

Advances in Group Theory and Applications
© 2026 AGTA - www.advgrouptheory.com/journal
23 (2026), pp. 85–116 ISSN: 2499-1287
DOI: 10.32037/agta-2026-006

The Period of Ducci Cycles on $\mathbb{Z}_{2^l}$ for Tuples of Length 2^k

Mark L. Lewis — Shannon M. Tefft

(*Received Aug. 20, 2024; Accepted Nov. 23, 2024 — Communicated by M.R. Dixon*)

Abstract

Let the Ducci function $D : \mathbb{Z}_m^n \to \mathbb{Z}_m^n$ be defined as

$$D(x_1, x_2, \ldots, x_n) = (x_1 + x_2 \mod m, x_2 + x_3 \mod m, \ldots, x_n + x_1 \mod m)$$

and let the Ducci sequence of u be the sequence $\{D^\alpha(u)\}_{\alpha=0}^\infty$. In this paper, we will provide another proof that for $n = 2^k$ and $m = 2^l$, all Ducci sequences will end in $(0, 0, \ldots, 0)$ and additionally prove that this will happen in at most $2^{k-1}(l+1)$ iterations of D.

Mathematics Subject Classification (2020): 20D60, 11B83, 11B50

Keywords: Ducci sequence; modular arithmetic; length, period; n-number game

1 Introduction

Consider a function $D : \mathbb{Z}_m^n \to \mathbb{Z}_m^n$, which we define as

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

Like [2, 10, 13], we call D the *Ducci function* and for a given tuple $u \in \mathbb{Z}_m^n$, we say that the *Ducci sequence of* u is the sequence $\{D^\alpha(u)\}_{\alpha=0}^\infty$.

Looking at an example, consider $(3,1,3) \in \mathbb{Z}_4^3$ and the first few terms in its Ducci sequence:

$$(3,1,3),\ (0,0,2),\ (0,2,2),\ (2,0,2),\ (2,2,0),\ (0,2,2).$$

One can see that if you continue the Ducci sequence, it cycles through the tuples

$$(0,2,2),\ (2,0,2),\ (2,2,0).$$

We say that these three tuples are the Ducci cycle of the Ducci sequence of $(3,1,3)$. More specifically, we say that the *Ducci cycle* of a tuple u is the set

$$\left\{v \mid \exists \alpha \in \mathbb{Z}^+ \cup \{0\}, \beta \in \mathbb{Z}^+ \ni v = D^{\alpha+\beta}(u) = D^{\alpha}(u)\right\},$$

a term [2, 7, 14] also uses. We define $\mathrm{Len}(u)$ to be the smallest α that can be found to satisfy the equation

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

from our definition for some $\beta \in \mathbb{Z}^+, v \in \mathbb{Z}_m^n$. We adopt the notations $\mathrm{Len}(u)$ and $\mathrm{Per}(u)$ from [2, Definition 1]. The notation $\mathrm{Per}(u)$ is also referred to as the *period* in the literature (see, for example, [3, 6, 10]).

Notice that $\mathrm{Per}(u)$ is also the number of distinct tuples in the Ducci cycle of u. If a tuple $v \in \mathbb{Z}_m^n$ is in the Ducci cycle of the Ducci sequence for some tuple u, we may simply say that v is in a Ducci cycle. Since $\mathbb{Z}_m^n$ is finite, every Ducci sequence enters a cycle.

Define

$$K(\mathbb{Z}_m^n) = \left\{u \in \mathbb{Z}_m^n \mid u \text{ is in some Ducci cycle}\right\},$$

which is given in [2, Definition 4]. The following theorem about $K(\mathbb{Z}_m^n)$ is stated in [2, p.6001] but we will provide a proof of it in Section 3.

Theorem 1.1 *The set $K(\mathbb{Z}_m^n)$ is a subgroup of $\mathbb{Z}_m^n$.*

If for a tuple u there exists a tuple v such that $D(v) = u$, we say that v is a *predecessor* of u. We believe [14, p.259] is the first time this term is used, then later by [2, 13].

It is not always the case that the Ducci sequence ends in a cycle containing more than one tuple. Notice that the Ducci cycle of $(0, 0, \ldots, 0)$ consists only of itself and that satisfies $\mathrm{Per}(u) = 1$. In addition to this, let us observe that $(0, 0, \ldots, 0)$ is the only tuple that satisfies the condition $D(u) = u$, which we believe is first noted in [6, Remark 5] and then again by [2]. This means that only $(0, 0, \ldots, 0)$ and tuples whose Ducci cycle are

$$\{(0, 0, \ldots, 0)\}$$

have a period of 1. We say that a Ducci sequence *vanishes* when its cycle is $\{(0, 0, \ldots, 0)\}$, a term first used by [6, p.117] and also by [2, 13].

A key Ducci sequence is the one corresponding to

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

We call the Ducci sequence of this tuple the *basic Ducci sequence* of $\mathbb{Z}_m^n$, following its first use in [10, p.302], and also in [2, 9, 13]. Following, in particular, [2, Definition 5] and [10, 13], we denote

$$L_m(n) = \mathrm{Len}(0, 0, \ldots, 0, 1) \quad \text{and} \quad P_m(n) = \mathrm{Per}(0, 0, \ldots, 0, 1).$$

These results are significant since, by [2, Lemma 1], for every $u \in \mathbb{Z}_m^n$, we have

$$L_m(n) \geqslant \mathrm{Len}(u) \qquad \text{and} \qquad \mathrm{Per}(u) | P_m(n).$$

The notation $P_m(n)$ for the maximal period of a Ducci sequence on $\mathbb{Z}_m^n$ is also used in [3, p.858].

In this paper, we focus on the case where $m = 2^l$ and $n = 2^k$ for integers $k, l \geqslant 1$. It is first proven [20, p.103, (I)] that all Duc-

ci sequences in $\mathbb{Z}_{2^l}^{2^k}$ vanish. Moreover, [9, Theorem 2.3] also provides a proof of this. However, we would like to establish a value for $L_m(n)$ in this case. Our main goal is to prove the following result.

Theorem 1.2 *Let $n = 2^k$, $m = 2^l$ for integers $l, k \geqslant 1$. Then*

$$P_m(n) = 1 \qquad \textit{and} \qquad L_m(n) = (l+1)2^{k-1}.$$

As part of the proof in [20], it is shown that

$$D^{l*2^k}(u) = (0, 0, \ldots, 0),$$

for every tuple $u \in \mathbb{Z}_{2^l}^{2^k}$; however, neither [20] nor [9] determine a value for $L_{2^l}(2^k)$.

It is worth noting that as a result of all Ducci sequences vanishing, we gain the following result.

Corollary 1.3 *The group $K(\mathbb{Z}_{2^l}^{2^k})$ is trivial.*

The research presented in this paper was conducted while the second author was a Ph.D. student at Kent State University under the supervision of the first author and will appear as part of the second author's dissertation.

2 Background

There are many different versions of the Ducci function. The first and most common Ducci function is

$$\overline{D} : (\mathbb{Z}^+ \cup \{0\})^n \to (\mathbb{Z}^+ \cup \{0\})^n$$

being defined as

$$\overline{D}(x_1, x_2, \ldots, x_n) = (|x_1 - x_2|, |x_2 - x_3|, \ldots, |x_n - x_1|),$$

with [10, 12, 13, 14] being a few examples, or similarly defined on $\mathbb{Z}^n$ like in [2].

