Summer 7-15-2020

Arithmetic Differential Operators on Z_p^r

Marshall Brandenburg

Marshall Brandenburg

Candidate

Mathematics and Statistics

Department

This thesis is approved, and it is acceptable in quality and form for publication:

Approved by the Thesis Committee:

Alexandru Buium , Chairperson

Janet Vassilev

Dimiter Vassilev

Arithmetic Differential Operators on $\mathbb{Z}_p^r$

by

Marshall Brandenburg

B.S., Applied Mathematics, University of New Mexico, 2016

THESIS

Submitted in Partial Fulfillment of the

Requirements for the Degree of

Master of Science

Mathematics

The University of New Mexico

Albuquerque, New Mexico

July, 2020

Dedication

To my parents, Fred and Kellee, for their unending support, encouragement, and unconditional love.

"The mathematician's patterns, like the painter's or the poet's must be beautiful; the ideas like the colours or the words, must fit together in a harmonious way. Beauty is the first test: there is no permanent place in the world for ugly mathematics."

– G.H. Hardy

Acknowledgments

I would like to thank my advisor, Dr. Alexandru Buium, for his support and unwavering patience. I would also like to thank Dr. Janet Vassilev for igniting my love of pure mathematics early in my undergraduate studies. Lastly, I would like to thank all of the wonderful and supportive mathematicians I've met along the way.

ARITHMETIC DIFFERENTIAL OPERATORS ON $\mathbb{Z}_p^r$

by

Marshall Brandenburg

B.S., University of New Mexico, 2016

M.S., Mathematics, University of New Mexico, 2020

Abstract

Given a prime p, we let $\delta x = (\frac{x_1 - x_1^p}{p}, \ldots, \frac{x_r - x_r^p}{p})$ be the Fermat quotient operator on $\mathbb{Z}_p^r$. We prove that if a function $f\colon \mathbb{Z}_p^r \to \mathbb{Z}_p$ can be represented as $f(x) = F(x, \delta x, \delta^2 x, \ldots, \delta^m x)$, where F is a restricted power series with $\mathbb{Z}_p$-coefficients in $m+1$ variables, then f is analytic.

Contents

Preliminaries

Given a prime number, p, we define the p-adic valuation $\nu_p(n)$ on $\mathbb{Z}$, $\nu_p(n)\colon \mathbb{Z} \to \mathbb{N}$ as follows:

$$\nu_p(n) = \begin{cases} \max\{r \in \mathbb{N}\colon p^r \mid n\} & \text{if } n \neq 0 \\ \infty & \text{if } n = 0 \end{cases}$$

There is a natural extension of this valuation to $\mathbb{Q}$ by $\nu_p\colon \mathbb{Q} \to \mathbb{N}$

$$\nu_p(\frac{a}{b}) = \nu_p(a) - \nu_p(b)$$

for $a, b \in \mathbb{Z}$, $b \neq 0$.

The p-adic valuation allows us to construct a norm on $\mathbb{Q}$,

$$\|x\|_p = \begin{cases} \frac{1}{p^{\nu_p(x)}} & \text{if } x \neq 0 \\ 0 & \text{if } x = 0 \end{cases}$$

Hence, the p-adic norm allows one to complete $\mathbb{Q}$ via the induced metric. The completion of $\mathbb{Q}$ with respect to the p-adic norm is what we refer to as the p-adic numbers. We refer to the completion of $\mathbb{Q}$ with respect to the induced metric as $\mathbb{Q}_p$. It is worth noting that the induced metric d is *non-Archimedean*; that is,

$$d(x, y) \leq \max\{d(x, z), d(y, z)\} \quad \forall\ x, y, z \in \mathbb{Q}_p\,.$$

The subset of $\mathbb{Q}_p$ with which this thesis is concerned is the p-adic integers, denoted $\mathbb{Z}_p$, and defined as follows:

$$\mathbb{Z}_p = \{a \in \mathbb{Q}_p \mid \|a\|_p \leq 1\}$$

We consider the *Fermat quotient operator* on the ring of p-adic integers as follows:

$$\delta a = \frac{a - a^p}{p},$$

which can be viewed analogously as the "derivative of a with respect to p." We denote the i-th iterate of δ as δ^i. Our results concern analytic functions from $\mathbb{Z}_p$ to $\mathbb{Z}_p$ and functions from $\mathbb{Z}_p^r$ to $\mathbb{Z}_p$.

