THE MAXIMUM LENGTH FOR DUCCI SEQUENCES ON $\mathbb{Z}_M^N$ WHEN N IS EVEN

Mark L. Lewis
Department of Mathematical Sciences, Kent State University, Kent, Ohio
lewis@math.kent.edu

Shannon M. Tefft
Department of Mathematical Sciences, Kent State University, Kent, Ohio
stefft@kent.edu

Received: 12/20/24, Accepted: 12/28/25, Published: 1/19/26

Abstract

Let $D : \mathbb{Z}_m^n \to \mathbb{Z}_m^n$ be defined so

$$D(x_1, x_2, ..., x_n) = (x_1 + x_2 \pmod m), x_2 + x_3 \pmod m), ..., x_n + x_1 \pmod m)).$$

This function D is known as the Ducci function and for $\mathbf{u} \in \mathbb{Z}_m^n$, $\{D^\alpha(\mathbf{u})\}_{\alpha=0}^\infty$ is the Ducci sequence of $\mathbf{u}$. Every Ducci sequence enters a cycle because $\mathbb{Z}_m^n$ is finite. In this paper, we aim to establish an upper bound for how long it will take for a Ducci sequence in $\mathbb{Z}_m^n$ to enter its cycle when n is even.

1. Introduction

We focus on an endomorphism, D, on $\mathbb{Z}_m^n$ such that

$$D(x_1, x_2, ..., x_n) = (x_1 + x_2 \pmod m), x_2 + x_3 \pmod m), ..., x_n + x_1 \pmod m)).$$

We call D the *Ducci function*, similar to [2], [7], and [9]. If $\mathbf{u} \in \mathbb{Z}_m^n$, then $\{D^\alpha(\mathbf{u})\}_{\alpha=0}^\infty$ is known as the *Ducci sequence of* $\mathbf{u}$. Because $\mathbb{Z}_m^n$ is finite, every Ducci sequence eventually enters a cycle. We have a specific name for this cycle, which we give in the following definition.

Definition 1. The *Ducci cycle of* $\mathbf{u}$ is

$$\{\mathbf{v} \mid \text{there exists } \alpha \in \mathbb{Z}^+ \cup \{0\}, \beta \in \mathbb{Z}^+ \text{ such that } \mathbf{v} = D^{\alpha+\beta}(\mathbf{u}) = D^\alpha(\mathbf{u})\}.$$

The *length of* $\mathbf{u}$, $\text{Len}(u)$, is the smallest α satisfying the equation

$$\mathbf{v} = D^{\alpha+\beta}(\mathbf{u}) = D^\alpha(\mathbf{u})$$

DOI: 10.5281/zenodo.18304994

for some $v \in \mathbb{Z}_m^n$ and the *period of* $\mathbf{u}$, $\mathrm{Per}(\mathbf{u})$, is the smallest β that satisfies the equation.

To see this in action, let us look at the Ducci sequence of $(0,0,0,1) \in \mathbb{Z}_5^4$: $(0,0,0,1),(0,0,1,1),(0,1,2,1),(1,3,3,1),(4,1,4,2),(0,0,1,1)$. From here, we can see that the Ducci cycle of $(0,0,0,1)$ is $(0,0,1,1)$, $(0,1,2,1)$, $(1,3,3,1)$, and $(4,1,4,2)$. We can also determine that $\mathrm{Len}(0,0,0,1) = 1$ and $\mathrm{Per}(0,0,0,1) = 4$.

The tuple $(0,0,0,1)$ and any tuple of the form $(0,0,...,0,1) \in \mathbb{Z}_m^n$ are important when it comes to Ducci sequences. The Ducci sequence of $(0,0,...,0,1) \in \mathbb{Z}_m^n$ is called the *basic Ducci sequence of* $\mathbb{Z}_{\mathbf{m}}^{\mathbf{n}}$. This definition is first used in [7, page 302]. We also define

$$\mathbf{P_m(n)} = \mathrm{Per}(0,0,...,0,1)$$

and

$$\mathbf{L_m(n)}^1 = \mathrm{Len}(0,0,...,0,1).$$

Using these, our example from the previous paragraph tells us that $P_5(4) = 4$ and $L_5(4) = 1$. These values are significant because by [2, Lemma 1], if $\mathbf{u} \in \mathbb{Z}_m^n$, then $\mathrm{Len}(\mathbf{u}) \leq L_m(n)$ and $\mathrm{Per}(\mathbf{u}) | P_m(n)$. Therefore, $P_m(n)$ and $L_m(n)$ provide a maximal value for $\mathrm{Per}(\mathbf{u})$ and $\mathrm{Len}(\mathbf{u})$, respectively, for any $\mathbf{u} \in \mathbb{Z}_m^n$.

For the rest of this paper, we are most interested in the value of $L_m(n)$, particularly when n is even. Our goal is to prove the following theorem.

Theorem 1. *Let n be even. Then the following are true.*

1. *If $gcd(n,m) = 1$, then $L_m(n) = 1$.*
2. *If there exists p prime, $k, n_1, m_1 \in \mathbb{Z}^+$, such that $n = p^k n_1$, $m = pm_1$, $gcd(n_1, m_1) = 1$, and $p \nmid n_1, m_1$, then $L_m(n) = p^k$.*
3. *If there exists p prime and $k, l, n_1, m_1 \in \mathbb{Z}^+$ such that $n = p^k n_1$, $m = p^l m_1$, $gcd(n_1, m_1) = 1$, and $p \nmid n_1, m_1$, then $L_m(n) \leq p^{k-1}(l(p-1)+1)$.*
4. *If there exists $p_1, p_2, ..., p_t$ prime where $p_1 < p_2 < \cdots < p_t$, for $1 \leq i \leq t$, and $n = p_1^{k_1} p_2^{k_2} \cdots p_t^{k_t} n_1$, $m = p_1^{l_1} p_2^{l_2} \cdots p_t^{l_t} m_1$ with $gcd(n_1, m_1) = 1$ and $p_i \nmid n_1, m_1$ for every i, then*
$$L_m(n) = max\{L_{p_i^{l_i}}(n) \mid 1 \leq i \leq t\}.$$

It is worth noting that we believe that the inequality in Part (3) of Theorem 1 is, in fact, an equality. We are able to confirm this is true for all $m \leq 50$ and even $n \leq 20$ where $gcd(n,m)$ is a power of a prime. We would test for larger n, m, but our program for computing $L_m(n)$ requires first finding $P_m(n)$, which typically gets

[1] Both of these notations are very similar to how [2, Definition] defines them, and for $P_m(n)$, the notation is also like [7] and [9].

larger as n, m increase. The values of $P_m(n)$ get too large for our MATLAB [13] program to find.

The work in this paper was done while the second author was a Ph.D. student at Kent State University under the advisement of the first author and appeared as part of the second author's dissertation, found at [16].