Other sources, such as [5, 7, 18], define it on $\mathbb{R}^n$. Note that if $u \in \mathbb{Z}^n$, then $\overline{D}(u) \in (\mathbb{Z}^+ \cup \{0\})^n$. Therefore, for simplicity, we will refer to the Ducci case on $(\mathbb{Z}^+ \cup \{0\})^n$ or $\mathbb{Z}^n$ as the Ducci case on $\mathbb{Z}^n$.

For both Ducci on $\mathbb{Z}^n$ and Ducci on $\mathbb{R}^n$, it has been proven that all Ducci sequences enter a cycle. Some examples of sources that explain why this happens on $\mathbb{Z}^n$ are [6, 10, 13, 14] and [18] proves it for $\mathbb{R}^n$ in Theorem 2. For Ducci on $\mathbb{Z}^n$, when looking at the tuples in a Ducci cycle, all of the entries belong to $\{0, c\}$, for some $c \in \mathbb{Z}^+$, which is proved in [14, Lemma 3] and then again later by [16]. Because $\overline{D}(\lambda u) = \lambda \overline{D}(u)$ when $\lambda \in \mathbb{Z}$ and $u \in \mathbb{Z}^n$, this means that for this case, one only needs to worry about when Ducci is defined on $\mathbb{Z}_2$ when examining Ducci cycles and periods, something that [2, 10, 13, 14] all talk about. For the $\mathbb{R}^n$ case, [18] proves a similar result in Theorem 1: if the Ducci sequence reaches a limit point, then all of the entries in the tuple belong to $\{0, c\}$, for some $c \in \mathbb{R}$.

It has been proven that the Ducci sequence will eventually vanish for all tuples in $\mathbb{Z}^n$ if and only if if n is a power of 2. According to [4, 7], the paper [8] is the first to provide a proof of this with other papers, like [13, 14], also citing [8] for a proof of this fact. The first paper published that talks about Ducci sequences is also [8]. Unfortunately, we are unable to find a copy of [8]; a review of the paper can be found at [17]. Many different proofs for the fact that all Ducci sequences vanish have been made since [8], with [10, 12, 15, 16] being a few. As discussed in the introduction, this conclusion can be extended to $m = 2^l$ where $l \geqslant 1$. Our ultimate goal is to establish how long we can expect it to take for a sequence to reach $(0, 0, \ldots, 0)$.

For the Ducci case on $\mathbb{Z}_2^n$, there have been a few sources that look at the maximum value of the length of a Ducci sequence, $L_2(n)$, for a variety of values for n. The first source is [10, p.303], which shows that for odd n, $L_2(n) = 1$. The next

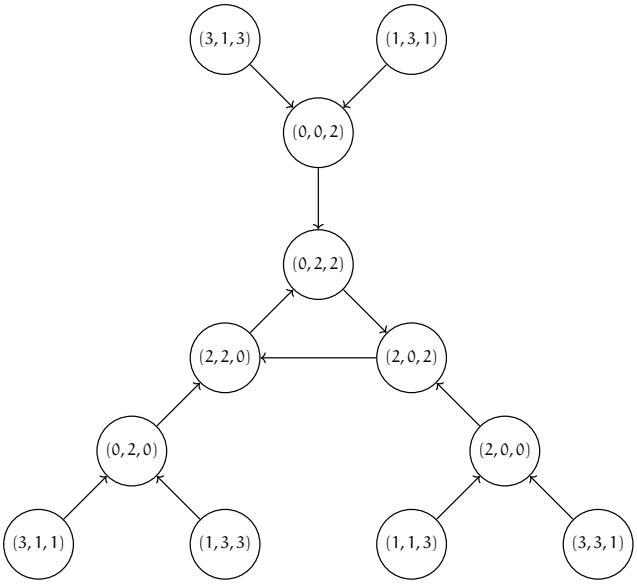


Figure 1: Transition graph for $\mathbb{Z}_4^3$

example is the specific case where

$$n = 2^{k_1} + 2^{k_2},$$

for $k_1 > k_2 \geqslant 0$, considered in [13, Theorem 6], where it is shown that $L_2(n) = 2^{k_2}$. As proved in [1, Theorem 4] the result extends to all even n, showing that if $n = 2^k n_1$ where n_1 is odd, then $L_2(n) = 2^k$. This supports the case where $l = 1$ for Theorem 1.2.

Returning to our Ducci case, [20] is the first paper to look at Ducci sequences on $\mathbb{Z}_m^n$, followed by [2, 3, 9].

We start by discussing more about our example of the Ducci cycle of $(3,1,3)$ to provide a better visualization of what Ducci sequences in $\mathbb{Z}_m^n$ look like. We can do this by creating a transition graph that maps all of the Ducci sequences of $\mathbb{Z}_4^3$ and direct our focus to the connected component containing $(3,1,3)$, which can be found in Figure 2.

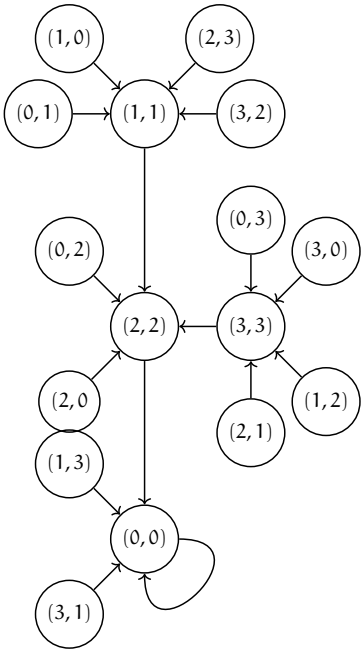


Figure 2: Transition graph for $\mathbb{Z}_4^2$

Using our earlier definitions, one can see

$$\text{Len}(3,1,3) = 2,\ \text{Len}(0,0,2) = 1, \quad \text{and} \quad \text{Len}(0,2,2) = 0.$$

Although $(1,3,1)$ is not in the Ducci sequence of $(3,1,3)$, we can see that the Ducci sequences of $(3,1,3)$ and $(1,3,1)$ have the same Ducci cycle, as well as every other tuple, in this connected component. In addition to this, all of these tuples have period 3.

Notice that $(0,0,2)$ has two predecessors, $(3,1,3)$ and $(1,3,1)$. But not all tuples have predecessors; both $(3,1,3)$ and $(1,3,1)$ are examples of this.

We also present the transition graph for $\mathbb{Z}_4^2$ to give an example where all Ducci sequences vanish in Figure 2. For this graph, all tuples in $\mathbb{Z}_4^2$ are part of the same component. Here, we can see that $L_2(4) = 3$, but not all tuples without predecessors have this length. For example, $(2,3)$ and $(1,3)$ both do not have

predecessors, but

$$\mathrm{Len}(2,3) = 3 \qquad \text{and} \qquad \mathrm{Len}(1,3) = 1.$$

Notice that all tuples in $\mathbb{Z}_4^2$ that have a predecessor have exactly four predecessors. This is not a coincidence, in fact, the following result holds.

Theorem 2.1 *Let n be even. If a tuple $u = (x_1, x_2, \ldots, x_n) \in \mathbb{Z}_m^n$ has a predecessor $(y_1, y_2, \ldots, y_n)$, then*

$$(y_1 + z, y_2 - z, \ldots, y_{n-1} + z, y_n - z)$$

is also a predecessor of u where $z \in \mathbb{Z}_m$. Moreover, if a tuple u has a predecessor, it has exactly m predecessors.

