DUCCI-PROCESSES OF 4-TUPLES

Gerd Schöffl*
Sieboldstr. 5, 97072 Würzburg, Germany
(Submitted February 1996–Final Revision August 1996)

INTRODUCTION

The aim of this note is to investigate some properties of special sequences of 4-tuples. These sequences were first examined by Wong [7] and are called *Ducci-processes*. Wong defines them as follows ([7], pp. 97, 102):

> The successive iterations of a function f are called a Ducci-process if f satisfies the following conditions:
> 1. There exists a function $g(x, y)$ whose domain is the set of pairs of nonnegative integers and whose range is the set of nonnegative integers.
> 2. $f(x_1, x_2, \ldots, x_n) = (g(x_1, x_2), g(x_2, x_3), \ldots, g(x_{n-1}, x_n), g(x_n, x_1))$.
> 3. The n entries of $f^k(x_1, x_2, \ldots, x_n)$ are bounded for all k. The bound depends on the initial choice of $x_1, x_2, \ldots, x_n$.

For $g(x, y) = |x - y|$ we obtain so-called *Ducci-sequences* of n-tuples and so Ducci-processes are generalized Ducci-sequences. Since Ducci-sequences were introduced in the 30s (see Ciamberlini & Marengoni [1]), they have been extensively examined (for references, see Meyers [6] or Ehrlich [2]). Most studies dealt with the following questions:

- Does every sequence of n-tuples lead to $(0, \ldots, 0)$?
- How many steps in the sequence of a given n-tuple are necessary to reach $(0, \ldots, 0)$ or a cycle of n-tuples?
- What can be said about the length of the cycles?

It seems that there have been no further studies about Ducci-processes. Only Engel [3] uses them for a computer exercise for school children. He asks them to find properties of cycles of the Ducci-processes of 4-tuples for $g(x, y) = (x + y) \bmod m$.

We want to answer the above questions for this Ducci-process of 4-tuples.

STABILITY

Before giving an answer to the first question, we need some definitions. Many techniques that are applied for studying Ducci-sequences transfer in a quite obvious way to our problem. So we will use similar notation to [2] as far as possible. We denote our 4-tuples by (a, b, c, d).

Definition 1: Let $\mathcal{D}_m$ be the operator on 4-tuples over $\mathbb{Z}$, which is defined as follows:

$$\mathcal{D}_m(a, b, c, d) = ((a + b) \bmod m, (b + c) \bmod m, (c + d) \bmod m, (d + a) \bmod m).$$

It is clear from the definition of $\mathcal{D}_m$ that we can choose the entries of the 4-tuples under investigation from $\mathbb{Z}_m$. As we are always—if not otherwise stated—computing over $\mathbb{Z}_m$ for some m, we will omit "mod m."

---

* The author is working on his doctoral thesis at the Universität Würzburg and is supported by the Konrad-Adenauer-Stiftung e. V.

Since the number of 4-tuples in $\mathbb{Z}_m$ is bounded, we reach a cycle of 4-tuples after a finite number of applications of $\mathcal{D}_m$.

Definition 2: Let A be a given 4-tuple. Then the smallest natural number k satisfying $\mathcal{D}_m^{k+\ell}A = \mathcal{D}_m^k A$ for some $\ell \in \mathbb{N}$ is called the *life span of A* and will be denoted as $\mathcal{L}_m(A)$.

Thus, $\mathcal{L}_m(A)$ is the number of applications of $\mathcal{D}_m$ needed to reach the cycle produced by A.

Definition 3: For a given 4-tuple A, we call the smallest natural number $\ell > 0$ satisfying $\mathcal{D}_m^{k+\ell}A = \mathcal{D}_m^k A$ for every $k \geq \mathcal{L}_m(A)$ the length of the cycle generated by A.

Considering the cycles that are produced by all possible 4-tuples with entries in $\mathbb{Z}_m$, we find at least one cycle of maximum length. We use $\ell(m)$ for this maximum length.

Definition 4: A Ducci-process is called *stable* if the cycle generated by every 4-tuple contains only one 4-tuple, i.e., $\ell(m) = 1$ (see [7]).

Obviously, the first question breaks down into two parts now:

1. For which m is the Ducci-process produced by $\mathcal{D}_m$ stable?
2. Which 4-tuples can be in a cycle of length 1?

The first part has been answered by Wong ([7], 3.(1)).

Theorem 1: The Ducci-process produced by $\mathcal{D}_m$ is stable if and only if $m = 2^r$ for some $r \in \mathbb{N}$.