2. Background

The Ducci function was originally defined as an endomorphism on $\mathbb{Z}^n$ or $(\mathbb{Z}^+ \cup \{0\})^n$ such that $\bar{D}(x_1, x_2, ..., x_n) = (|x_1 - x_2|, |x_2 - x_3|, ..., |x_n - x_1|)$, with this being the most common definition of the Ducci function. Note that if $\bar{D}$ is defined on $\mathbb{Z}^n$, then $\bar{D}(\mathbf{u}) \in (\mathbb{Z}^+ \cup \{0\})^n$. Therefore, for simplicity, we will refer to both of these cases as Ducci on $\mathbb{Z}^n$. Other papers, including [3], [5], and [14], use the same formula for $\bar{D}$ but define Ducci on $\mathbb{R}^n$. It is, of course, necessary that we handle the cases of Ducci on $\mathbb{Z}^n$ and on $\mathbb{R}^n$ separately.

Ducci sequences on $\mathbb{Z}^n$ also always enter a cycle. There are discussions of why this happens in [4], [7], [9], and [12]. A well-known fact for Ducci functions on $\mathbb{Z}^n$ is proved in [12, Lemma 3]: all of the entries of a tuple in a Ducci cycle belong to $\{0, c\}$ for some $c \in \mathbb{Z}^+$. Since $\bar{D}(\lambda\mathbf{u}) = \lambda\bar{D}(\mathbf{u})$ for all $\mathbf{u} \in \mathbb{Z}^n$, this means that we can focus on when Ducci is defined on $\mathbb{Z}_2$ where we are using our definition of D given at the beginning of the paper, particularly when examining Ducci cycles. Because of the significance of Ducci on $\mathbb{Z}_2^n$ to the original Ducci case, this leads us to wonder what happens if we define Ducci on $\mathbb{Z}_m^n$ for other values of m using our definition given at the beginning of the paper. The first paper to look at Ducci on $\mathbb{Z}_m^n$ is [17].

When looking at $L_2(n)$ in particular, [7, page 303] is the first to show that $L_2(n) = 1$ when n is odd. When n is even, [9, Theorem 6] tells us that if $n = 2^{k_1} + 2^{k_2}$ where $k_1 > k_2 \geq 0$, then $L_2(n) = 2^{k_2}$. This is then extended by [1, Theorem 4] to all even $n = 2^k n_1$ where n_1 is odd. Here, $L_2(n) = 2^k$. Notice that this supports Part (2) of Theorem 1 when $m = p = 2$.

If we allow n to be odd, we have a formula for $L_m(n)$ from [11, Theorem 2]. Specifically, if $m = 2^l m_1$ where n, m_1 are odd, then $L_m(n) = l$. For a case where n is even, [10, Theorem 2] proves that if $n = 2^k$ and $m = 2^l$, then $L_m(n) = 2^{k-1}(l+1)$.

Before moving on, we would also like to give a few definitions that will be useful later. If $\mathbf{u}, \mathbf{v} \in \mathbb{Z}_m^n$, then $\mathbf{v}$ is a *predecessor* to $\mathbf{u}$ if $D(\mathbf{v}) = \mathbf{u}$. We let $\mathbf{K}(\mathbb{Z}_\mathbf{m}^\mathbf{n})$ be the set of all tuples in a Ducci cycle. It is stated that $K(\mathbb{Z}_m^n)$ is a subgroup of $\mathbb{Z}_m^n$ in [2, page 6001]. A proof of this is provided in [10, Theorem 1].

We now consider another example of a Ducci sequence and its cycle. For this, we will look at the basic Ducci sequence of $\mathbb{Z}_2^6$. We create a transition graph that maps out all Ducci sequences on $\mathbb{Z}_2^6$ and then look at the connected component that

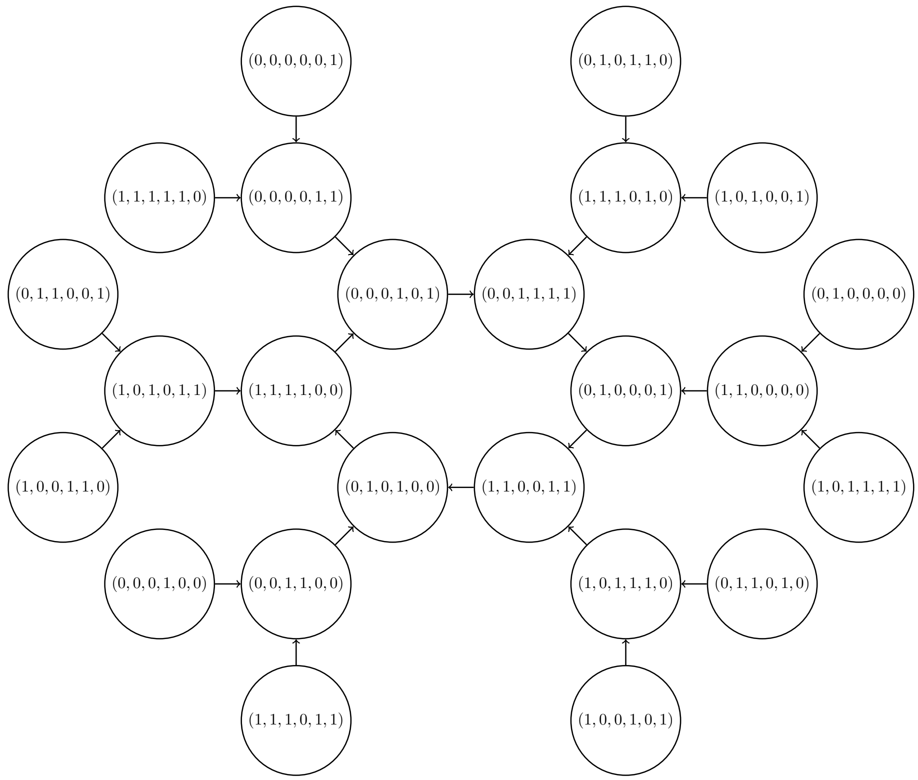

Figure 1: Transition Graph for $\mathbb{Z}_2^6$

includes the basic Ducci sequence. This connected component is given in Figure 1. Notice that we can determine that $L_2(6) = 2$ from Figure 1, which agrees with Theorem 1. We can also see that $P_2(6) = 6$. It is worth noting that every tuple in Figure 1 that has a predecessor has exactly two, which is the same as our m in this case. This is because of [10, Theorem 4], which says that if n is even, then every tuple that has a predecessor has exactly m predecessors. This theorem also tells us that if $\mathbf{u} \in \mathbb{Z}_m^n$ has a predecessor, call it $(x_1, x_2, ..., x_n)$, then the remaining predecessors are of the form

$$(x_1 + z, x_2 - z, x_3 + z, ..., x_n - z)$$

for some $z \in \mathbb{Z}_m$ and all tuples of this form are predecessors to $\mathbf{u}$. All of the tuples in the transition graph in Figure 1 that have a predecessor, call them $(x_1, x_2, ..., x_n)$, also satisfy the condition that $x_1 - x_2 + x_3 - \cdots - x_n \equiv 0 \pmod 2$. In fact, the following theorem addresses this.