Proof — Let $x_i, y_i \in \mathbb{Z}_m$. Clearly, if $(y_1, y_2, \ldots, y_n)$ is a predecessor to $(x_1, x_2, \ldots, x_n)$, then so is $(y_1 + z, y_2 - z, \ldots, y_n - z)$ if $z \in \mathbb{Z}_m$. This gives us at least m predecessors to $(x_1, x_2, \ldots, x_n)$, each beginning with a different element in $\mathbb{Z}_m$.

We now confirm that these are all the predecessors of the tuple $(x_1, x_2, \ldots, x_n)$. If we consider two tuples that are predecessors to $(x_1, x_2, \ldots, x_n)$ that both begin with the same element, say $(y_1, y_2, \ldots, y_n)$ and $(y_1, y_2', \ldots, y_n')$, then we have the relations

$$y_1 + y_2 \equiv x_1 \mod m \qquad \text{and} \qquad y_1 + y_2' \equiv x_1 \mod m,$$

which gives us $y_2 = y_2'$. We can repeat this to see $y_i = y_i'$, for every $i, 1 \leqslant i \leqslant n$ and, as a result, $(x_1, x_2, \ldots, x_n)$ only has one unique predecessor beginning with y_1, so it has exactly m predecessors. □

Let us now draw our attention back to D specifically. Because

$$\begin{aligned} &D((x_1, x_2, \ldots, x_n) + (x_1', x_2', \ldots, x_n')) \\ &= D(x_1 + x_1', x_2 + x_2', \ldots, x_n + x_n') \end{aligned}$$

$$= (x_1 + x_2 + x_1' + x_2', x_2 + x_3 + x_2' + x_3', \ldots, x_n + x_1 + x_n' + x_1')$$
$$= (x_1 + x_2, x_2 + x_3, \ldots, x_n + x_1) + (x_1' + x_2', x_2' + x_3', \ldots, x_n' + x_1')$$
$$= D(x_1, x_2, \ldots, x_n) + D(x_1', x_2', \ldots, x_n'),$$

it is true that $D \in \mathrm{End}(\mathbb{Z}_m^n)$. Also, it remains true that

$$D(\lambda u) = \lambda D(u)$$

when $\lambda \in \mathbb{Z}_m$ and $u \in \mathbb{Z}_m^n$. Since this means $D^\alpha(\lambda u) = \lambda D^\alpha(u)$ for $\alpha \in \mathbb{Z}^+$, the Ducci sequence for λu is $\left\{\lambda D^\alpha(u)\right\}_{\alpha=0}^{\infty}$ and if $u \in K(\mathbb{Z}_m^n)$, then so is λu.

Define $H : \mathbb{Z}_m^n \to \mathbb{Z}_m^n$ as

$$H(x_1, x_2, \ldots, x_n) = (x_2, x_3, \ldots, x_n, x_1).$$

We also have that $H \in \mathrm{End}(\mathbb{Z}_m^n)$ and $D = I + H$ where I is the identity endomorphism. This function was first introduced in [10, p.302] and is also used by [2, 13]. Note that

$$H(D(x_1, x_2, .., x_n)) = H(x_1 + x_2, x_2 + x_3, \ldots, x_n + x_1)$$
$$= (x_2 + x_3, x_3 + x_4, \ldots, x_n + x_1, x_2 + x_1)$$
$$= D(x_2, x_3, .., x_n, x_1) = D(H(x_1, x_2, \ldots, x_n)),$$

and therefore H, D commute. This means that if $\{D^\alpha(u)\}_{\alpha=0}^{\infty}$ is the Ducci sequence for $u \in \mathbb{Z}_m^n$, then $\{H^\beta(D^\alpha(u))\}_{\alpha=0}^{\infty}$ is the Ducci sequence for $H^\beta(u)$ when $0 \leqslant \beta \leqslant n-1$. Consequently, if $u \in K(\mathbb{Z}_m^n)$, then so is $H^\beta(u)$.

3 Findings on Ducci for n, m arbitrary

We can now prove Theorem 1.1 from Section 1. Note that this theorem is stated as a fact in [2], but a proof is provided here for completeness.

Proof of Theorem 1.1 — We start by showing that

$$\begin{aligned} &D^{\alpha}((x_1, x_2, \ldots, x_n) + (x_1', x_2', \ldots, x_n')) \\ &= D^{\alpha}(x_1, x_2, \ldots, x_n) + D^{\alpha}(x_1', x_2', \ldots, x_n') \end{aligned}$$

by induction for $\alpha \in \mathbb{Z}^+$. This is true for $\alpha = 1$ because D is an endomorphism.

Assume that it is true for $\alpha - 1$, then

$$\begin{aligned} &D^{\alpha}((x_1, x_2, \ldots, x_n) + (x_1', x_2', \ldots, x_n')) \\ &= D(D^{\alpha-1}((x_1, x_2, \ldots, x_n) + (x_1', x_2', \ldots, x_n')). \end{aligned}$$

By induction, we have

$$D(D^{\alpha-1}(x_1, x_2, \ldots, x_n) + D^{\alpha-1}(x_1', x_2', \ldots, x_n'))$$

and

$$D(D^{\alpha-1}(x_1, x_2, \ldots, x_n)) + D(D^{\alpha-1}(x_1', x_2', \ldots, x_n')),$$

which is equal to

$$D^{\alpha}(x_1, x_2, \ldots, x_n) + D^{\alpha}(x_1', x_2', \ldots, x_n').$$

Now suppose $(x_1, x_2, \ldots, x_n), (x_1', x_2', \ldots, x_n') \in K(\mathbb{Z}_m^n)$. Consequently, if $d = P_m(n)$, then $D^d(x_1, x_2, \ldots, x_n) = (x_1, x_2, \ldots, x_n)$ and $D^d(x_1', x_2', \ldots, x_n') = (x_1', x_2', \ldots, x_n')$. Therefore,

$$\begin{aligned} &D^{d}((x_1, x_2, \ldots, x_n) + (x_1', x_2', \ldots, x_n')) \\ &= D^{d}(x_1, x_2, \ldots, x_n) + D^{d}(x_1', x_2', \ldots, x_n'), \end{aligned}$$

which equals $(x_1, x_2, \ldots, x_n) + (x_1', x_2', \ldots, x_n')$ and thus

$$((x_1, x_2, \ldots, x_n) + (x_1', x_2', \ldots, x_n')) \in K(\mathbb{Z}_m^n).$$

It follows then that $K(\mathbb{Z}_m^n) \leqslant \mathbb{Z}_m^n$. □

When examining a Ducci sequence, it is useful to determine the value of $D^r(u)$ for a given $u \in \mathbb{Z}_m^n$. To this end, define $a_{r,s}$, with $r, s \in \mathbb{Z}$, $r \geqslant 0$, and $1 \leqslant s \leqslant n$, so that

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

Now, any tuple $(x_1, x_2, \ldots, x_n) \in \mathbb{Z}_m^n$ can be written as

$$(x_1, x_2, \ldots, x_n) = \sum_{s=1}^{n} x_s H^{-s}(0,0,..,0,1),$$

which gives

$$D^r(x_1, x_2, \ldots, x_n) = \sum_{s=1}^{n} x_s H^{-s}(a_{r,n}, a_{r,n-1}, \ldots, a_{r,1})$$

or

$$\sum_{s=1}^{n} x_s (a_{r,s}, a_{r,s-1}, \ldots, a_{r,s+1}).$$

Using this, we can now define $a_{r,s}$ as the coefficient on x_{s-i+1} in the ith coordinate of $D^r(x_1, x_2, \ldots, x_n)$, with

$$a_{0,s} = \begin{cases} 0 & \text{if } s \neq 1 \\ 1 & \text{if } s = 1 \end{cases}.$$

We now aim to prove a few more observations about $a_{r,s}$.