Introduction

Given a multi-index $\alpha = (\alpha_0, \ldots, \alpha_k)$ of non-negative integers, we say that $\alpha \geq 0$ and use x^α to denote the quantity $x_0^{\alpha_0} \cdots x_k^{\alpha_k}$. By $|\alpha|$ we mean $|\alpha| = \alpha_0 + \cdots + \alpha_k$. We say that the series

$$F(x) = \sum_{\alpha \geq 0} a_\alpha x^\alpha \ \in \mathbb{Z}_p[[x_0, \ldots, x_k]]$$

is said to be a *restricted* power series if $\lim_{|\alpha| \to \infty} a_\alpha = 0$.

Definition 1. A function $f\colon \mathbb{Z}_p \to \mathbb{Z}_p$ is said to be an *arithmetic differential operator of order m* if there exists a restricted power series $F \in \mathbb{Z}_p[[x_0, x_1, \ldots, x_m]]$ such that

$$f(a) = F(a, \delta a, \ldots, \delta^m a)$$

for all $a \in \mathbb{Z}_p$. We say that the series *F δ-represents f.*

Definition 2. A function $f\colon \mathbb{Z}_p \to \mathbb{Z}_p$ is called an *analytic of level m* if for every $a \in \mathbb{Z}_p$, there exists a restricted power series $F_a \in \mathbb{Z}_p[[x]]$ such that

$$f(a + p^m u) = F_a(u)$$

for all $u \in \mathbb{Z}_p$. We say that the collection of series *F_a represents f.*

If there is such an m that the a function is *analytic of level m* then the function is analytic.

Remark. Analytic functions were first introduced by Jean-Pierre Serre in his theory of p-adic analytic manifolds and p-adic Lie groups. Serre used analytic functions to prove his results on Galois representations of elliptic curves. Arithmetic differential

operators were introduced by Alexandru Buium in [3] as functions from $f\colon \mathbf{R} \to \mathbf{R}$ where $\mathbf{R}$ is the completion of the maximum unramified extension of $\mathbb{Z}_p$ and were used to prove results on Diophantine equations. This thesis examines the paper [2] by Buium, Ralph, Simanca and discusses possible extensions to the multivariate case. In [2], it is shown that the theory of arithmetic differential operators reduces to Serre's p-adic theory of analytic functions if one restricts the domain of arithmetic differential operators from $\mathbf{R}$ to $\mathbb{Z}_p$. The full power of arithmetic differential operators is felt in applications that involve $\mathbf{R}$ rather than $\mathbb{Z}_p$.

The Univariate Case

Theorem 1. *Any arithmetic differential operator $f\colon \mathbb{Z}_p \to \mathbb{Z}_p$ of order m is an analytic function of level m.*

Theorem 2. *Any analytic function $f\colon \mathbb{Z}_p \to \mathbb{Z}_p$ of level m is an arithmetic differential operator of order m.*

Theorem 1 and Theorem 2 are due to Buium, Ralph, and Simanca. In this thesis, we generalize Theorem 1 to the multivariate case in Theorem 4 and formulate a conjecture that extends Theorem 2 to the multivariate case; cf. Conjecture 1.

Lemma 1. *If $a \in \mathbb{Z}_p$ and $x = a + p^n u$ in the disc $a + p^n\mathbb{Z}_p$, write $\delta^k x$ as a polynomial function of u of degree p^k,*

$$\delta^k x = \sum_{j=0}^{p^k} c_{a,j}^k u^j$$

with $c_{a,j} \in \mathbb{Q}_p$, then we have the following p-adic estimates:

(i) $\|c_{a,0}^k\|_p \leq 1$

(ii) $\|c_{a,1}^k\|_p = \frac{1}{p^{n-k}}$

(iii) $\|c_{a,j}^k\|_p \leq \frac{1}{p^{(n-k+1)j-1}}$, $\quad 2 \leq j \leq p^k$

Proof. Assertion (i) follows immediately from the equality $c^k_{a,\,0} = \delta^k a$. We will prove (ii) and (iii) by induction on k. In the case where $k = 0$, we have that