Theorem 2. *Let n be even. Then $(x_1, x_2, ..., x_n) \in \mathbb{Z}_m^n$ has a predecessor if and only if $x_1 - x_2 + x_3 - x_4 + \cdots + x_{n-1} - x_n \equiv 0 \pmod{m}$.*

We first note that [12, Lemma 5] proves that this is true for $m = 2$ and [2, Lemma 4] proves it is true when m is prime.

Proof of Theorem 2. For the forward direction, assume $(x_1, x_2, ..., x_n)$ has a predecessor $(y_1, y_2, ..., y_n)$. Then

$$
\begin{aligned}
y_1 + y_2 &\equiv x_1 \pmod{m} \\
y_2 + y_3 &\equiv x_2 \pmod{m} \\
&\vdots \\
y_n + y_1 &\equiv x_n \pmod{m}.
\end{aligned} \tag{2.1}
$$

Subtracting the second congruence from the first yields

$$y_1 - y_3 \equiv x_1 - x_2 \pmod{m}.$$

Adding this to the third congruence produces $y_1 + y_4 \equiv x_1 - x_2 + x_3 \pmod{m}$. Continuing creates the congruences

$$y_1 - y_{n-1} \equiv x_1 - x_2 + \cdots - x_{n-2} \pmod{m}$$

and

$$y_1 + y_n \equiv x_1 - x_2 + \cdots + x_{n-1} \pmod{m}.$$

Using this and Congruence (2.1), we see that

$$x_n \equiv x_1 - x_2 + \cdots + x_{n-1} \pmod{m},$$

which gives

$$x_1 - x_2 + \cdots + x_{n-1} - x_n \equiv 0 \pmod{m},$$

and the forward direction follows.

For the backward direction, assume $x_1 - x_2 + x_3 - x_4 + \cdots + x_{n-1} - x_n \equiv 0 \pmod{m}$. It suffices to show that there exist $y_1, y_2, ..., y_n$ that satisfy the congruences

$$
\begin{aligned}
y_1 + y_2 &\equiv x_1 \pmod{m} \\
y_2 + y_3 &\equiv x_2 \pmod{m} \\
&\vdots \\
y_n + y_1 &\equiv x_n \pmod{m}.
\end{aligned}
$$

Let $y_1 = 0$. If we let $y_2 = x_1$, then the first congruence will be satisfied. If we then let $y_3 = x_2 - x_1$, the second congruence will be satisfied. If we continue this, following the structure $y_j = x_{j-1} - x_{j-2} + \cdots + x_1$ when j is even and $y_j = x_{j-1} - x_{j-2} + \cdots - x_1$ when j is odd, then the first $n-1$ congruences will be satisfied. This results in $y_n = x_{n-1} - x_{n-2} + \cdots + x_1$. We then see that

$$y_1 + y_n \equiv x_{n-1} - x_{n-2} + \cdots + x_1 \pmod{m}.$$

By assumption, $x_{n-1} - x_{n-2} + \cdots + x_1 \equiv x_n \pmod{m}$ and $y_1 + y_n \equiv x_n \pmod{m}$ follow, and the final congruence is satisfied. Therefore, $(x_1, x_2, ..., x_n)$ has at least one predecessor, $(y_1, y_2, ..., y_n)$. □

Moving forward, if $\mathbf{u} \in \mathbb{Z}_m^n$, it will be useful to have a tool that gives us information about tuples in the Ducci sequence of $\mathbf{u}$. To do this, let us first look at the first few tuples in the Ducci sequence of a tuple $(x_1, x_2, ..., x_n) \in \mathbb{Z}_m^n$:

$$\begin{gathered}
(x_1, x_2, ..., x_n) \\
(x_1 + x_2, x_2 + x_3, ..., x_n + x_1) \\
(x_1 + 2x_2 + x_3, x_2 + 2x_3 + x_4, ..., x_n + 2x_1 + x_2) \\
(x_1 + 3x_2 + 3x_3 + x_4, x_2 + 3x_3 + 3x_4 + x_5, ..., x_n + 3x_1 + 3x_2 + x_3) \\
\vdots
\end{gathered}$$

.

We can see that the coefficients of the x_j in the first entry of each tuple in the Ducci sequence occur in all of the entries of that tuple for some x_i. For this reason, we will let $a_{r,s}$ represent the coefficient of x_s in the first entry of $D^r(x_1, x_2, ..., x_n)$. Here $r \geq 0$ and $1 \leq s \leq n$. The s-coordinate reduces modulo n, with the exception that we write $a_{r,n}$ instead of $a_{r,0}$. Note that $a_{r,s}$ also appears as the coefficient of x_{s-i+1} in the ith entry of $D^r(x_1, x_2, ..., x_n)$. A more thorough explanation of why we can do this can be found in [10, page 6]. We also have that

$$D^r(0, 0, ..., 0, 1) = (a_{r,n}, a_{r,n-1}, ..., a_{r,1}).$$

Additionally, by [10, Theorem 5], when $r < n$, we have $a_{r,s} = \binom{r}{s-1}$. This theorem also tells us that $a_{r,s} = a_{r-1,s} + a_{r-1,s-1}$, and more generally that

$$a_{r+t,s} = \sum_{i=1}^{n} a_{t,i} a_{r,s-i+1}$$

when $t \geq 1$.

3. Proving the Main Theorem

Before we can prove Theorem 1, there are a few lemmas that we will need. We begin with two lemmas about particular binomial coefficients. We believe that both Lemmas 1 and 2 are known and have been proven before, but we are providing proofs here for completeness.

Lemma 1. *Let p be prime and $j \leq p^k - 1$, $k \geq 1$. Then*

$$\binom{p^k - 1}{j} \equiv (-1)^j \ (mod\, p).$$

Proof. To prove this, we will do induction on j. Our base case is when $j = 0$, which is satisfied by $\binom{p^k-1}{0} = 1$. For our inductive step, assume

$$\binom{p^k - 1}{j-1} \equiv (-1)^{j-1} \ (\text{mod } p).$$

Note

$$\binom{p^k}{j} = \binom{p^k - 1}{j} + \binom{p^k - 1}{j-1}.$$

Because we proved the $j = 0$ case in the base case, we can assume $0 < j \leq p^k - 1$, which will give us

$$\binom{p^k - 1}{j} + \binom{p^k - 1}{j-1} \equiv 0 \ (\text{mod } p).$$

Solving for $\binom{p^k-1}{j}$, we find that

$$\binom{p^k - 1}{j} \equiv -\binom{p^k - 1}{j-1} \ (\text{mod } p).$$

By induction, $\binom{p^k-1}{j}$ is congruent to

$$-(-1)^{j-1}$$

modulo p or

$$(-1)^j$$

modulo p, and the lemma follows. □

The next lemma is similar to Lemma 1.