Theorem 3.1 *Let $r \geqslant 1$, $1 \leqslant s \leqslant n$. The the following are satisfied*:

(1) $a_{r,s} = a_{r-1,s} + a_{r-1,s-1}$.

(2) *For $r < n$,* $a_{r,s} = \binom{r}{s-1}$.

(3) $a_{r+t,s} = \sum_{i=1}^{n} a_{t,i} a_{r,s-i+1}$, *where $t \geqslant 1$.*

PROOF — (1) We first note that

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

Hence, by the definition of D, the s-th entry of $D^r(0,0,\ldots,0,1)$ will be

$$a_{r-1,s} + a_{r-1,s-1}.$$

This, by definition, is also $a_{r,s}$ and (1) follows.

We proceed to prove statement (2) by induction on r, and statement (3) by induction on t.

(2) *Basis Step*: $r = 1$. This follows from (1) and

$$a_{0,s} = \begin{cases} 0 & \text{if } s \neq 1 \\ 1 & \text{if } s = 1 \end{cases}.$$

Inductive Step: Note that if $s - 1 > r$, we use the convention that

$$a_{r,s} = \binom{r}{s-1} = 0.$$

Assume $a_{r-1,s} = \binom{r-1}{s-1}$ when $r < n$. By (1), we have that for $1 < s \leqslant n$, $a_{r,s} = a_{r-1,s} + a_{r-1,s-1}$, which by induction is

$$\binom{r-1}{s-1} + \binom{r-1}{s-2} \qquad \text{or} \qquad \binom{r}{s-1}.$$

For $s = 1$, we have $a_{r,1} = a_{r-1,1} + a_{r-1,n}$. By induction, this is

$$\binom{r-1}{0} + \binom{r-1}{n-1}$$

which is 1 or $\binom{r}{0}$ as long as $r < n$.

(3) We prove this via induction on t.

Basis Steps: $t = 1, 2$. Calculating $a_{r,s}$ in terms of $a_{r-1,i}$ we obtain that $a_{r,s} = a_{r-1,s} + a_{r-1,s-1}$, which can be further expanded in terms of $a_{r-2,i}$ as $a_{r,s} = a_{r-2,s} + 2a_{r-2,s-1} + a_{r-2,s-2}$. This is

$$a_{2,1}a_{r-2,s} + a_{2,2}a_{r-2,s-1} + a_{2,3}a_{r-2,s-2}$$

and the basis case follows.

Inductive Step: Assume that for $t' < t$, $a_{r+t',s} = \sum_{i=1}^{n} a_{t',i}a_{r,s-i+1}$. Then calculating $a_{r+t,s}$, we have

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

Breaking down $a_{r,s-i+1}$, this is

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

Distributing $a_{t-1,i}$ and breaking the sum up, this is

$$\sum_{i=1}^{n} a_{t-1,i}a_{r,s-i+1} + \sum_{i=1}^{n} a_{t-1,i}a_{r,s-i}\,. \tag{3.1}$$

Note that, for the sum $\sum_{i=1}^{n} a_{t-1,i}a_{r,s-i}$, from equation (3.1), we have

$$\sum_{i=1}^{n} a_{t-1,i}a_{r,s-i} = \sum_{i=2}^{n+1} a_{t-1,i-1}a_{r,s-i+1}\,.$$

As the s-coordinate of $a_{r,s}$ is reduced modulo n, it follows that

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

Therefore, equation (3.1) is equal to

$$\sum_{i=1}^{n}(a_{t-1,i} + a_{t-1,i-1})a_{r,s-i+1} \qquad \text{or} \qquad \sum_{i=1}^{n} a_{t,i}a_{r,s-i+1}\,.$$

Therefore, equation (3) holds. □

We now prove some other useful facts about the $a_{r,s}$ coefficients that we will need later.

Corollary 3.2 *For all integers n and s with $1 \leqslant s \leqslant n$, the terms $a_{n,s}$ are given by*

$$a_{n,s} = \begin{cases} \binom{n}{s-1} & s \neq 1 \\ 2 & s = 1 \end{cases}$$

Proof — Let $s > 1$. Then $a_{n,s} = a_{n-1,s} + a_{n-1,s-1}$ gives us

$$a_{n,s} = \binom{n-1}{s-1} + \binom{n-1}{s-2} \qquad \text{or} \qquad \binom{n}{s-1},$$

by Theorem 3.1.

For $s = 1$, $a_{n,1} = a_{n-1,1} + a_{n-1,n}$ gives us

$$a_{n,1} = \binom{n-1}{0} + \binom{n-1}{n-1} \qquad \text{or} \qquad 2\,,$$

by Theorem 3.1. □

We have one last lemma about the $a_{r,s}$ that is true for all n, m.

Lemma 3.3 *For $r \geqslant 0$, $a_{r,s} = a_{r,r-s+2}$.*

Proof — We work by induction on r.

Basis Step: We take advantage of Theorem 3.1 to see that when $r < n$,

$$a_{r,s} = \binom{r}{s-1} = \binom{r}{r-s+1} = a_{r,r-s+2}.$$

Inductive Step: Suppose that the theorem is true for $r-1$. Then we have

$$a_{r-1,s} = a_{r-1,r-s+1} \qquad \text{and} \qquad a_{r-1,s-1} = a_{r-1,r-s+2}.$$

Since $a_{r,s} = a_{r-1,s} + a_{r-1,s-1}$,

$$a_{r,s} = a_{r-1,r-s+1} + a_{r-1,r-s+2},$$

which is equal to $a_{r,r-s+2}$. Therefore, the claim follows. □

4 All tuples vanish in $\mathbb{Z}_{2^l}^{2^k}$

Recall that it is our main goal to prove that for $m = 2^l, n = 2^k$, then $L_m(n) = (l+1)2^{k-1}$. In order to do this, we first aim to prove a number of lemmas, starting with a few lemmas that explore the value of certain binomial coefficients. We believe that Lemmas 4.1–4.3, and 4.5 are known but we are including the following proofs for the sake of completeness. Throughout these proofs, we rely on the well known fact that $\binom{2^j}{t}$ is even when $t \neq 0, 2^j$, a proof of which can be found in [11, Theorem 3].

Lemma 4.1 *For any integer* $j \geqslant 2$*, we have*

$$\binom{2^j}{2^{j-1}} \equiv 2 \mod 4.$$

Proof — By the Chu–Vandermonde identity (see [19]), we obtain

$$\binom{2^j}{2^{j-1}} = \sum_{i=0}^{2^{j-1}} \binom{2^{j-1}}{i}^2 = \binom{2^{j-1}}{0}^2 + \binom{2^{j-1}}{2^{j-1}}^2 + \sum_{i=1}^{2^{j-1}-1} \binom{2^{j-1}}{i}^2,$$

which is congruent to 2 mod 4. □

For the other binomial coefficients $\binom{2^j}{t}$, we have the following result.