$$\delta^0 x = x = a + p^n\, u = a + p^n u = \sum_{j=0}^{1} c_{a,\,j} u^j$$

so $\|c^0_{a,\,0}\|_p = \|a\|_p \leq 1$ as $a \in \mathbb{Z}_p$, and $\|c^1_{a,\,1}\|_p = \|p^n\|_p = \frac{1}{p^n}$. Now, one can assume that the result holds for $k-1$ and prove it for k. By assumption, we have that

$$\delta^{k-1} x = \sum_{j=0}^{p^{k-1}} c^{k-1}_{a,j} u^j\,,$$

where for $j \geq 1$ the coefficients $c^{k-1}_{a,j}$ satisfy the estimates

$$\|c^{k-1}_{a,j}\|_p \;\leq\; \frac{1}{p^{(n-k+2)j-1}}\,,$$

and in the case where $j = 1$, we have equality. We use the definition of the *Fermat quotient operator* to write the k-th iterate as

$$\delta^k x = \sum_{j=0}^{p^k} c^k_{a,\,j} u^j = \frac{\sum\limits_{j=0}^{p^{k-1}} c^{k-1}_{a,\,j}\, u^j - (\sum\limits_{j=0}^{p^{k-1}} c^{k-1}_{a,\,j}\, u^j)^p}{p}\,.$$

Now we consider a fixed index $j \geq 1$. It follows that $c^k_{a,\,j}$ is equal to $\frac{c^{k-1}_{a,\,j}}{p}$ minus a sum of elements of the form $\gamma \frac{c^{k-1}_{a,\,j_1} \cdots c^{k-1}_{a,\,j_p}}{p}$ where γ is a rational integer and $j_1 + \cdots + j_p = j$. As $\mathbb{Q}_p$ is a field, we may commute the elements $j_1, \ldots, j_p$ and assume that there exists an s such that $j_1 \ldots j_s \geq 1$ and $j_t = 0$ for $t > s$. Then $s \leq j_1 + \cdots + j_s = j$. We now apply assertion (i) and the inductive hypothesis to each of the factors and conclude that

$$\left\| \frac{c^{k-1}_{a,\,j_1} \cdots c^{k-1}_{a,\,j_p}}{p} \right\|_p \leq \left\| \frac{c^{k-1}_{a,\,j_1} \cdots c^{k-1}_{a,\,j_s}}{p} \right\|_p \leq \frac{1}{p^{(n-k+2)(j_1 + \,\cdots\, + j_s) - s - 1}} \leq \frac{1}{p^{(n-k+1)j-1}}\,.$$

Thus, assertion (iii) follows. The equality in assertion (ii) follows from the inductive hypothesis and the identity

$$c_{a,1}^k = c_{a,1}^{k-1}(\frac{1}{p} - (c_{a,0}^{k-1})^{p-1}).$$

This concludes the proof. □

We are now able to prove Theorem 1.

Proof. Let $f(x) = F(x, \delta x, \ldots, \delta^m x)$ be an arithmetic differential operator of order m given by the restricted power series $F \in \mathbb{Z}_p[[t_0, \ldots, t_m]]$. Thus,

$$f(x) = \sum_{\alpha=(\alpha_0,\ldots,\alpha_m)} a_\alpha x^{\alpha_0} (\delta x)^{\alpha_1} \cdots (\delta^m x)^{\alpha_m} \ ,$$

where $a_\alpha \to 0$ p-adically as $|\alpha| \to \infty$. Let $I = \{0, 1, \ldots, p^m - 1\}$. The family of discs $\{a + p^n \mathbb{Z}_p\}_{\alpha \in I}$ forms a covering of $\mathbb{Z}_p$. By Lemma 1, if $a \in I$, we have that $f(a + p^m u) = F_a(u)$ where

$$F_a(u) = \sum_{\alpha=(\alpha_0,\ldots,\alpha_m)} a_\alpha \left(\sum_{j_0=0}^{p^0} c_{a,j_0}^0 u^{j_0} \right)^{\alpha_0} \left(\sum_{j_1=0}^{p^1} c_{a,j_1}^1 u^{j_1} \right)^{\alpha_1} \cdots \left(\sum_{j_m=0}^{p^m} c_{a,j_m}^m u^{j_m} \right)^{\alpha_m} \ ,$$

with all the c_{a,j_i}^ks in $\mathbb{Z}_p$. Notice that $F_a(u)$ is a power series in u with $\mathbb{Z}_p$ coefficients that go to zero p-adically as $|\alpha| \to \infty$. □

In the following lemma, we consider the set of all p-adic integer roots of the function $x \mapsto \delta^m x$:

$$C_m \coloneqq \{a \in \mathbb{Z}_p : \ \delta^m a = 0\} .$$

Since the m-th iterate of δ is given by a polynomial of degree p^m with $\mathbb{Q}_p$-coefficients, C_m has at most p^m elements.