Lemma 2. *For $k > 1$ and p an odd prime*

$$\binom{p^k - p^{k-1}}{j} \equiv \begin{cases} (-1)^c \ (mod\, p) & j = cp^{k-1} \\ 0 \ (mod\, p) & otherwise. \end{cases}$$

Proof. We prove this via induction on j. Our base case covers when $j = 0, 1$, which follow from

$$\binom{p^k - p^{k-1}}{0} \equiv 1 \pmod{p}$$

and

$$\binom{p^k - p^{k-1}}{1} \equiv 0 \pmod{p}.$$

For our inductive step, assume that the lemma is true for $j^* < j$. For $j > 0$, we use the Chu–Vandermonde identity, which says that

$$\sum_{\gamma=0}^{\delta} \binom{\alpha}{\gamma}\binom{\beta}{\delta-\gamma} = \binom{\alpha+\beta}{\delta}.$$

A proof of this can be found in [15, Identity 57]. As a result,

$$\binom{p^k}{j} = \sum_{i=0}^{j} \binom{p^{k-1}}{i}\binom{p^k - p^{k-1}}{j-i} \equiv 0 \pmod{p}. \tag{3.1}$$

If $j < p^{k-1}$, the sum in Equation (3.1) is also congruent to

$$\binom{p^{k-1}}{0}\binom{p^k - p^{k-1}}{j}$$

modulo p, in addition to being congruent to 0 modulo p, so $\binom{p^k - p^{k-1}}{j}$ is congruent to 0 modulo p. If $j \geq p^{k-1}$, the sum in Equation (3.1) is congruent to

$$\binom{p^{k-1}}{0}\binom{p^k - p^{k-1}}{j} + \binom{p^{k-1}}{p^{k-1}}\binom{p^k - p^{k-1}}{j - p^{k-1}}$$

modulo p. This sum is congruent to 0 modulo p by Equation (3.1), which produces

$$\binom{p^k - p^{k-1}}{j} \equiv -\binom{p^k - p^{k-1}}{j - p^{k-1}} \pmod{p}.$$

If $j \neq cp^{k-1}$ for some c, then $\binom{p^k - p^{k-1}}{j}$ is congruent to 0 modulo p by induction. If $j = cp^{k-1}$ for some c, then $\binom{p^k - p^{k-1}}{j}$ is congruent to $-(-1)^{c-1}$ modulo p or $(-1)^c$ modulo p, and the lemma follows. □

Next, we would like to look at the $a_{r,s}$ coefficient for a particular r in Lemmas 3 and 4.

Lemma 3. *Let $n = p^k n_1$ where p is prime, $n_1 > 1$, and $c \geq 1$. Then for $s \neq bp^k + 1$ and $0 \leq b < n_1$, we have $a_{cp^k,s} \equiv 0 \ (mod\, p)$.*

Proof. We prove this via induction on c with our base case being when $c = 1$, which, by [10, Theorem 5] follows from

$$a_{p^k,s} = \binom{p^k}{s-1} \equiv 0 \pmod{p}$$

precisely when $s \neq 1, p^k + 1$. For the inductive step, assume

$$a_{(c-1)p^k,s} \equiv 0 \pmod{p}$$

for $s \not\equiv b'p^k + 1 \pmod{n}$, $0 \leq b' \leq n_1 - 1$. Using [10, Theorem 5], we can break down $a_{cp^k,s}$ as follows:

$$a_{cp^k,s} = \sum_{i=1}^{n} a_{p^k,i} a_{(c-1)p^k,s-i+1}. \tag{3.2}$$

Using $a_{p^k,i} = \binom{p^k}{i-1}$, Equation (3.2) is congruent to

$$a_{p^k,1} a_{(c-1)p^k,s} + a_{p^k,p^k+1} a_{(c-1)p^k,s-p^k}$$

modulo p. Notice that for $s \not\equiv bp^k + 1 \pmod{n}$, Equation (3.2) is congruent to 0 modulo p where $0 \leq b \leq n_1 - 1$ by induction, and the lemma follows. □

For the remaining cases where $s = bp^k + 1$, we have the following lemma.

Lemma 4. *Let $n = p^k n_1$ for some k and $n_1 > 1$, $a_{r,s}$ be the coefficients for n, and $a^*_{r,s}$ be the coefficients for n_1. Then, for $c \geq 1$ and $0 \leq b < n_1$,*

$$a_{cp^k,bp^k+1} \equiv a^*_{c,b+1} \ (mod\, p).$$

Proof. We prove this via induction on c, starting with the base case of $c = 1$. Notice that because $p^k < n$, we have $a_{p^k,1} = \binom{p^k}{0}$, which is 1. Since $a^*_{1,1} = \binom{1}{0} = 1$, we have that

$$a_{p^k,1} \equiv a^*_{1,1} \pmod{p}.$$

Similarly,

$$a_{p^k,p^k+1} = \binom{p^k}{p^k} = 1$$

and

$$a^*_{1,2} = \binom{1}{1} = 1,$$

so $a_{p^k,p^k+1} \equiv a^*_{1,2} \pmod{p}$. Finally, for $2 \le b < n_1$, because $\binom{p^k}{j_1} \equiv 0 \pmod{p}$ when $j_1 \ne 1, p^k$ and $\binom{1}{j_2} = 0$ when $j_2 > 1$, we have

$$a_{p^k,bp^k+1} \equiv a^*_{1,b+1} \pmod{p}$$

for every $2 \le b < n_1$. The base case follows from here.

Moving on to the inductive step, assume

$$a_{(c-1)p^k,bp^k+1} \equiv a^*_{c-1,b+1} \pmod{p}$$

when $0 \le b < n_1$. Then,

$$a_{cp^k,bp^k+1} = \sum_{i=1}^{n} a_{p^k,i} a_{(c-1)p^k,bp^k+2-i}. \tag{3.3}$$

Notice that $a_{p^k,s} = \binom{p^k}{s-1} \equiv 0 \pmod{p}$ when $s \ne 1, p^k+1$. Therefore, our remaining pieces tell us Equation (3.3) is congruent to

$$a_{p^k,1} a_{(c-1)p^k,bp^k+1} + a_{p^k,p^k+1} a_{(c-1)p^k,(b-1)p^k+1}$$

modulo p. By induction, Equation (3.3) is congruent to

$$a^*_{c-1,b+1} + a^*_{c-1,b}$$

modulo p, which is congruent to $a^*_{c,b+1}$ modulo p and the lemma follows. □

Putting Lemmas 3 and 4 together allows us to visualize what $D^{cp^k}(0,0,...,0,1)$ looks like in $\mathbb{Z}_p^n$ for $n = p^k n_1$:

$$D^{cp^k}(0,0,...,0,1) = (0,0,...,0,a^*_{c,n_1},0,...,0,a^*_{c,n_1-1},0,...,0,a^*_{c,1}). \tag{3.4}$$

Bear in mind that the last set of ... in the right side of Equation (3.4) covers a much larger area then the first two. We now have the pieces we need to prove Theorem 1.