Lemma 4.2 *When* $t \neq 0, 2^{j-1}, 2^j$ *and* $j \geqslant 2$*, then*

$$\binom{2^j}{t} \equiv 0 \textit{ mod } 4.$$

Proof — First to address the cases when $t \in \{0, 2^{j-1}, 2^j\}$, we know

$$\binom{2^j}{0} = \binom{2^j}{2^j} = 1 \qquad \text{and} \qquad \binom{2^j}{2^{j-1}} \equiv 2 \mod 4.$$

We prove the rest of the lemma by induction on j.

Basis Step: $j = 2$.

$$\binom{4}{1} = \binom{4}{3} = 4.$$

Inductive Step: Assume that

$$\binom{2^{j-1}}{t} \equiv 0 \mod 4$$

when $t \neq 0, 2^{j-2}, 2^{j-1}$. We start with when $0 < t < 2^{j-2}$ and use

the Chu–Vandermonde Identity to see that

$$\begin{aligned}\binom{2^j}{t} &= \sum_{i=0}^{t} \binom{2^{j-1}}{i}\binom{2^{j-1}}{t-i} \\ &= \binom{2^{j-1}}{0}\binom{2^{j-1}}{t} + \binom{2^{j-1}}{t}\binom{2^{j-1}}{0} + \sum_{i=1}^{t-1} \binom{2^{j-1}}{i}\binom{2^{j-1}}{t-i},\end{aligned}$$

which is congruent to 0 mod 4 by induction. Next, we consider $2^{j-2} < t < 2^{j-1}$. Then

$$\begin{aligned}\binom{2^j}{t} &= \binom{2^{j-1}}{0}\binom{2^{j-1}}{t} + \binom{2^{j-1}}{t}\binom{2^{j-1}}{0} + \binom{2^{j-1}}{2^{j-2}}\binom{2^{j-1}}{t-2^{j-2}} \\ &+ \binom{2^{j-1}}{t-2^{j-2}}\binom{2^{j-1}}{2^{j-2}} + \sum_{\substack{i=1 \\ i\neq 2^{j-2}, t-2^{j-2}}}^{t-1} \binom{2^{j-1}}{i}\binom{2^{j-1}}{t-i},\end{aligned}$$

which by induction is congruent to 0 mod 4. Now if we consider $t = 2^{j-2}$, then

$$\begin{aligned}\binom{2^j}{2^{j-2}} &= \binom{2^{j-1}}{0}\binom{2^{j-1}}{2^{j-2}} + \binom{2^{j-1}}{2^{j-2}}\binom{2^{j-1}}{0} \\ &+ \sum_{i=1}^{2^{j-2}-1} \binom{2^{j-1}}{i}\binom{2^{j-1}}{t-i},\end{aligned}$$

which is equivalent to 0 mod 4 by Lemma 4.1 and induction.

Now suppose that $2^{j-1} < t < 2^j$. Then $0 < 2^j - t < 2^{j-1}$, so

$$\binom{2^j}{t} = \binom{2^j}{2^j - t} \equiv 0 \bmod 4$$

and the lemma follows. □

We still need to know more about the value of $\binom{2^j}{2^{j-1}}$ so we prove the following result.

Lemma 4.3 *For* $j \geqslant 2$,

$$\binom{2^j}{2^{j-1}} \equiv 6 \text{ mod } 8.$$

Proof — *Basis Step*: $j = 2$. The claim holds for the base case, since

$$\binom{4}{2} = 6.$$

Inductive Step: Assume $\binom{2^{j-1}}{2^{j-2}} \equiv 6 \mod 8$. Therefore, by the Chu–Vandermonde Identity,

$$\begin{aligned}\binom{2^j}{2^{j-1}} &= \sum_{i=0}^{2^{j-1}} \binom{2^{j-1}}{i}^2 \\ &= \binom{2^{j-1}}{0}^2 + \binom{2^{j-1}}{2^{j-1}}^2 + \binom{2^{j-1}}{2^{j-2}}^2 + \sum_{\substack{i=1 \\ i \neq 2^{j-2}}}^{2^{j-1}-1} \binom{2^{j-1}}{i}^2.\end{aligned}$$

Hence, by induction and Lemma 4.2, we obtain that

$$\binom{2^j}{2^{j-1}} \equiv 6 \mod 8.$$

Therefore, the claim follows. □

The next result is a consequence of Lucas's Theorem, which can be found, for example, in [11, Theorem 1].

Lemma 4.4 *For every integer* t *with* $0 \leqslant t \leqslant 2^j - 1$, *we have*

$$\binom{2^j - 1}{t}$$

is odd.

To be more specific about $\binom{2^j - 1}{2^{j-1}}$, we state the result below.

Lemma 4.5 *For $j \geqslant 2$, we have*

$$\binom{2^j - 1}{2^{j-1}} \equiv 3 \bmod 4.$$

Proof — We prove this via induction.

Basis Step: $j = 2$. The claim holds for the base case, since

$$\binom{3}{2} = 3.$$

Inductive Step: Assume that $\binom{2^{j-1}-1}{2^{j-2}} \equiv 3 \bmod 4$. Hence, by the Chu–Vandermonde Identity,

$$\binom{2^j - 1}{2^{j-1}} = \sum_{i=0}^{2^{j-1}} \binom{2^{j-1}}{i}\binom{2^{j-1}-1}{2^{j-1}-i}$$

or

$$\binom{2^{j-1}}{0}\binom{2^{j-1}-1}{2^{j-1}} + \binom{2^{j-1}}{2^{j-1}}\binom{2^{j-1}-1}{0} + \binom{2^{j-1}}{2^{j-2}}\binom{2^{j-1}-1}{2^{j-2}} + \sum_{\substack{i=1 \\ i \neq 2^{j-2}}}^{2^{j-1}-1} \binom{2^{j-1}}{i}\binom{2^{j-1}-1}{2^{j-1}-i}.$$

This is equivalent to $1 + (2 * 3) \bmod 4 \equiv 3 \bmod 4$. Therefore, the claim follows. □

We now direct our attention back to the $a_{r,s}$ coefficients and examine what happens at certain values of r. We first note that for $n = 2^k$, $a_{r,s+2^{k-1}} = a_{r,s-2^{k-1}}$.

Lemma 4.6 *Let $l \geqslant 1$ and $n = 2^k$. Then, for every $1 \leqslant s \leqslant 2^k$,*

$$a_{l2^{k-1},s} + a_{l2^{k-1},s-2^{k-1}} \equiv 0 \bmod 2^l.$$

Proof — We prove this by induction on l. To simplify the nota-

tion in the following proofs, we introduce functions to represent certain coefficients $a_{r,s}$. To this end, we define

$$f(\gamma, \delta) = a_{\gamma 2^{k-1}, \delta}.$$

It is worth noting that, by Lemma 3.3,

$$f(\gamma, \delta) = f(\gamma, \gamma * 2^{k-1} - \delta + 2).$$

Additionally, when $n = 2^k$, we have

$$f(\gamma, \delta + 2^{k-1}) = f(\gamma, \delta - 2^{k-1}).$$

In terms of f, we want to show

$$f(l, s) + f(l, s - 2^{k-1}) \equiv 0 \mod 2^l.$$

Basis Step: $l = 1$. It suffices to show

$$f(1, s) + f(1, s - 2^{k-1}) \equiv 0 \mod 2.$$

Then, for $s \neq 1, 2^{k-1} + 1$,

$$f(1, s) + f(1, s - 2^{k-1}) = \binom{2^{k-1}}{s-1} + \binom{2^{k-1}}{s - 2^{k-1} - 1} \equiv 0 \mod 2$$

since both of these binomial coefficients are even by Lemma 4.2. For $s = 1, 2^{k-1} + 1$,

$$f(1, 1) + f(1, 1 + 2^{k-1}) = \binom{2^{k-1}}{0} + \binom{2^{k-1}}{2^{k-1}} = 2$$

and the basis case follows.