Lemma 2. *The composition*

$$C_m \subset \mathbb{Z}_p \to \mathbb{Z}_p/p^m\mathbb{Z}_p$$

is bijective.

Proof. We proceed by induction on m. When $m = 0$, we have $C_0 = \{0\}$. We now assume that the statement holds for $m-1$ and show it for m. Given $a \in C_{m-1}$, we consider the polynomial $t^p - t + pa \in \mathbb{Z}_p[t]$. Applying Hensel's lemma, $t^p - t + pa$ has p distinct roots that we denote by $a_1, \ldots, a_p \in \mathbb{Z}_p$. We remark that $\delta a_j = a$ for all js, and since $\delta^{m-1}a = 0$, it follows that $\delta^m a_j = 0$. We claim that if $a, a' \in C_{m-1}$ we have that

$$a_j \equiv a'_{j'} \mod p^m ,$$

for some j, j', then $a = a'$ and $j = j'$ as well. This claim, together with the inductive hypothesis, gives us that C_m contains a set of p^m elements that maps injectively into $\mathbb{Z}_p/p^m\mathbb{Z}_p$. As C_m has at most p^m elements, this forces the map $C_m \to \mathbb{Z}_p/p^m\mathbb{Z}_p$ to be bijective. □

Using Lemma 2, we can write $C_m = \{a_0, \ldots a_{p^{m-1}}\}$, where $a_\alpha \equiv \alpha \mod p^m$, for all αs in the set $I = \{0, \ldots, p^{m-1}\}$. On the other hand, we fix an ordering in the set

$$I' = \{\beta = (\beta_0, \ldots, \beta_{m-1}) \in \mathbb{Z}^m : 0 \leq \beta_0, \ldots, \beta_{m-1} \leq p-1\} ,$$

and consider the $p^m \times p^m$ matrix $W = (w_{\alpha\beta})_{\alpha\in I,\ \beta\in I'}$, whose entries are given by

$$w_{\alpha\beta} := (a_\alpha)^{\beta_0}(\delta a_\alpha)^{\beta_1} \cdots (\delta^{m-1}a_\alpha)^{\beta_{m-1}} \in \mathbb{Z}_p ,$$

where we use the convention that $a^0 = 1$ for all $a \in \mathbb{Z}_p$.

Lemma 3. *The determinant of the matrix W is invertible in $\mathbb{Z}_p$.*

Proof. We use the reduction mod p mapping

$$\mathbb{Z}_p \to \mathbb{F}_p \coloneqq \mathbb{Z}_p/p\mathbb{Z}_p$$
$$a \mapsto \overline{a}.$$

By Lemma 3.20 in [1], the function

$$\mathbb{Z}_p \to \mathbb{F}_p^m \coloneqq \mathbb{Z}_p/p^m\mathbb{Z}_p$$
$$a \mapsto (\overline{a}, \overline{\delta a}, \ldots, \overline{\delta^{m-1}a})$$

induces a bijection $\mathbb{Z}_p/p^m\mathbb{Z}_p \simeq \mathbb{F}_p^m$. For any $\gamma = (\gamma_0, \ldots, \gamma_{m-1}) \in \mathbb{F}_p^m$ and any $\beta \in I'$, we set

$$v_{\gamma\,\beta} = \gamma_0^{\beta_0} \cdots \gamma_{m-1}^{\beta_{m-1}}.$$

Notice that $\delta^i a_\alpha \equiv \delta^i \alpha \mod p$ if $i \leq m-1$. Using Lemma 2, we now only need to demonstrate that $\det(v_{\gamma\,\beta}) \neq 0 \in \mathbb{F}_p$. Assume for the sake of contradiction that $\det(v_{\gamma\,\beta}) = 0$. Then there exist constants $\lambda_{\beta_0 \ldots \beta_{m-1}} \in \mathbb{F}_p$ for $(\beta_0, \ldots \beta_{m-1}) \in I'$, not all zero, such that

$$\sum_{\beta_0=0}^{p-1} \cdots \sum_{\beta_{m-1}=0}^{p-1} \lambda_{\beta_0 \ldots \beta_{m-1}} \gamma_0^{\beta_0} \cdots \gamma_{m-1}^{\beta_{m-1}} = 0$$

for all $\gamma \in \mathbb{F}_p$. Applying induction on m, we see that all the λs vanish, which is a contradiction. Thus we conclude that $\det(v_{\gamma\,\beta}) \neq 0$, as desired. □

We now begin the proof of Theorem 3. In the following proof, we note that $I = \{0, \ldots, p^{m-1}\}$ and $I' = \{\beta_0, \ldots, \beta_{m-1}\}$.