Proof of Theorem 1. Assume n is even. Before proving Part (1) of this theorem, we would like to first note that when m is prime, this case follows from [2, Lemma 5]. Assume that $gcd(n,m) = 1$. We want to prove

$$(0,0,...,0,1,1) \in K(\mathbb{Z}_m^n)$$

and

$$(0,0,...,0,1) \notin K(\mathbb{Z}_m^n).$$

We first use Theorem 2 to note that since $-1 \not\equiv 0 \pmod{m}$, the n-tuple $(0, 0, ..., 0, 1)$ does not have a predecessor and therefore $(0, 0, ..., 0, 1) \notin K(\mathbb{Z}_m^n)$. We now note that $(0, 0, ..., 0, 1, 1)$ has m predecessors and that if any of these predecessors are in the cycle, then so is $(0, 0, ..., 0, 1, 1)$. In addition to this, if there exists $\mathbf{u}, \mathbf{v} \in \mathbb{Z}_m^n$ such that $D^2(\mathbf{v}) = D(\mathbf{u}) = (0, 0, ..., 0, 1, 1)$, then $\mathbf{u} \in K(\mathbb{Z}_m^n)$ because otherwise we would have

$$\text{Len}(\mathbf{v}) > \text{Len}(\mathbf{u}) = \text{Len}(0, 0, ..., 0, 1) = L_m(n),$$

which cannot happen. Since $(0, 0, ..., 0, 1)$ is a predecessor for $(0, 0, ..., 0, 1, 1)$, it follows by [10, Theorem 4] that the other predecessors of $(0, 0, ..., 0, 1, 1)$ will be of the form

$$\mathbf{u} = (z, m - z, z, ..., z, 1 - z)$$

for some nonzero $z \in \mathbb{Z}_m$, so we only need to prove that there exists such a z where $\mathbf{u}$ has a predecessor. By Theorem 2, $\mathbf{u}$ has a predecssor if and only if

$$z - (m - z) + z - (m - z) + \cdots + z - (1 - z) \equiv 0 \pmod{m},$$

or, equivalently,

$$nz - 1 \equiv 0 \pmod{m}.$$

Since $gcd(n, m) = 1$, there exists a unique z such that $nz \equiv 1 \pmod{m}$. Therefore we have a z that satisfies the above and $(z, m - z, z, ..., z, 1 - z)$ has a predecessor. Therefore, $L_m(n) = 1$ and Part (1) follows.

For Part (2) of the theorem, it is worth noting that if $m = p$, then this case follows from [2, Theorem 4]. Assume $n = p^k n_1$, $m = pm_1$ where $gcd(n_1, m_1) = 1$, and $p \nmid n_1, m_1$. We must then start with proving that $L_m(n) \leq p^k$.

Let $P_m(n) = d$. From the first case of this theorem, we know $L_{\frac{m}{p}}(n) = 1$, which means

$$a_{d+1,s} \equiv a_{1,s} \ (\text{mod } \frac{m}{p})$$

or

$$a_{d+1,s} \equiv \begin{cases} 1 \ (\text{mod } \frac{m}{p}) & s = 1, 2 \\ 0 \ (\text{mod } \frac{m}{p}) & \text{otherwise.} \end{cases}$$

We will use this to write

$$a_{d+1,s} \equiv \begin{cases} \delta_s \frac{m}{p} + 1 \pmod{m} & s = 1, 2 \\ \delta_s \frac{m}{p} \pmod{m} & \text{otherwise} \end{cases} \tag{3.5}$$

for some $0 \leq \delta_s < p$. We start by showing $a_{p^k+d,s} \equiv a_{p^k,s} \pmod{m}$ for every s. First,

$$a_{p^k+d,s} = \sum_{i=1}^{n} a_{d+1,i} a_{p^k-1,s-i+1}. \tag{3.6}$$

Substituting in our values for $a_{d+1,s}$ from Congruence (3.5), we see that Equation (3.6) is congruent to

$$(\delta_1 \frac{m}{p} + 1)a_{p^k-1,s} + (\delta_2 \frac{m}{p} + 1)a_{p^k-1,s-1} + \frac{m}{p} \sum_{i=3}^{n} \delta_i a_{p^k-1,s-i+1}$$

modulo m, which after some rearranging is congruent to

$$a_{p^k-1,s} + a_{p^k-1,s-1} + \frac{m}{p} \sum_{i=1}^{n} \delta_i a_{p^k-1,s-i+1}$$

modulo m. Using $a_{r,s} = a_{r-1,s} + a_{r-1,s-1}$ from [10, Theorem 5] and substituting $a_{p^k-1,s-i+1}$ for the appropriate binomial coefficient, Equation (3.6) is congruent to

$$a_{p^k,s} + \frac{m}{p} \sum_{i=1}^{n} \delta_i \binom{p^k-1}{s-i}$$

modulo m. Notice that this base case will follow if $\frac{m}{p} \sum_{i=1}^{n} \delta_i \binom{p^k-1}{s-i} \equiv 0 \pmod{m}$, which will follow if $\sum_{i=1}^{n} \delta_i \binom{p^k-1}{s-i} \equiv 0 \pmod{p}$. Note that in this sum, $\binom{p^k-1}{s-i}$ is nonzero for only p^k many consecutive terms for every s. We would like to use this and the following three claims to prove

$$\sum_{i=1}^{n} \delta_i \binom{p^k-1}{s-i} \equiv 0 \pmod{p}.$$

The claims are as follows:

1. $\delta_s = 0$ as long as $s \neq bp^k + 1, bp^k + 2$ for some $0 \leq b < \frac{n}{p^k}$;

2. $\delta_{bp^k+1} = \delta_{bp^k+2}$, when $0 \leq b < \frac{n}{p^k}$;

3. $\delta_{bp^k+1} + \delta_{(b-1)p^k+2} \equiv 0 \pmod{p}$ where $0 \leq b < \frac{n}{p^k}$.

Notice that $\sum_{i=1}^{n} \delta_i \binom{p^k-1}{s-i} \equiv 0 \pmod{p}$ will follow if all three claims true; the claims will give us that most of the δ_i will be congruent to 0 modulo p, and since at most p^k terms in the sum will already be nonzero, there will only be 2 nonzero terms in the entire sum, as for every p^k consecutive δ_i you pick, only 2 will be nonzero. This leaves us with 2 cases.

In the first case, the two nonzero terms in the sum are adjacent to each other. If p is odd, then because of Claim 1 and Lemma 1, we have that $\sum_{i=1}^{n} \delta_i \binom{p^k-1}{s-i}$ is either congruent to

$$\delta_{bp^k+1} - \delta_{bp^k+2}$$

modulo p or

$$-\delta_{bp^k+1} + \delta_{bp^k+2}$$

modulo p, both of which are congruent to 0 modulo p by Claim 2.

If $p = 2$ for our first case, then by Claim 1 and the well-known Lucas's Theorem (a proof of which can be found in [8, Theorem 1]), the sum

$$\sum_{i=1}^{n} \delta_i \binom{2^k-1}{s-i} \equiv \delta_{2^k b+1} + \delta_{2^k b+2} \pmod{2},$$

which is congruent to 0 modulo 2 by Claim 2, and $L_m(n) \leq p^k$ would follow.