Inductive Step: Assume

$$f(l - 1, s) + f(l - 1, s - 2^{k-1}) \equiv 0 \mod 2^{l-1}.$$

Then

$$
\begin{aligned}
&f(l,s)+f(l,s-2^{k-1})\\
&=\sum_{i=1}^{2^k}[f(l-1,i)f(1,s-i+1)+f(l-1,i)f(1,s-2^{k-1}-i+1)]
\end{aligned}
$$

by part (3) of Theorem 3.1. We now break this up into the following two sums:

$$
\begin{aligned}
&\sum_{i=1}^{2^{k-1}}[f(l-1,i)f(1,s-i+1)+f(l-1,i)f(1,s-2^{k-1}-i+1)]\\
&+\sum_{i=2^{k-1}+1}^{2^k}[f(l-1,i)f(1,s-i+1)\\
&+f(l-1,i)f(1,s-2^{k-1}-i+1)].
\end{aligned}
$$

Changing the indices of the second sum to match the first, this is

$$
\begin{aligned}
&\sum_{i=1}^{2^{k-1}}[f(l-1,i)f(1,s-i+1)\\
&+f(l-1,i)f(1,s-2^{k-1}-i+1)]\\
&\quad+\sum_{i=1}^{2^{k-1}}[f(l-1,i-2^{k-1})f(1,s-i+2^{k-1}+1)\\
&\quad+f(l-1,i-2^{k-1})f(1,s-i+1)],
\end{aligned}
$$

which can be factored into

$$
\begin{aligned}
&\sum_{i=1}^{2^{k-1}}[f(1,s-i+1)\\
&+f(1,s-i+2^{k-1}+1)][f(l-1,i)+f(l-1,i-2^{k-1})].
\end{aligned}
\tag{4.1}
$$

By induction, since

$$f(l-1,i)+f(l-1,i-2^{k-1}) \equiv 0 \mod 2^{l-1},$$

the addend in the sum from (4.1) is congruent to $0 \mod 2^l$ if both $f(1,s-i+1)$ and $f(1,s-i+2^{k-1}+1)$ are even. The only times this does not happen is when $i=s$ and $i=s+2^{k-1}$. In both cases, the addend in the sum of (4.1) is

$$[f(1,1)+f(1,2^{k-1}+1)][f(l-1,s)+f(l-1,s-2^{k-1})].$$

This is $2[f(l-1,s)+f(l-1,s-2^{k-1})]$, and, by induction, we obtain that $2[f(l-1,s)+f(l-1,s-2^{k-1})] \equiv 0 \mod 2^l$. Therefore, equation (4.1) is congruent to $0 \mod 2^l$ and the lemma follows. □

We have one last lemma to prove before Theorem 1.2. We are once more interested in a sum of two specific $a_{r,s}$ coefficients.

Lemma 4.7 *Let* $n=2^k$. *For* $l \geqslant 3$,

$$a_{(l-1)2^{k-1},l2^{k-2}+1} + a_{(l-1)2^{k-1},l2^{k-2}-2^{k-1}+1} \equiv 0 \mod 2^l.$$

Proof — Let us define

$$g(\gamma,\epsilon,\delta) = a_{\gamma 2^{k-1},\epsilon 2^{k-2}+\delta}.$$

In terms of g, we aim to show that

$$g(l-1,l,1)+g(l-1,l,2^{k-1}+1) \equiv 0 \mod 2^l.$$

Using Theorem 3.1, we obtain that

$$\begin{aligned} &g(l-1,l,1)+g(l-1,l,2^{k-1}+1) \\ &= \sum_{i=1}^{2^k} [f(1,i)g(l-2,l,2-i)+f(1,i)g(l-2,l,2^{k-1}+2-i)]. \end{aligned}$$

As in the proof of Lemma 4.6, we decompose the sum and adjust the indices to obtain

$$\sum_{i=1}^{2^{k-1}} [f(1,i)g(l-2,l,2-i) + f(1,i)g(l-2,l,2^{k-1}+2-i)]$$
$$+ \sum_{i=1}^{2^{k-1}} [f(1,i-2^{k-1})g(l-2,l,2^{k-1}+2-i)$$
$$+ f(1,i-2^{k-1})g(l-2,l,2-i)].$$

Factoring yields

$$\sum_{i=1}^{2^{k-1}} [f(1,i) + f(1,i-2^{k-1})][g(l-2,l,2-i) + g(l-2,l,2^{k-1}+2-i)]. \tag{4.2}$$

Note that by Lemma 4.6,

$$g(l-2,l,2-i) + g(l-2,l,2^{k-1}+2-i) \equiv 0 \mod 2^{l-2}.$$

Consequently, if $f(1,i) + f(1,i-2^{k-1}) \equiv 0 \mod 4$, then each term in the sum in (4.2) is congruent to $0 \mod 2^l$.

Observe that if

$$i \neq 1, 2^{k-2}+1, 2^{k-1}+1, 2^{k-1}+2^{k-2}+1,$$

then both $f(1,i)$ and $f(1,i-2^{k-1})$ are equivalent to $0 \mod 4$ by Lemma 4.2. Thus, reducing modulo 2^l, expression (4.2) becomes

$$\begin{aligned}
&[f(1,1) + f(1,2^{k-1}+1)][g(l-2,l,1) \\
&+ g(l-2,l,2^{k-1}+1)] \\
&+ [f(1,2^{k-1}+1) + f(1,1)][g(l-2,l,2^{k-1}+1) \\
&+ g(l-2,l,1)] + [g(1,1,1) \\
&+ g(1,1,2^{k-1}+1)][g(l-2,l-1,1)
\end{aligned} \tag{4.3}$$

$$+ g(l-2, l-1, 2^{k-1}+1)] + [g(1,1,2^{k-1}+1)$$
$$+ g(1,1,1)][g(l-2, l-1, 2^{k-1}+1) + g(l-2, l-1, 1)].$$

Notice that

$$f(1,1) + f(1, 2^{k-1}+1) = \binom{2^{k-1}}{0} + \binom{2^{k-1}}{2^{k-1}}$$

and

$$g(1,1,1) + g(1,1,2^{k-1}+1 = \binom{2^{k-1}}{2^{k-2}} + \binom{2^{k-1}}{2^{k-1}+2^{k-2}}.$$

Moreover, by Lemma 4.6,

$$g(l-2, l, 1) + g(l-2, l, 2^{k-1}+1) \equiv 0 \mod 2^{l-1}$$

and

$$g(l-2, l-1, 1) + g(l-2, l-1, 2^{k-1}+1) \equiv 0 \mod 2^{l-1}.$$

It follows that expression (4.3) is congruent to $0 \pmod{2^l}$, thereby completing the proof of the lemma. □

We are now equipped with all the tools required to prove the main theorem.