Theorem 3. *Let $f\colon \mathbb{Z}_p \to \mathbb{Z}_p$ be an analytic function of level m. Then there exists a unique restricted power series $F \in \mathbb{Z}_p[[x_0, x_1, \ldots, x_m]]$ with the following properties:*

(i) $F(x_0, x_1, \ldots, x_m) = \sum_{n\geq 0} \sum_{\beta \in I'} a_{\beta,n}\, x_0^{\beta_0} x_1^{\beta_1} \ldots x_{m-1}^{\beta_{m-1}} x_n^m,$

(ii) $f(a) = F(a, \delta a, \ldots, \delta^m a),\ a \in \mathbb{Z}_p$

Proof. We begin by proving the existence of F. Notice that if $g\colon \mathbb{Z}_p \to \mathbb{Z}_p$ is an arithmetic differential operator of order m and $a \in \mathbb{Z}_p$ then $h(x) \coloneqq g(x + a)$ is also an arithetic differential operator of order m. With this fact and without any loss of generality, we may assume that the function f in the statement of the Theorem is zero on all discs of radius $\frac{1}{p^m}$ except for $p^m\mathbb{Z}_p$. Again, we may assume with no loss of generality that there exists an $l \geq 0$ such that $f(p^m u) = u^l$ for all $u \in \mathbb{Z}_p$. We recall the set $C_m = \{a_0, \ldots a_{p^{m-1}}\}$. The family of discs $\{a + p^m\mathbb{Z}_p\}_{a\in C_m}$ forms a covering of $\mathbb{Z}_p$. It is worth noting that $a_0 = 0$. Applying Lemma 1, for $a \in C_m$, and $0 \leq k \leq m$, we have $\delta^k(a + p^m u) = \sum_{j=0}^{p^m} c_{a,\,j} u^j$ with $c^k_{a,\,0} = \delta^k a$, and

$$\|c^k_{a,\,0}\|_p \leq 1\,, \quad \|c^k_{a,\,1}\|_p = \frac{1}{p^{m-k}}\,, \quad \|c^k_{a,\,j}\|_p \leq \frac{1}{p^{(m-k+1)j-1}}\,,\ 2 \leq j \leq p^k\,.$$

We may consider $\delta^k(a + p^m u)$ as an element in the ring of polynomials $\mathbb{Z}_p[u]$. Since $\delta^m a = 0$, it follows that $c^m_{a,\,j} = 0$. We now proceed inductively to determine coefficients $a_{\beta,\,n}$ in the series F appearing in the statement of the Theorem so that

$$\|a_{\beta,\,n}\|_p \leq \min\left\{1, \frac{1}{p^{n-1}}\right\}\ , \quad n \geq 0\,,\ \beta \in I'\,,$$

and so that, if $F_a(u) = F(a + p^m u)$, for $a \in C_m$, then, viewing these as equalities of functions of $u \in \mathbb{Z}_p$, we have

$$\begin{cases} F_a(u) = u^l \quad \text{if} \ \ a = 0, \\ F_a(u) = 0 \quad \text{if} \ \ a \neq 0. \end{cases}$$

Since each $F_a(u)$ is defined by a restricted power series in $\mathbb{Z}_p[[u]]$, it suffices to check the above as equalities in the ring of formal power series $\mathbb{Z}_p[[u]]$. Consider the polynomials $F_a^k(u) \in \mathbb{Z}_p[u]$ defined by

$$F_a^k(u) \coloneqq \sum_{n=0}^{k} \sum_{\beta \in I'} a_{\beta,\,n} \left(\sum_{j=0}^{p^0} c_{a,\,j}^0 u^j \right)^{\beta_0} \cdots \left(\sum_{j=0}^{p^{m-1}} c_{a,\,j}^{m-1} u^j \right)^{\beta_{m-1}} \left(\sum_{j=1}^{p^m} c_{a,\,j}^m u^j \right)^n$$

