic numbers and in proving the following results.

Definition. For any prime $p \in \mathbb{Z}$, $\mathbb{Z}_p$, the **p-adic integers**, is the set of all infinite sequences such that: $...a_m a_{m-1}...a_1 a_0$ where each a_m is one of the elements $0, 1, 2, ..., p-1$.

Definition. $\mathbb{Q}_p$, the **p-adic numbers**, is the set of all two-sided sequences such that $...a_2 a_1 a_0.a_{-1} a_{-2}...$ for which $a_i \in \{0, 1, 2, ..., p-1\}$ for each i and such that $a_{-n} = 0$ for large n.

Definition. Fix p prime. For any rational number x, there are some integers n, s, and t with $p \nmid s, t$ so

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

The **p-adic valuation** of x is then $|x|_p := p^{-n}$.

Ostrowski Theorem. (Schikhof, p.22, [2]) Each non-trivial absolute value on $\mathbb{Q}$ is equivalent to either the absolute value, or some p-adic valuation, i.e. the only completions of $\mathbb{Q}$ are $\mathbb{R}$ or some $\mathbb{Q}_p$.

Proposition. (Schikhof, p.61, [2]) Let $\{a_n\}$ be a sequence in $\mathbb{Z}p$. $\sum a_n$ converges if and only if $lim_{n\to\infty} a_n = 0$

Proposition. (Newton Approximation) Let f be a $\mathbb{C}_p$-valued function on a disc $B := B_a(r) \subset \mathbb{C}_p$. Suppose there exists $s \in \mathbb{C}_p$ such that

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

Then $s^{-1} f$ is an isometry and f maps discs onto discs; i.e. for all $b \in B$, $r_1 \in (0, r]$, $f : B_b(r_1) \to B_{f(b)}(|s|_p r_1)$ is a surjection.

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

Theorem. (Schikhof, p.68, [2]) D open and convex in $\mathbb{C}_p$; let $f : D \to \mathbb{C}_p$ be analytic. For any $v \in D$, there exists a sequence $\{b_i\} \subset \mathbb{C}_p$ so that for all $x \in D$

$$f(x) = \sum_{n=0}^{\infty} b_n (x - v)^n.$$

Theorem. (Hensel's Lemma) f analytic on $B_0(1)$,

$$f(x) = \sum_{n=0}^{\infty} a_n x^n, \qquad x \in B_0(1)$$

Suppose each $|a_n|_p \leq 1$ and there exists $a \in B_0(1)$ for which $f(a) < 1$ and $|f(a)|_p = 1$. Then there exists $b \in B_0(1)$ such that $|b - a|_p \leq |f(a)|$ and $f(b) = 0$.

Coefficients of $\mathbf{AH_p(x)}$ are in $\mathbb{Z}_{(p)}$

In the following section, let G be a topological group; let S_n be the symmetric group on n letters with the discrete topology. Let t_n be the number of continuous homomorphisms $G \to S_n$; let s_n be the number of such homomorphisms where the image is a transitive subgroup of S_n.

Lemma 1.1 Let G, S_n, t_n, and s_n be as above. Then

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

Lemma 1.2 Let M_n be the number of open subgroups of G with index n. Then $s_n = M_n \cdot (n-1)!$.

Lemma 1.3 Let G be a topological group such that for every integer n, there are finitely many open subgroups of index n. Then

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

Theorem 1.4 Let G be a topological group so that for every integer n, there are finitely many open subgroups of index n. Then

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

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

Theorem 1.5 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 are $t_{\mathbb{Z}_p, n}/n!$, so

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

Theorem 1.6 $AH_p(x) \in \mathbb{Z}_{(p)}[[x]]$.

$\mathbb{C}_\mathbf{p}$ Roots of Unity in the Image of $\mathbf{AH_p}$

Since the domain of convergence of the p-adic exponential is small, the only root of unity in the image of $\exp$ is 1; this leaves us with no way of representing roots of unity as $\exp(2\pi i\theta)$ as we do in $\mathbb{C}$.
This result that the p^k roots of unity in $\mathbb{C}_p$ are in the image of AH_p provides us with an appropriate analogue for the p-adic numbers.

Lemma 2.1 If $x \in m_p := \{\alpha \in \mathbb{C}_p : |\alpha|_p < 1\}$, then $AH_p(x)$ converges.