In the second case, the two nonzero terms are p^k terms apart. This will only happen if the remaining terms of $\sum_{i=1}^{n} \delta_i \binom{p^k-1}{s-i}$ are congruent to

$$\delta_{bp^k+1} \binom{p^k-1}{0} + \delta_{(b-1)p^k+2} \binom{p^k-1}{p^k-1}$$

modulo p, which, by Claim 3, would be congruent to 0 modulo p and $L_m(n) \leq p^k$ would follow from here as well.

To prove the claims, note that by [2, Proposition 4], $P_p(p^k n_1) = p^k P_p(n_1)$. We therefore write $d = cp^k$ where $c = P_p(n_1)$. By Lemma 3, $a_{d,s} \equiv 0 \pmod{p}$ where $s \neq bp^k + 1$ for some $0 \leq b \leq \frac{n}{p^k}$. Then for $s \neq bp^k + 1, bp^k + 2$,

$$a_{d+1,s} = a_{d,s} + a_{d,s-1},$$

which is congruent to 0 modulo p. This implies $\delta_s = 0$ for $s \neq bp^k + 1, bp^k + 2$ and Claim 1 follows.

For Claim 2,

$$a_{d+1,bp^k+1} - a_{d+1,bp^k+2} = a_{d,bp^k+1} + a_{d,bp^k} - a_{d,bp^k+2} - a_{d,bp^k+1},$$

which is

$$a_{d,bp^k} - a_{d,bp^k+2} \equiv 0 \pmod{p}$$

because of Lemma 3 and because $p^k | d$. Therefore, Claim 2 follows.

As for Claim 3, we have

$$a_{d+1,bp^k+1} + a_{d+1,(b-1)p^k+2} = a_{d,bp^k+1} + a_{d,bp^k} + a_{d,(b-1)p^k+2} + a_{d,(b-1)p^k+1},$$

which is congruent to

$$a_{d,bp^k+1} + a_{d,(b-1)p^k+1}$$

modulo p. By Lemma 4, this sum is congruent to

$$a^*_{c,b+1} + a^*_{c,b}$$

modulo p or

$$a^*_{c+1,b+1}$$

modulo p, where $a^*_{r,s}$ is the coefficient for n_1. Therefore, by Part (1) of Theorem 1,

$$a_{d+1,bp^k+1} + a_{d+1,(b-1)p^k+2} \equiv \begin{cases} 0 \pmod{p} & b > 1 \\ 1 \pmod{p} & b = 0, 1. \end{cases}$$

For $b > 1$,

$$a_{d+1,bp^k+1} + a_{d+1,(b-1)p^k+2} \equiv (\delta_{bp^k+1} + \delta_{(b-1)p^k+2})\frac{m}{p} \pmod{m},$$

which will give us $\delta_{bp^k+1} + \delta_{(b-1)p^k+2} \equiv 0 \pmod{p}$. For $b = 0, 1$,

$$a_{d+1,bp^k+1} + a_{d+1,(b-1)p^k+2} \equiv (\delta_{bp^k+1} + \delta_{(b-1)p^k+2})\frac{m}{p} + 1 \pmod{m}$$

gives us $\delta_{bp^k+1} + \delta_{(b-1)p^k+2} \equiv 0 \pmod{p}$ for $b = 0, 1$ and Claim 3 follows. Since all three claims follow, this gives us $L_m(n) \leq p^k$.

We now need to prove that $L_m(n) = p^k$. Suppose $L_m(n) \leq p^k - 1$. Then $a_{d+p^k-1,s} \equiv a_{p^k-1,s} \pmod{m}$ for every s and

$$a_{d+p^k-1,s} = \sum_{i=1}^{n} a_{d+1,i}a_{p^k-2,s-i+1}. \tag{3.7}$$

If we separate out the terms where $i = 1, 2$, Equation (3.7) is

$$a_{d+1,1}a_{p^k-2,s} + a_{d+1,2}a_{p^k-2,s-1} + \sum_{i=3}^{n} a_{d+1,i}a_{p^k-2,s-i+1}.$$

Substituting our values for $a_{d+1,s}$ from Congruence (3.5) and binomial coefficients in for $a_{p^k-2,s-i+1}$ into the sum and rearranging, Equation (3.7) is congruent to

$$a_{p^k-2,s} + a_{p^k-2,s-1} + \frac{m}{p}\sum_{i=1}^{n} \delta_s \binom{p^k-2}{s-i}$$

modulo m or

$$a_{p^k-1,s} + \frac{m}{p}\sum_{i=1}^{n} \delta_i \binom{p^k-2}{s-i}$$

modulo m. This implies that $\frac{m}{p}\sum_{i=1}^{n}\delta_i\binom{p^k-2}{s-i} \equiv 0 \pmod{m}$, which produces

$$\sum_{i=1}^{n}\delta_i\binom{p^k-2}{s-i} \equiv 0 \pmod{p}. \tag{3.8}$$

Substituting $\delta_i = 0$ for $i \neq bp^k+1, bp^k+2$ by using Claim 1, Congruence (3.8) is congruent to

$$\sum_{b=0}^{n_1-1}\delta_{bp^k+1}\binom{p^k-2}{s-bp^k-1} + \delta_{bp^k+2}\binom{p^k-2}{s-bp^k-2}$$

modulo p. Using Claim 2, Congruence (3.8) is congruent to

$$\sum_{b=0}^{n_1-1}\delta_{bp^k+1}(\binom{p^k-2}{s-bp^k-1} + \binom{p^k-2}{s-bp^k-2})$$

modulo p or

$$\sum_{b=0}^{n_1-1}\delta_{bp^k+1}\binom{p^k-1}{s-bp^k-1}$$

modulo p. Notice that only one of the $\binom{p^k-1}{s-bp^k-1}$ is not congruent to 0 modulo p. Therefore, we find that $\sum_{i=1}^{n}\delta_i\binom{p^k-2}{s-i}$ is congruent to either

$$\delta_{bp^k+1}$$

modulo p or

$$-\delta_{bp^k+1}$$

modulo p for some $0 \leq b \leq n_1-1$. As long as one of the δ_{bp^k+1} coefficients is nonzero, we have a contradiction. Suppose then that $\delta_{bp^k+1} = 0$ for every b. Then, we would have $L_m(n) = 1$. Then $(0,0,...,0,1,1)$ has a predecessor that is also in the cycle. This is equivalent to one of its predecessors having a predecessor itself. Since one of $(0,0,...,0,1,1)$ is $(0,0,...,0,1)$, all of its other predecessors will be of the form $(z, m-z, z, ..., z, 1-z)$ for some $z \in \mathbb{Z}_m$. Suppose there exists nonzero z such that this tuple has a predecessor. Then it must be true that

$$z + z + z + \cdots + z - 1 + z \equiv 0 \pmod{m},$$

which would suggest $nz \equiv 1 \pmod{m}$. However, since $gcd(n,m) > 1$, we cannot have this and we have a contradiction. Therefore, $L_m(n) = p^k$.