We can determine the $a_{\beta,\,n}$s inductively such that they satisfy $\|a_{\beta,\,n}\|_p \leq \min\left\{1, \frac{1}{p^{n-1}}\right\}$ and such that the following congruences hold in the ring $\mathbb{Z}_p[u]$:

$$\begin{cases} F_a^k(u) \equiv u^l \mod u^{k+1} & \text{if } a = 0, \\ F_a^k(u) \equiv 0 \mod u^{k+1} & \text{if } a \neq 0. \end{cases} \tag{1}$$

In what follows we use δ_{ij} to denote the Kronecker symbol. To begin the induction, we choose coefficients $a_{\beta,\,0}$, $\beta \in I'$ such that $\|a_{\beta,\,0}\|_p \leq \min\{1, p\}$ and (1) hold. We can achieve this by solving the system of equations

$$\sum_{\beta \in I'} w_{\alpha\,\beta}\, a_{\beta,\,0} = \delta_{l\,0}\, \delta_{\alpha\,0}\,, \qquad \alpha \in I\ ,$$

where $W = (w_{\alpha\,\beta})$ is the matrix in Lemma 3. By Lemma 3, we can readily solve for the $a_{\beta\,0}$s with the solution being a vector of p-adic integers. Now, for the k-th step of the induction, we notice that for $a = a_\alpha$ the coefficient of u^k in $F_a^k(u)$ is given by

$$(c_{a,\,1}^m)^k \sum_{\beta \in I'} w_{\alpha\,\beta} a_{\beta\,k} + \sum_{n=0}^{k-1} \sum_{\beta \in I'} a_{\beta,\,n} b_{\beta,\,n,\,k}\ ,$$

where $b_{\beta,\,n,\,k}$ is the coefficient of u^k in

$$\left(\sum_{j=0}^{p^0} c_{a,\,j}^0 u^j \right)^{\beta_0} \cdots \left(\sum_{j=0}^{p^{m-1}} c_{a,\,j}^{m-1} u^j \right)^{\beta_{m-1}} \left(\sum_{j=1}^{p^m} c_{a,\,j}^m u^j \right)^n \ .$$

Now we have that $b_{\beta,\,n,\,k}$ is a $\mathbb{Z}$-linear combination of products of the form

$$\left(\prod_{i=1}^{\beta_0} c^{0}_{a,\,j_{0,\,i}}\right)\cdots\left(\prod_{i=1}^{\beta_{m-1}} c^{m-1}_{a,\,j_{m-1,\,i}}\right)\left(\prod_{i=1}^{n} c^{m}_{a,\,j_{m-1,\,i}}\right)\ ,$$

with

$$\sum_{r=0}^{m-1}\sum_{i=1}^{\beta_r} j_{ri} + \sum_{i=1}^{n} j_{mi} = k\ .$$

Now, let s_r be such that $j_{ri} \geq 1$ for $i \leq s_r$ and $j_{ri} = 0$ for $i > s_r$. So we have

$$s_r \leq \sum_{i=1}^{s_r} j_{ri}\ , \qquad \sum_{r=0}^{m-1}\sum_{i=1}^{s_r} j_{ri} + \sum_{j=1}^{n} j_{mi} = k\,. \tag{2}$$

By the estimates in Lemma 1 and applying the inductive hypothesis,

$$\|a_{\beta,\,n} b_{\beta,\,n,\,k}\|_p \leq \min\left\{1, \frac{1}{p^{n-l+\sigma}}\right\}\ . \tag{3}$$

where

$$\sigma = \sum_{r=0}^{m-1}[(m-r+1)\sum_{i=1}^{s_r} j_{ri}] + \sum_{i=1}^{n} j_{mi} - n\ . \tag{4}$$

Now, by (2), we have that

$$\begin{aligned}\sigma &\geq \sum_{r=0}^{m-1}[2\left(\sum_{i=1}^{s_r} j_{ri}\right) - s_r] + \sum_{i=1}^{n} j_{mi} - n \\ &\geq \sum_{r=0}^{m-1}\sum_{i=1}^{s_r} j_{ri} + \sum_{i=1}^{n} j_{mi} - n \\ &= k - n\ .\end{aligned}$$