As with Ducci-sequences, only one 4-tuple can be contained in a *trivial* cycle, i.e., a cycle of length 1.

Lemma 1: The 4-tuple $(0, 0, 0, 0)$ is the only 4-tuple contained in a trivial cycle and so a 4-tuple A leads to a trivial cycle if and only if $\mathcal{D}_m^k A = (0, 0, 0, 0)$ for some k.

Proof: Let $A = (a, b, c, d)$ such that $\mathcal{D}_m A = A$. Then

$$\mathcal{D}_m A = (a+b, b+c, c+d, d+a) = (a, b, c, d) = A.$$

Comparing the first entries, we deduce that $b = 0$. The other entries show that $c = 0$, $d = 0$, and $a = 0$. □

Thus, every 4-tuple in a Ducci-process produced by $\mathcal{D}_m$ leads to $(0, 0, 0, 0)$ if and only if $m = 2^r$.

Theorem 1 also shows that $\ell(m) = 1$ if and only if $m = 2^r$. Consequently, for every m that is not a power of 2 there are *nontrivial* cycles, i.e., cycles of length greater than 1.

CYCLES OF 4-TUPLES

In order to determine a special 4-tuple that produces a nontrivial cycle for every $m \neq 2^r$, we introduce a very helpful symbol.

Definition 5: Let $A = (a, b, c, d)$. Set $S(A) = a + b + c + d \pmod{m}$ and call $S(A)$ the *sum of A*.

We set $A_0 = (1, 0, 0, 0)$ (as with Ducci-sequences, the cyclic permutations of a given n-tuple all behave alike so they are not considered separately) and $A_k = \mathcal{D}_m^k A_0$.

Lemma 2: If $m \neq 2^r$ for any r, then $A_0 = (1, 0, 0, 0)$ leads to a nontrivial cycle.

Proof: Let $B = (a, b, c, d)$ and so $S(B) = a+b+c+d$. Obviously, we have $S(\mathcal{D}_m B) = 2S(B)$ and it follows by induction that $S(\mathcal{D}_m^k B) = 2^k S(B)$.

For A_0 we get $S(A_0) = 1$ and so $S(\mathcal{D}_m^k A_0) = 2^k$. But, as m does not equal a power of 2, it follows that $2^k \not\equiv 0 \bmod m$ for every $k \in \mathbb{N}$. Thus, $(0, 0, 0, 0)$ cannot be found in the sequence produced by A_0. □

The 4-tuple A_0 also gives rise to a cycle of maximum length.

Theorem 2: The length of the cycle produced by A_0 equals $\ell(m)$ for every m and the length of the cycle produced by any 4-tuple divides $\ell(m)$.

Proof: We observe that $\mathcal{D}_m$ is a linear operator and that every 4-tuple can be written as a linear combination of the cyclic permutations of A_0. Let ℓ be the length of the cycle produced by A_0, k such that $\mathcal{D}_m^k A_0$ is in the cycle, and $B = (a, b, c, d)$ a given 4-tuple. Then $B = a(1, 0, 0, 0) + b(0, 1, 0, 0) + c(0, 0, 1, 0) + d(0, 0, 0, 1)$ and

$$\begin{aligned}\mathcal{D}_m^{\ell+k} B &= a\mathcal{D}_m^{\ell+k}(1, 0, 0, 0) + b\mathcal{D}_m^{\ell+k}(0, 1, 0, 0) + c\mathcal{D}_m^{\ell+k}(0, 0, 1, 0) + d\mathcal{D}_m^{\ell+k}(0, 0, 0, 1)\\ &= a\mathcal{D}_m^{k}(1, 0, 0, 0) + b\mathcal{D}_m^{k}(0, 1, 0, 0) + c\mathcal{D}_m^{k}(0, 0, 1, 0) + d\mathcal{D}_m^{k}(0, 0, 0, 1) = \mathcal{D}_m^k B.\end{aligned}$$

Thus, the cycle produced by A_0 has maximum length and the length of the cycle produced by B must divide $\ell(m)$. □

Here we have a close relation to the cycles of Ducci-sequences. The n-tuple $(1, 0, \ldots, 0)$ produces a cycle of maximum length in a Ducci-sequence for every n and it is not contained in a cycle itself (see [2], Corollary 2). The second statement is also valid for our 4-tuple A_0.

Lemma 3: The 4-tuple $A_0 = (1, 0, 0, 0)$ is not contained in any cycle.