We prove Part (3) of the theorem via induction on l, where Part (2) of this theorem serves as the base case of $l = 1$. Assume that if $n = p^k n_1$, $m^* = p^{l-1} m_1^*$, $gcd(n_1, m_1^*) = 1$, and $p \nmid n_1, m_1^*$, then $L_{m^*}(n) \leq p^{k-1}((l-1)(p-1)+1) = \gamma$. Now assume that $n = p^k n_1$ and $m = p^l m_1$ with $gcd(n_1, m_1) = 1$ and $p \nmid n_1, m_1$. We set out to prove that $L_m(n) \leq \gamma + p^k - p^{k-1}$. Choose d such that $p^k | d$ and $P_m(n) | d$. Then

$$a_{\gamma+d,s} \equiv a_{\gamma,s} \pmod{\frac{m}{p}}.$$

We use this to write

$$a_{\gamma+d,s} \equiv a_{\gamma,s} + \delta_s \frac{m}{p} \pmod{m} \tag{3.9}$$

for some $0 \leq \delta_s < p$. Note also that

$$a_{\gamma+p^k-p^{k-1},s} = \sum_{i=1}^{n} a_{p^k-p^{k-1},i} a_{\gamma,s-i+1}.$$

Since $a_{p^k-p^{k-1},i} = \binom{p^k - p^{k-1}}{i-1}$, we plug these into $a_{p^k-p^{k-1},i}$ to see that the sum above is

$$\sum_{i=1}^{n} \binom{p^k - p^{k-1}}{i-1} a_{\gamma,s-i+1}. \tag{3.10}$$

Now consider $a_{\gamma+p^k-p^{k-1}+d,s}$:

$$a_{\gamma+p^k-p^{k-1}+d,s} = \sum_{i=1}^{n} a_{p^k-p^{k-1},i} a_{\gamma+d,s-i+1}. \tag{3.11}$$

Plugging our values for the $a_{\gamma+d,s-i+1}$ from Equation (3.9) into Equation (3.11), we find that $a_{\gamma+p^k-p^{k-1}+d,s}$ is congruent to

$$\sum_{i=1}^{n} a_{p^k-p^{k-1},i}(a_{\gamma,s-i+1} + \delta_{s-i+1}\frac{m}{p})$$

modulo m. Separating the sums and plugging $a_{p^k-p^{k-1},i} = \binom{p^k - p^{k-1}}{i-1}$ into the sum in the line above, Equation (3.11) is congruent to

$$\sum_{i=1}^{n} \binom{p^k - p^{k-1}}{i-1} a_{\gamma,s-i+1} + \frac{m}{p} \sum_{i=1}^{n} \binom{p^k - p^{k-1}}{i-1} \delta_{s-i+1}$$

modulo m. Using Expression (3.10), Equation (3.11) is congruent to

$$a_{\gamma+p^k-p^{k-1},s} + \frac{m}{p} \sum_{i=1}^{n} \binom{p^k - p^{k-1}}{i-1} \delta_{s-i+1}$$

modulo m. Therefore, we only need that $\sum_{i=1}^{n}\binom{p^k-p^{k-1}}{i-1}\delta_{s-i+1} \equiv 0 \pmod{p}$ to see that

$$L_m(n) \leq \gamma + p^k - p^{k-1}.$$

We consider two cases.

In our first case, we address when p is an odd prime. Note that by Lemma 2, we have

$$\sum_{i=1}^{n}\binom{p^k-p^{k-1}}{i-1}\delta_{s-i+1} \equiv \delta_s - \delta_{s-p^{k-1}} + \delta_{s-2p^{k-1}} - \cdots + \delta_{s-p^k+p^{k-1}} \pmod{p}.$$

Note that

$$(a_{\gamma+d,s} - a_{\gamma,s}) - (a_{\gamma+d,s-p^{k-1}} - a_{\gamma,s-p^{k-1}}) + \cdots + (a_{\gamma+d,s-p^k+p^{k-1}} - a_{\gamma,s-p^k+p^{k-1}}) \tag{3.12}$$

is congruent to

$$\frac{m}{p}(\delta_s - \delta_{s-p^{k-1}} + \cdots + \delta_{s-p^k+p^{k-1}})$$

modulo m. We can show $\delta_s - \delta_{s-p^{k-1}} + \cdots + \delta_{s-p^k+p^{k-1}} \equiv 0 \pmod{p}$ by showing Expression (3.12) is congruent to 0 modulo m. Since we already know that this sum is congruent to 0 modulo $\frac{m}{p}$, it suffices to show Expression (3.12) is congruent to 0 modulo p. Rewriting the sum in Expression (3.12) yields

$$\sum_{i=0}^{p-1}(-1)^i a_{\gamma+d,s-ip^{k-1}} - \sum_{i=0}^{p-1}(-1)^i a_{\gamma,s-ip^{k-1}}. \tag{3.13}$$

Note that if $s \neq bp^{k-1}+1$ for some b, then Expression (3.13) is congruent to 0 modulo p by Lemma 3 and because $p^{k-1}|\gamma, d$. Assume then that $s = bp^{k-1}+1$ for some b. Since $p^k|d$, write $d = cp^k$ for some $c \in \mathbb{Z}^+$, which yields

$$\gamma + d = p^{k-1}((l-1)(p-1)+1+cp).$$

So the first sum in Expression (3.13) is

$$\sum_{i=0}^{p-1}(-1)^i a_{\gamma+d,s-ip^{k-1}} = \sum_{i=0}^{p-1}(-1)^i a_{\gamma+d,(b-i)p^{k-1}+1},$$

which by Lemma 4, is congruent to

$$\sum_{i=0}^{p-1}(-1)^i a^*_{(l-1)(p-1)+1+cp,b-i+1} \tag{3.14}$$

modulo p. By [2, Proposition 4], $P_p(n) = p^k P_p(n_1)$. By [6, Proposition 3.1], $P_p(n)|P_m(n)$. So

$$p^k P_p(n_1)|cp^k$$

and we conclude that $P_p(n_1)|c$. Using this yields that Expression (3.14) is congruent to

$$\sum_{i=0}^{p-1}(-1)^i a^*_{(l-1)(p-1)+1,b-i+1}$$

modulo p. Looking at our other sum in Expression (3.13),

$$\sum_{i=0}^{p-1}(-1)^i a_{\gamma,s-ip^{k-1}} = \sum_{i=0}^{p-1}(-1)^i a_{\gamma,(b-i)p^{k-1}+1},$$

which by Lemma 4 is congruent to

$$\sum_{i=0}^{p-1}(-1)^i a^*_{(l-1)(p-1)+1,b-i+1}$$

modulo p. So we have that Expression (3.13) is

$$\sum_{i=0}^{p-1}(-1)^i a_{\gamma+d,s-ip^{k-1}} - \sum_{i=0}^{p-1}(-1)^i a_{\gamma,s-ip^{k-1}} \equiv 0 \pmod{p},$$

which gives us that $L_m(n) \leq p^{k-1}(l(p-1)+1)$.