Hence,

$$\|a_{\beta,\,n} b_{\beta,\,n,\,k}\|_p \leq \min\left\{1, \frac{1}{p^{k-l}}\right\}\ . \tag{5}$$

Now, the inductive hypothesis also give us that $F^k_a(u)$ satisfies (1) if we have

$$\sum_{\beta\in I'} w_{\alpha\,\beta} a_{\beta,\,k} = (c^{m}_{a_\alpha,\,1})^{-k}\left(\delta_{kl}\delta_{\alpha 0} - \sum_{n=1}^{k-1}\sum_{\beta\in I'} a_{\beta,\,n} b_{\beta,\,n,\,k}\right),\ \alpha \in I\,. \tag{6}$$

By the estimates established in Lemma 1 and by (5), the p-adic norm of the right hand side of (6) is bounded above by $\min\left\{1, \frac{1}{p^{k-1}}\right\}$. Applying Lemma 3, we can solve the system (6) for the $a_{\beta,k}$s with the solution satisfying

$$\|a_{\beta,n}\|_p \leq \min\left\{1, \frac{1}{p^{n-1}}\right\} \ , \quad n \geq 0\,,\ \beta \in I'\,.$$

This completes the induction and we have established the existence of the desired restricted power series. In order to show uniqueness, we need to demonstrate that if a restricted power series F satisfies condition (i) and (ii) in the statement of Theorem 3 for $f = 0$, then $a_{\beta,n} = 0$ for all $\beta \in I', n \geq 0$. This follows at once from an induction on n in view of the equalities

$$\sum_{\beta \in I'} w_{\alpha\beta} a_{\beta,k} = -(c^m_{a_\alpha,1})^{-k} \left(\sum_{n=0}^{k-1} \sum_{\beta \in I'} a_{\beta,n} b_{\beta,n,k} \right) \ , \ \alpha \in I\,.$$

This completes the proof. □

Extending to the Multivariate Case

We now seek to adapt our definitions and notation to facilitate extending our result to the multivariate case. Let p be a fixed prime integer.As the quotient operator is analogous to the derivative, we adopt prime notation for convenience. We consider the *Fermat quotient operator* on $\mathbb{Z}_p^r$ as

$$a' = \delta a = \delta(a_1, \dots a_r) = (\delta a_1, \dots \delta a_r) = (a_1', \ \dots, \ a_r')$$

for $a \in \mathbb{Z}_p^r$ and we denote the i-th iterate of δ as $\delta^{(i)}$. Given a set of non-negative integers, $i_j^{(s)}$ for each $j \in \{1, \dots, r\}$ and for each $s \in \{0, \dots, m\}$, we can form the following:

$$I = (i_1, \dots, i_r), \ I' = (i_1', \dots, i_r'), \ \dots \ , I^{(m)} = (i_1^{(m)}, \dots, i_r^{(m)})$$

with $\mathbf{I} = (I, I', \dots, I^{(m)})$. We shall say that $|\mathbf{I}| \geq 0$ if $|\mathbf{I}| = \sum_{s=0}^{m} \sum_{j=1}^{r} i_j^{(s)}$ and use the expression

$$x^I (x')^{I'} (x'')^{I''} \dots \ (x^{(m)})^{I^{(m)}}$$

to denote the quantity

$$x_1^{i_1} \dots x_r^{i_r} (x_1')^{i_1'} \dots (x_r')^{i_r'} \dots (x_1^{(m)})^{i_1^{(m)}} \dots (x_r^{(m)})^{i_r^{(m)}}.$$

Recall that

$$F(x) = \sum_{\mathbf{I} \geq 0} a_{\mathbf{I}} x^I (x')^{I'} \dots (x^{(m)})^{I^{(m)}} \in \mathbb{Z}_p[[x_1, \dots, x_r, x_1', \dots, x_r', \dots, x_1^{(m)}, \dots, x_r^{(m)}]]$$

is said to be a *restricted power series* if $\lim_{|\mathbf{I}| \to \infty} a_{\mathbf{I}} = 0$.

Definition 3. A function $f\colon \mathbb{Z}_p^r \to \mathbb{Z}_p$ is called an

arithmetic differential operator of order m if there exists a restricted power series

$$F \in \mathbb{Z}_p[[x_1, \ldots, x_r, x_1', \ldots, x_r', \ldots, x_1^{(m)}, \ldots, x_r^{(m)}]]$$

such that

$$f(a) = F(a_1, \ldots, a_r, \delta a_1, \ldots, \delta a_r, \ldots, \delta^m a_1, \ldots, \delta^m a_r)$$

for all $a \in \mathbb{Z}_p^r$. We say that the series F δ-represents f.