Proof: Assume that A_0 is contained in a cycle. Then there is a $B = (a, b, c, d)$ such that $\mathcal{D}_m B = A_0$. Consequently,

$$a+b=1,\ b+c=0,\ c+d=0,\ d+a=0.$$

Thus, $b=-c, -c=d, d=-a$, and $b=-a$. But then $a+b=a-a=0$, which is a contradiction to the equation for the first entry. □

In the next theorem, we use a well-known fact from number theory: $\mathbb{Z}_m \cong \mathbb{Z}_{p_1^{t_1}} \oplus \cdots \oplus \mathbb{Z}_{p_r^{t_r}}$ if $p_1^{t_1} \cdot \ldots \cdot p_r^{t_r}$ is the decomposition of m into prime numbers, where $\oplus$ denotes the "usual" direct sum.

Theorem 3: Let $m = p_1^{t_1} \cdot \ldots \cdot p_r^{t_r}$. Then $\ell(m) = \mathrm{lcm}\{\ell(p_1^{t_1}), \ldots, \ell(p_r^{t_r})\}$ (lcm denotes the least common multiple.

Proof: We consider a sequence with A_0 as the first 4-tuple. There is a k_l for every l so that $\mathcal{D}_l^{k_l} A_0$ is contained in a cycle.

Let $m = p_1^{t_1} \cdot \ldots \cdot p_r^{t_r}$ and k be the maximum of $\{k_{p_1^{t_1}}, \ldots, k_{p_r^{t_r}}, k_m\}$. Then $\mathcal{D}_m^k A_0 = (a, b, c, d)$ lies in a cycle over $\mathbb{Z}_m$ as well as over each of the $\mathbb{Z}_{p_i^{t_i}}$. Since $\mathcal{D}_m$ is linear, we obtain

$$\underbrace{(a,b,c,d)}_{\in\mathbb{Z}_m^4} \cong (\underbrace{(a_1,b_1,c_1,d_1)}_{\in\mathbb{Z}_{p_1^{t_1}}^4}, \ldots, \underbrace{(a_r,b_r,c_r,d_r)}_{\in\mathbb{Z}_{p_r^{t_r}}^4}).$$

Further, $\mathfrak{D}_m(a,b,c,d) \cong (\mathfrak{D}_{p_1^{t_1}}(a_1,b_1,c_1,d_1), \ldots, \mathfrak{D}_{p_r^{t_r}}(a_r,b_r,c_r,d_r))$. Let $B=\mathfrak{D}_m^k A_0$. From the above construction, it follows that $\mathfrak{D}_m^h B = B$ over $\mathbb{Z}_m$ for some minimal h if and only if $\mathfrak{D}_m^h B = B$ over all $\mathbb{Z}_{p_i^{t_i}}$. Clearly, h is the least common multiple of the $\ell(p_i^{t_i})$ and $\ell(m)=h$. □

Corollary 1: Let m be odd. Then $\ell(2^r m) = \ell(m)$.

Proof: The proof is obvious since $\ell(2^r)=1$ by Theorem 1. □

For our further investigation, we have to examine four special 4-tuples more closely. Let

$$X_1=(1,-1,1,-1),\ X_2=(1,1,1,1),\ X_3=(1,-1,-1,1),\ X_4=(1,1,-1,-1).$$

If p is an odd prime, these 4-tuples are linearly independent over $\mathbb{Z}_p$, so every 4-tuple can be written as a linear combination of the X_i over $\mathbb{Z}_p$ in exactly one way. Further, the 4-tuples X_i have some special properties:

$$\begin{aligned}
\mathfrak{D}_p X_1 &= (0,0,0,0),\\
\mathfrak{D}_p X_2 &= 2X_2,\\
\mathfrak{D}_p X_3 &= X_3 - X_4,\\
\mathfrak{D}_p^2 X_3 &= -2X_4,\\
\mathfrak{D}_p X_4 &= X_3 + X_4,\\
\mathfrak{D}_p^2 X_4 &= 2X_3.
\end{aligned}$$