Proof of Theorem 1.2 — We note once again that, according to [20, (I), p.103] and [9, Theorem 2.3]), all tuples vanish in $\mathbb{Z}_{2^l}^{2^k}$, for all $l, k \in \mathbb{Z}^+$. We also provide a proof of this result. Indeed, to show that

$$L_{2^l}(2^k) = (l+1)2^{k-1},$$

we are going to prove that

$$D^{(l+1)2^{k-1}}(0,0,\ldots,0,1) = (0,0,\ldots,0),$$

which in turn implies that $P_{2^l}(2^k) = 1$ and that all tuples in $\mathbb{Z}_{2^l}^{2^k}$ vanish.

We prove this result by induction on l, with two base cases.

However, since several results used in the proof require the assumption $k \geqslant 2$, we first treat the case $k = 1$. That is, we show that $L_{2^l}(2) = l + 1$ and that $P_{2^l}(2) = 1$, for every $l > 0$.

Basis Step: $k = 1$. Notice that $D^{\alpha}(0,1) = (2^{\alpha-1}, 2^{\alpha-1})$. It follows that $D^{l+1}(0,1) = (0,0)$ and hence $P_{2^l}(2) = 1$. Moreover, since

$$D^{l}(0,1) = (2^{l-1}, 2^{l-1}) \not\equiv (0,0) \pmod{2^l},$$

we conclude that $L_{2^l}(2) = l + 1$.

For the rest of the proof, we assume $n = 2^k$, $k \geqslant 1$.

Basis Step: $l = 1$. We first prove $f(2,s) \equiv 0 \mod 2$, for all $1 \leqslant s \leqslant n$. Recall that $f(2,1) = 2$ and, for $1 < s \leqslant 2^k$,

$$f(2,s) = \binom{2^k}{s-1} \equiv 0 \mod 2$$

which gives us $P_2(2^k) = 1$. Note also that, for $r < 2^k$,

$$a_{r,1} = 1 \not\equiv 0 \mod 2.$$

Therefore, this is the first time we have that $a_{r,s} \equiv 0 \mod 2$, for all s, so $L_2(2^k) = 2^k$.

Basis Step: $l = 2$. It suffices to show that $L_4(2^k) = 3 * 2^{k-1}$ and $P_4(2^k) = 1$. We begin by showing that $f(3,s) \equiv 0 \mod 4$, for every s. We first observe that, by Theorem 3.1, we have

$$f(3,s) = \sum_{i=1}^{2^k} f(1,i) f(2, s-i+1).$$

We then separate the terms where $i = 1, 2^{k-1}+1$ to produce

$$\begin{aligned} &f(1,2^{k-1}+1) f(2, s-2^{k-1}) + f(1,1) f(2,s) \\ &+ \sum_{\substack{i=2 \\ i \neq 2^{k-1}+1}}^{2^k} f(1,i) f(2, s-i+1). \end{aligned} \tag{4.4}$$

We do this because $f(1,i) \equiv 0 \mod 2$ for $i \neq 1, 2^{k-1}+1$ and

$$f(2, s-i+1) \equiv 0 \mod 2$$

as shown in our first basis case. Hence, expression (4.4) is equivalent to

$$f(2, s-2^{k-1}) + f(2,s) \pmod 4, \tag{4.5}$$

which, by Lemma 4.6, is congruent to $0 \pmod 4$. Therefore we have that $P_4(2^k) = 1$ and $L_4(2^k) \leqslant 3 * 2^{k-1}$. We now need to show that there exists s such that $a_{3*2^{k-1}-1,s} \not\equiv 0 \mod 4$. To this end, define

$$h(\gamma, \delta) = a_{\gamma 2^{k-1}-1,\delta}.$$

Calculating $h(3,s)$ for general s using Theorem 3.1, we obtain

$$h(3,s) = \sum_{i=1}^{2^k} f(1,i)h(2, s-i+1).$$

We now separate the terms where i is $1, 2^{k-2}+1$ or $2^{k-1}+1$, which gives

$$\begin{aligned} &f(1,1)h(2,s) + f(1,2^{k-1}+1)h(2,s-2^{k-1}) \\ &+ g(1,1,1)h(2,s-2^{k-2}) + \sum_{i\in J} f(1,i)h(2,s-i+1) \end{aligned} \tag{4.6}$$

where

$$J = \left\{2 \leqslant i \leqslant 2^k \mid i \neq 2^{k-1}, 2^{k-2}+1\right\}.$$

We do this so the sum over J is congruent to $0 \mod 4$ by Lemma 4.2. If we also consider $s = 1$, then expression (4.6) is congruent to

$$\begin{aligned} &f(1,1)h(2,1) + f(1,2^{k-1}+1)h(2,2^{k-1}+1) \\ &+ g(1,1,1)h(2,2^k - 2^{k-2}+1) \mod 4, \end{aligned}$$

which is equivalent to $1 + h(2, 2^{k-1} + 1) + 2 \mod 4$ because

$$g(1, 1, 1) \equiv 2 \mod 4$$

and $h(2, 2^k - 2^{k-2} + 1)$ is odd. From Lemma 4.5, this is congruent to $2 \mod 4$ and $h(3, 1) \not\equiv 0 \mod 4$, so $L_4(2^k) = 3 * 2^{k-1}$.

Inductive Step: Assume that

$$L_{2^{l-1}}(2^k) = l2^{k-1} \qquad \text{and} \qquad P_{2^{l-1}}(2^k) = 1.$$

This implies that $f(l, s) \equiv 0 \mod 2^{l-1}$, for every s. Calculating $f(l + 1, s)$ with Theorem 3.1, we have

$$f(l + 1, s) = \sum_{i=1}^{2^k} f(l, i) f(1, s - i + 1).$$

If we separate out the terms where $s - i + 1 = 1, 2^{k-1} + 1$, this becomes

$$\begin{aligned} &f(l, s) f(1, 1) + f(l, s - 2^{k-1}) f(1, 2^{k-1} + 1) \\ &+ \sum_{i \in J} f(l, i) f(1, s - i + 1) \end{aligned} \tag{4.7}$$

where

$$J = \left\{ 1 \leqslant i \leqslant 2^k \mid i \neq s, s - 2^{k-1} \right\}.$$

We do this so the sum over J is equivalent to $0 \mod 2^l$ by induction and because $f(1, s - i + 1)$ is even over J. Therefore, expression (4.7) is equivalent to

$$f(l, s) + f(l, s - 2^{k-1}) \mod 2^l,$$

which, by Lemma 4.6, is congruent to $0 \mod 2^l$. This gives us that

$$P_m(n) = 1 \qquad \text{and} \qquad L_m(n) \leqslant (l + 1) 2^{k-1}.$$

It remains to show that $L_m(n) > (l + 1) 2^{k-1} - 1$, which will

then establish the remainder of the theorem. Observe that, since $P_m(n) = 1$, it suffices to show the existence of s such that

$$h(l+1, s) \not\equiv 0 \mod 2^l.$$

We begin by decomposing $h(l+1, s)$ as follows:

$$h(l+1, s) = \sum_{i=1}^{2^k} f(l, i) h(1, s-i+1). \tag{4.8}$$

Since $a_{r,s} = a_{r,r-s+2}$, by Lemma 3.3, most $a_{r,s}$ coefficients have another coefficient that it is equal to. The case where this does not happen is when $s \equiv r - s + 2 \mod 2^k$. In our case, $h(l, i)$ is not equal to any other coefficient when

$$i = l2^{k-1} - i + 2 \qquad \text{and} \qquad i = l2^{k-1} - i + 2^k + 2.$$

Solving for i, this is when

$$i = l2^{k-2} + 1 \qquad \text{and} \qquad i = l2^{k-2} + 2^{k-1} + 1.$$

We separate these out from our sum so, using equation (4.8), we can view $h(l+1, s)$ as

$$\begin{aligned} &g(l, l, 1) h(1, s - l2^{k-2}) + g(l, l, 2^{k-1} + 1) h(1, s - l2^{k-2} - 2^{k-1}) \\ &+ \sum_{i \in M} [f(l, i) h(1, s - i + 1) + g(l, 2l, 2 - i) h(1, s - l2^{k-1} + i - 1) \end{aligned}$$

where M is defined to preserve equality. We now consider the case $s = l2^{k-2} + 1$, so $h(l+1, l2^{k-2} + 1)$ is

$$\begin{aligned} &g(l, l, 1) h(1, 1) + g(l, l, 2^{k-1} + 1) h(1, 2^{k-1} + 1) \\ &+ \sum_{i \in M} [f(l, i) h(1, l2^{k-2} + 2 - i) \\ &+ g(l, l, 2 - i) h(1, l2^{k-2} - l2^{k-1} + i)]. \end{aligned} \tag{4.9}$$