Definition 4. A function $f\colon \mathbb{Z}_p^r \to \mathbb{Z}_p$ is said to be *analytic of level m* if for any $a \in \mathbb{Z}_p^r$ there exists a restricted power series $F_a \in \mathbb{Z}_p[[u]]$ such that $f(a + p^m u) = F_a(u)$ for all $u \in \mathbb{Z}_p^r$.

We say the collection of series F_a represents f.

Theorem 4. *Any arithmetic differential operator $f\colon \mathbb{Z}_p^r \to \mathbb{Z}_p$ of order m is an analytic function of level m.*

Proof. Let $f\colon \mathbb{Z}_p^r \to \mathbb{Z}$ be an arithmetic differential operator of order m. Then there exists a restricted power series

$$F \in \mathbb{Z}_p[[x_1, \ldots, x_r, x_1', \ldots, x_r', \ldots, x_1^{(m)}, \ldots, x_r^{(m)}]]$$

such that

$$f(x) = \sum_{\mathbf{I} \geq 0} a_{\mathbf{I}}\, x^I (x')^{I'} \ldots (x^{(m)})^{I^{(m)}}$$

for all $x \in \mathbb{Z}_p^r$.

Let $\mathbf{T} = \{0, 1, \ldots, p^m - 1\}$. We have that $\mathbb{Z}_p^r = \bigcup (a + p^m \mathbb{Z}_p^r)$ and

$a = (a_1, \ldots, a_r)$, $a_i \in \mathbf{T}$. Now, by lemma 10, we have that if $a \in \mathbf{T}^r$ and $x = a + p^n u$

in the set $a + p^n\mathbb{Z}_p^r$, we can express $\delta^k x$ as a polynomial function of u of degree p^k.

$$\delta^k x = (\delta^k x_1, \delta^k x_2, \ \dots \ , \delta^k x_r) = (\sum_{j=0}^{p^k} c_{a,j,1}^k u_1^j, \sum_{j=0}^{p^k} c_{a,j,2}^k u_2^j, \dots, \sum_{j=0}^{p^k} c_{a,j,r}^k u_r^j \ )$$

Thus, we have that $f(a + p^m u) = F_a(u)$ where $F_a(u) =$

$$\sum_{\mathbf{I}} a_{\mathbf{I}} \left(\sum_{j_0=0}^{p^0} c_{a,j_0,1}^0 u_1^{j_0} \right)^{i_1} \dots \left(\sum_{j_0=0}^{p^0} c_{a,j_0,r}^0 u_r^{j_0} \right)^{i_r} \dots \left(\sum_{j_m=0}^{p^m} c_{a,j_m,1}^m u_1^{j_m} \right)^{i_1^{(m)}} \dots \left(\sum_{j_m=0}^{p^m} c_{a,j_m,r}^m u_r^{j_m} \right)^{i_r^{(m)}}$$

with all the $c_{a,j_i,t}^k \in \mathbb{Z}_p$ and the p-adic norm $\|c_{a,j_i,t}^k\|_p \leq 1$ as in Lemma 1. Thus, as $a_{\mathbf{I}} \to 0$ p-adically, we have that $F_a(u)$ is a power series in u $\in \mathbb{Z}_p^r$ with $\mathbb{Z}_p$-coefficients that tend toward zero p-adically as $|\mathbf{I}| \to \infty$ □

It is natural to make the following conjecture:

Conjecture 1. *Any analytic function $f\colon \mathbb{Z}_p^r \to \mathbb{Z}_p$ of level m is an arithmetic differential operator of order m.*

References

[1] A. Buium, *Arithmetic Differential Equations*, Math. Surveys and Monographs, 118, American Mathematical Society, Providence, RI, 2005. xxxii+310 pp.

[2] A. Buium, C. Ralph, and S. Simanca, Arithmetic differential operators on $\mathbb{Z}_p$, J. Number Theory 131 (2011), pp. 96-105.

[3] A. Buium, Differential characters of Abelian varieties over p-adic fields, Invent. Math., 122, 2, (1995), 309-340