We consider $A_1=(1,0,0,1)=\mathfrak{D}_m A_0$. If m is an odd prime, we can write A_1 as

$$A_1 = 2^{-1}((1,1,1,1)+(1,-1,-1,1)) = 2^{-1}(X_2+X_3).$$

By induction, we deduce the following set of equations (the powers of 2 still have to be reduced modulo p):

$$\mathfrak{D}_p^{8k} A_1 = 2^{-1}(2^{8k}X_2 + 2^{4k}X_3), \tag{1}$$
$$\mathfrak{D}_p^{8k+1} A_1 = 2^{-1}(2^{8k+1}X_2 + 2^{4k}(X_3 - X_4)), \tag{2}$$
$$\mathfrak{D}_p^{8k+2} A_1 = 2^{-1}(2^{8k+2}X_2 - 2^{4k+1}X_4), \tag{3}$$
$$\mathfrak{D}_p^{8k+3} A_1 = 2^{-1}(2^{8k+3}X_2 - 2^{4k+1}(X_3 + X_4)), \tag{4}$$
$$\mathfrak{D}_p^{8k+4} A_1 = 2^{-1}(2^{8k+4}X_2 - 2^{4k+2}X_3), \tag{5}$$
$$\mathfrak{D}_p^{8k+5} A_1 = 2^{-1}(2^{8k+5}X_2 - 2^{4k+2}(X_3 - X_4)), \tag{6}$$
$$\mathfrak{D}_p^{8k+6} A_1 = 2^{-1}(2^{8k+6}X_2 + 2^{4k+3}X_4), \tag{7}$$
$$\mathfrak{D}_p^{8k+7} A_1 = 2^{-1}(2^{8k+7}X_2 + 2^{4k+3}(X_3 + X_4)), \tag{8}$$
$$\mathfrak{D}_p^{8(k+1)} A_1 = 2^{-1}(2^{8(k+1)}X_2 - 2^{4(k+1)}X_3). \tag{9}$$

Since 2 is in the group of units $\mathbb{Z}_m^*$ if and only if m is odd, these equations also hold for every such m. If m is even, the equations cannot be used, as 2 is not a unit in $\mathbb{Z}_m$ and 2^{-1} does not exist.

The above set of equations is the cornerstone of the following proofs. Before fully exploiting these equations, we need one more definition.

Definition 6: Let m be an odd number. Then we denote the order of 2 in the group of units of $\mathbb{Z}_m$ as $O_m(2)$.

Lemma 4: If m is odd, then A_1 is contained in the cycle produced by A_0.

Proof: We use equation (1):

$$\begin{aligned}\mathcal{D}_m^{8O_m(2)}A_1 &= 2^{-1}(2^{8O_m(2)}X_2 + 2^{4O_m(2)}X_3)\\ &= 2^{-1}((2^{O_m(2)})^8X_2 + (2^{O_m(2)})^4X_3)\\ &= 2^{-1}(X_2+X_3) = A_1. \quad \square\end{aligned}$$

Corollary 2: If m is odd, then $\ell(m)|8O_m(2)$.

Theorem 4: For every odd m, $O_m(2)|\ell(m)$.

Proof: By Theorem 2 and Lemma 4, A_1 is in the cycle of maximum length for every odd m. Obviously, $S(A_1)=2$. Since $S(\mathcal{D}_m^{\ell(m)}A_1)=S(A_1)=2$ and $S(\mathcal{D}_mC)=2S(C)$ for every 4-tuple C, it follows that $S(\mathcal{D}_m^{\ell(m)-1}A_1)=1$.

On the other hand, using $S(\mathcal{D}_mC)=2S(C)$, we can conclude by induction that $S(\mathcal{D}_m^{\ell(m)-1}A_1)=2^{\ell(m)-1}S(A_1)=2^{\ell(m)}$; thus, $2^{\ell(m)}\equiv 1 \bmod m$. Euler's well-known theorem completes the proof. $\square$

Now we can give a characterization of $\ell(p)$ for every prime p.

Theorem 5: Let p be an odd prime. Then

$$\ell(p)=\begin{cases} O_p(2) & : \ 4|O_p(2),\ 8\nmid O_p(2),\\ 2O_p(2) & : \ 8|O_p(2),\\ 4O_p(2) & : \ 2|O_p(2),\ 4\nmid O_p(2),\\ 8O_p(2) & : \ 2\nmid O_p(2).\end{cases}$$

Proof: Corollary 2 shows $\ell(p)|8O_p(2)$. On the other hand, we know from Theorem 4 that $O_p(2)|\ell(p)$. Thus, we only have to check $O_p(2), 2O_p(2)$, and $4O_p(2)$ as possible values for $\ell(p)$.