Lemma 2.2 In particular, $AH_p(x)$ diverges everywhere on the boundary

$$\{\alpha \in \mathbb{C}_p : |\alpha|_p = 1\}$$

thus the disc of convergence for $AH_p(x)$ is exactly m_p.

Lemma 2.3 $AH_p : m_p \to m_p + 1$ is a surjective isometry.

Theorem 2.4 For every p^k root of unity $\zeta \in \mathbb{C}_p$, there is $\alpha \in m_p$ for which $AH_p(\alpha) = \zeta$.

Outlines of Proofs

Lemma 1.1 We use a constructive counting argument

Lemma 1.2 Like Lemma 1.1, using concepts of continuous homomorphism and Orbit-Stabilizer theorem, we could prove it.

Lemma 1.3 Use Lemma 1.1 & 1.2

Theorem 1.4 Use Lemma 1.3 and the complete exponential Bell polynomials, then induction on n.

Theorem 1.5 Follows immediately from 1.4.

Theorem 1.6 Let $T = \{\sigma \in S_n : \sigma^{p^k} = 1, \, k \in \mathbb{N}\}$ be the elements of S_n. Using theorem of Frobenius, $p^{v_p(n!)}$ divides the size of

$$A := \{\sigma \in S_n : \sigma^{p^{v_p(n!)}} = 1\}.$$

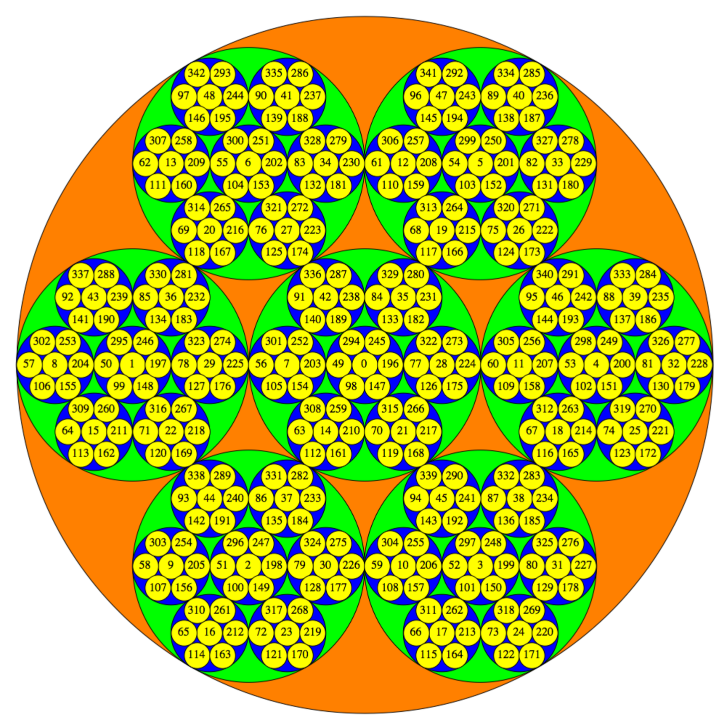
Clearly, $A \subseteq T$, and show that $T \subseteq A$ then done.

Lemma 2.1 From Theorem 1.6, all coefficients of $AH_p(x)$ in $\mathbb{Z}_p$. This means $|\text{coefficients}|_p \leq 1$, and since our domain is m_p. So, $AH_p(x)$ converges in m_p

Lemma 2.2 Theorem 2.10 (Conrad, p.6, [1])

Lemma 2.3 Use Theorem 2.5 (Conrad, p.4, [1]) to show the isometry and Lemma 27.4 (Schikhof, p.78-79, [2]) to show the surjectivity.

Theorem 2.4 As a result based on what we have proved from Theorem 1.1 to Theorem 2.3



Acknowledgements

We thank Professor Shiang Tang and graduate student mentor Ravi Donepudi for leading this project and the Illinois Geometry Lab for providing us the opportunity to participate in this project.

References

[1] Conrad, K. (n.d.). *Artin-Hasse-type Series and Roots of Unity.* University of Connecticut.`https://kconrad.math.uconn.edu/blurbs/gradnumthy/AHrootofunity.pdf`.

[2] Schikhof, W. H. (2006). *Ultrametric calculus: an introduction to p-adic analysis* (Ser. Cambridge studies in advanced mathematics). Cambridge University Press.