In our second case, assume $p = 2$. We want to show $L_m(n) \leq 2^{k-1}(l+1)$. Write $d = 2^k c$. Then the sum we are interested in is

$$\sum_{i=1}^{n}\binom{p^k - p^{k-1}}{i-1}\delta_{s-i+1} = \sum_{i=1}^{n}\binom{2^{k-1}}{i-1}\delta_{s-i+1},$$

which is congruent to

$$\delta_s + \delta_{s-2^{k-1}}$$

modulo 2. Note that

$$(a_{\gamma+d,s} - a_{\gamma,s}) + (a_{\gamma+d,s-2^{k-1}} - a_{\gamma,s-2^{k-1}}) \equiv \frac{m}{2}(\delta_s + \delta_{s-2^{k-1}}) \pmod{m},$$

so similar to before, $\delta_s + \delta_{s-2^{k-1}} \equiv 0 \pmod 2$ if

$$(a_{\gamma+d,s} + a_{\gamma+d,s-2^{k-1}}) - (a_{\gamma,s} + a_{\gamma,s-2^{k-1}}) \equiv 0 \pmod{2}. \tag{3.15}$$

Notice that Congruence (3.15) is congruent to 0 modulo 2 if $s \neq 2^{k-1}b + 1$ for some b. Assume then that $s = 2^{k-1}b + 1$. Then

$$(a_{\gamma+d,s} + a_{\gamma+d,s-2^{k-1}}) - (a_{\gamma,s} + a_{\gamma,s-2^{k-1}})$$
$$= (a_{\gamma+d,2^{k-1}b+1} + a_{\gamma+d,2^{k-1}(b-1)+1}) - (a_{\gamma,2^{k-1}b+1} + a_{\gamma,2^{k-1}(b-1)+1}).$$

Using $\gamma + d = 2^{k-1}((l-1)+1+2c)$, Congruence (3.15) is congruent to

$$(a^*_{(l-1)+1+2c,b+1} + a^*_{(l-1)+1+2c,b}) - (a^*_{(l-1)+1,b+1} + a^*_{(l-1)+1,b})$$

modulo 2. Like before, we still have that $P_p(n_1)|c$, so the left-hand side Congruence (3.15) is congruent to

$$(a^*_{(l-1)+1,b+1} + a^*_{(l-1)+1,b}) - (a^*_{(l-1)+1,b+1} + a^*_{(l-1)+1,b})$$

modulo 2, which is congruent to 0 modulo 2. Therefore, $L_m(n) \leq 2^{k-1}(l+1)$.

Finally, for Part (4), assume $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_t} n_1$ and $m = p_1^{l_1} p_2^{l_2} \cdots p_r^{l_t} m_1$ where p_i is prime, $p_i \nmid n_1, m_1$ for every i and $gcd(n_1, m_1) = 1$. We wish to show that

$$L_m(n) = max\{L_{p_i^{l_i}}(n) \mid 1 \leq i \leq t\}.$$

Let $\gamma_i = L_{p_i^{l_i}}(n)$, $\gamma = max\{\gamma_i \mid 1 \leq i \leq t\}$, and $d = P_m(n)$. We have that

$$a_{\gamma_i+d,s} \equiv a_{\gamma_i,s} \pmod{p_i^{l_i}}$$

$$a_{1+d,s} \equiv a_{1,s} \pmod{m_1}$$

for every s and every i. Then, since $\gamma \geq \gamma_i$ for every i, we have that

$$a_{\gamma+d,s} \equiv a_{\gamma,s} \pmod{p_i^{l_i}}$$

$$a_{\gamma+d,s} \equiv a_{\gamma,s} \pmod{m_1},$$

which gives $a_{\gamma+d,s} \equiv a_{\gamma,s} \pmod{m}$.

If we had that $L_m(n) < \gamma$, then $a_{\gamma+d-1,s} \equiv a_{\gamma-1,s} \pmod{m}$, which implies

$$a_{\gamma+d-1,s} \equiv a_{\gamma-1,s} \pmod{p_i^{l_i}}$$

for every i. But $a_{\gamma+d-1,s} \not\equiv a_{\gamma-1,s} \pmod{p_j^{l_j}}$ for some j, which gives us a contradiction. Therefore, $L_m(n) = \gamma$. □

References

[1] F. Breuer, A note on a paper by Glaser and Schöffl, *Fibonacci Quart.* **36** (5) (1998), 463-466.

[2] F. Breuer, Ducci Sequences over Abelian groups, *Comm. Algebra* **27** (12) (1999), 5999-6013.

[3] R. Brown and J. Merzel, The length of Ducci's four number game, *Rocky Mountain J. Math.* **37** (1) (2007), 45-65.

[4] M. Burmester, R. Forcade, and E. Jacobs, Circles of numbers, *Glasg. Math. J.* **19** (1978), 115-119.

[5] M. Chamberland, Unbounded Ducci Sequences, *J. Difference Equ. Appl.* **9** (10) (2003), 887-895.

[6] B. Dular, Cycles of sums of integers, *Fibonacci Quart.* **58** (2) (2020), 126-139.

[7] A. Ehrlich, Periods in Ducci's n-number game of differences, *Fibonacci Quart.* **28** (4) (1990), 302-305.

[8] N.J. Fine, Binomial coefficients modulo a prime, *Amer. Math. Monthly* **54** (10.1) (1947), 589-592.

[9] H. Glaser and G. Schöffl, Ducci Sequences and Pascal's Triangle, *Fibonacci Quart.* **33** (4) (1995), 313-324.

[10] M.L. Lewis and S.M. Tefft, The period of Ducci cycles on $\mathbb{Z}_{2^l}$ for tuples of length 2^k, *Adv. Group Theory Appl.*, to appear.

[11] M.L. Lewis and S.M. Tefft, Ducci on $\mathbb{Z}_m^n$ and the maximum length for n odd, *Int. J. Group Theory*, to appear.

[12] A. Ludington Furno, Cycles of differences of integers, *J. Number Theory* **13** (2) (1981), 255-261.

[13] The MathWorks Inc., MATLAB version 9.14.0 (R2023a), The MathWorks Inc., Natick, Massachuesetts. https://www.mathworks.com.

[14] M. Misiurewicz and A. Schinzel, On n numbers in a circle, *Hardy-Ramanujan J.* **11** (1988), 30-39.

[15] M. Spivey, *The Art of Proving Binomial Identities*, Taylor and Francis Group, Boca Raton, FL, 2019.

[16] Tefft, S.M., *Ducci Sequences on Z_m^n*, Ph.D. thesis, Kent State University, OhioLink, 2025.

[17] F.B. Wong, Ducci processes, *Fibonacci Quart.* **20** (2) (1982), 97-105.