Examining each term of (4.9), we note that

$$g(l, l, 2^{k-1} + 1)\, h(1, 2^{k-1} + 1) = 0,$$

since $h(1, 2^{k-1} + 1) = 0$. For the sum in (4.9), this becomes

$$\sum_{i \in M} f(l, i)\left[h(1, l2^{k-2} + 2 - i) + h(1, l2^{k-2} - l2^{k-1} + i)\right],$$

because $f(l, i) = g(l, l, 2 - i)$. Since $h(1, s)$ is odd, for all s, by Lemma 4.4, we obtain that

$$h(1, l2^{k-2} - i + 2) + h(1, l2^{k-2} - l2^{k-1} + i)$$

is even. We know $f(l, i) \equiv 0 \mod 2^{l-1}$, therefore the whole sum is congruent to $0 \mod 2^l$. Hence, reducing expression (4.9) modulo 2^l, we conclude that

$$g(l + 1, l, 1) \equiv g(l, l, 1) \mod 2^l.$$

Thus, if we can show that $g(l, l, 1) \not\equiv 0 \mod 2^l$, then the statement will follow. Since we already know that

$$g(l, l, 1) \equiv 0 \mod 2^{l-1},$$

we are left to prove the following claim:

$$g(l, l, 1) \equiv 2^{l-1} \mod 2^l,$$

for $l \geqslant 2$. Let us prove this claim by induction on l.

Basis Step: $l = 2$. By Lemma 4.1, we have

$$g(2, 2, 1) \equiv 2 \mod 4,$$

hence the basis case follows.

Inductive Step: Assume that $g(l - 1, l - 1, 1) \equiv 2^{l-2} \mod 2^{l-1}$, then

$$g(l,l,1) = \sum_{i=1}^{2^k} f(l-1,i)g(1,l,2-i).$$

Let

$$J^* = \left\{1 \leqslant i \leqslant 2^k \mid i \neq (l-1)2^{k-2}+1, l2^{k-2}+1, l2^{k-2}-2^{k-1}+1\right\}$$

and separate all terms not in J^* to see this is

$$\begin{aligned} &g(l-1,l-1,1)g(1,1,1) + g(l-1,l,1)f(1,1) \\ &+ g(l-1,l,2^{k-1}+1)g(1,2,1) \\ &+ \sum_{i\in J^*} f(l-1,i)g(1,l,2-i) \end{aligned} \tag{4.10}$$

Once more, we separate this sum over J^* because it is congruent to $0 \mod 2^l$ because

$$f(l-1,i) \equiv 0 \mod 2^{l-2} \quad \text{and} \quad g(1,l,2-i) \equiv 0 \mod 4,$$

by Lemma 4.2. Looking at the remaining pieces from expression (4.10),

$$g(l-1,l-1,1)g(1,1,1) \equiv 2^{l-1} \mod 2^l$$

by induction and Lemma 4.1. Next, we have

$$\begin{aligned} &g(l-1,l,1)f(1,1) + g(l-1,l,2^{k-1}+1)g(1,2,1) \\ &= g(l-1,l,1) + g(l-1,l,2^{k-1}+1) \end{aligned}$$

which, by Lemma 4.7, is congruent to $0 \mod 2^l$. Thus, the claim follows.

Hence, $g(l+1,l,1) \equiv 2^{l-1} \mod 2^l$ and $L_m(n) > (l+1)2^{k-1}-1$. Therefore,

$$L_m(n) = (l+1)2^{k-1},$$

which concludes the proof. □

REFERENCES

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

[2] F. Breuer: "Ducci sequences over abelian groups", *Comm. Algebra* 27 (1999), 5999–6013.

[3] F. Breuer: "Ducci sequences and cyclotomic fields", *J. Difference Equ. Appl.* 16 (2010), 847–862.

[4] R. Brown – J.L. Merzel: "Limiting behavior in Ducci sequences", *Period. Math. Hungar.* 47 (2003), 45–50.

[5] R. Brown – J.L. Merzel: "The length of Ducci's four-number game", *Rocky Mountain J. Math.* 37 (2007), 45–65.

[6] M. Burmester – R. Forcade – E. Jacobs: "Circles of numbers", *Glasgow Math. J.* 19 (1978), 115–119.

[7] M. Chamberland: "Unbounded Ducci sequences", *J. Difference Equ. Appl.* 9 (2003), 887–895.

[8] C. Ciamberlini – A. Marengoni: "Su una interessante curiosità numerica", *Periodico Mat.* 17 (1937), 25–30.

[9] B. Dular: "Cycles of sums of integers", *Fibonacci Quart.* 58 (2020), 126–139.

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

[11] N.J. Fine: "Binomial coefficients modulo a prime", *Amer. Math. Monthly* 54 (1947), 589–592.

[12] B. Freedman: "The four number game", *Scr. Math.* 14 (1948), 35–47.

[13] H. Glaser – G. Schöffl: "Ducci-sequences and Pascal's triangle", *Fibonacci Quart.* 33 (1995), 313–324.

[14] A.L. Furno: "Cycles of differences of integers", *J. Number Theory* 13 (1981), 255–261.

[15] R. Miller: "Mathematical notes: a game with n numbers", *Amer. Math. Monthly* 85 (1978), 183–185.

[16] F. Pompili: "Evolution of finite sequences of integers...", *Math. Gaz.* 80 (1996), 322–332.

[17] H. Rothe-Ille: ZbMath Review on the paper "Su una interessante curiosità numerica" by C. Ciamberlini and A. Marengoni.

[18] M. Misiurewicz – A. Schinzel: "On n numbers on a circle", *Hardy–Ramanujan J.* 11 (1988), 30–39.

[19] M.Z. Spivey: "The Art of Proving Binomial Identities", *Chapman*, New York (2019).

[20] F.B. Wong: "Ducci processes", *Fibonacci Quart.* 20 (1982), 97–105.

Mark L. Lewis
Department of Mathematical Sciences
Kent State University
1300 Lefton Esplanade
Kent, OH 44242 (USA)
e-mail: lewis@math.kent.edu

Shannon M. Tefft (*corresponding author*)
Department of Mathematical Sciences
Kent State University
1300 Lefton Esplanade
Kent, OH 44242 (USA)

Department of Mathematics
Rose-Hulman Institute of Technology
Terre Haute, IN 47803

e-mail: stefft@kent.edu