1. $4|O_p(2)$, $8\nmid O_p(2)$: We can write $O_p(2)=4(2s+1)=8s+4$ for an $s\in\mathbb{N}_0$. Equation (5) shows:

$$\begin{aligned}\mathcal{D}_p^{O_p(2)}A_1 &= 2^{-1}(2^{8s+4}X_2 - 2^{4s+2}X_3)\\ &= 2^{-1}(2^{O_p(2)}X_2 - 2^{\frac{O_p(2)}{2}}X_3)\\ &= 2^{-1}(X_2+X_3)=A_1.\end{aligned}$$

Thus, $\ell(p)=O_p(2)$. Here we have used the fact that $(2^{[O_p(2)]/2})^2=2^{O_p(2)}\equiv 1 \bmod p$ and, since $\mathbb{Z}_p$ is a field, the equation $x^2\equiv 1 \bmod p$ has the two solutions 1 and -1. From the definition of $O_p(2)$, it follows that $2^{[O_p(2)]/2}\equiv -1 \bmod p$.

2. $8|O_p(2)$: Assume that $\ell(p)=O_p(2)$. Since $O_p(2)=8(2s+1)$, we can use equation (9):

$$\begin{aligned}\mathcal{D}_p^{O_p(2)}A_1 &= 2^{-1}(2^{8(2s+1)}X_2 + 2^{4(2s+1)}X_3)\\ &= 2^{-1}(X_2-X_3)\neq A_1.\end{aligned}$$

Using equation (9) again, we can conclude that $\mathfrak{D}_p^{2O_p(2)} A_1 = A_1$ and thus $\ell(p) = 2O_p(2)$.

3. $2|O_p(2)$, $4\nmid O_p(2)$: We consider $4O_p(2)$. Obviously, $8|4O_p(2)$ and so, by equation (1),

$$\begin{aligned}\mathfrak{D}_p^{4O_p(2)} A_1 &= 2^{-1}(2^{4O_p(2)} X_2 + 2^{2O_p(2)} X_3)\\ &= 2^{-1}(X_2 + X_3) = A_1.\end{aligned}$$

Now assume $\ell(p) = 2O_p(2)$. Since $O_p(2) = 2(2s+1)$, we can use equation (5):

$$\begin{aligned}\mathfrak{D}_p^{2O_p(2)} A_1 &= 2^{-1}(2^{2O_p(2)} X_2 - 2^{O_p(2)} X_3)\\ &= 2^{-1}(X_2 - X_3) \neq A_1.\end{aligned}$$

So $\ell(p) = 4O_p(2)$.

4. $2\nmid O_p(2)$: Now we can write $4O_p(2) = 4(2s+1)$ and, using basically the same calculations as in the case above, we see that $\ell(m)$ cannot equal $4O_p(2)$ or one of its divisors. □

Corollary 3: If p is a prime and $p \equiv -1 \bmod 4$, then

$$\ell(p) = \begin{cases} 4O_p(2) & : \ 2|O_p(2), \\ 8O_p(2) & : \ 2\nmid O_p(2). \end{cases}$$

Proof: By Euler's formula, $O_p(2)|(p-1)$. But $p-1 \equiv -2 \bmod 4$; thus, neither $p-1$ nor $O_p(2)$ is divisible by 4. □

Before stating another consequence of Theorem 5, we want to mention an easy way to determine whether $O_p(2)$ is even or odd.

Lemma 5: If p is a prime and $p \equiv -1 \bmod 4$, then $O_p(2)$ is odd if and only if $(p+1)/4$ is even.

For further details and the proof, see Lemma 13 in [4].

Corollary 4: Let p be a prime. If $p \equiv -1 \bmod 4$, then $\ell(p)|4(p-1)$. If $p \equiv 1 \bmod 4$, then $\ell(p)|2(p-1)$.

Proof: We treat the case $p \equiv -1 \bmod 4$ first. Obviously, $p-1$ is even. If $O_p(2)$ is odd, then $O_p(2)\Big|\frac{p-1}{2}$ and so $8O_p(2)\Big|8\frac{p-1}{2}$. If $O_p(2)$ is even, the result is obvious.

The proof for $p \equiv 1 \bmod 4$ runs along the same lines. □

Remark: If $p \equiv 1 \bmod 4$, then $\ell(p)$ is even a divisor of $p-1$. This can be shown using some techniques of Ehrlich [2] and writing $\mathfrak{D}_p$ as a sum of two operators.

We have shown that every $\ell(m)$ can be computed if the decomposition of m into prime numbers and $\ell(p^r)$ for $p^r|m$ are known. We have determined $\ell(p)$ [in terms of $O_p(2)$] but have not yet investigated powers of primes. In this case, we can give only a partial solution.

Theorem 6: Let $m = p^r$ for some odd prime p. Then

1. $\ell(p)|\ell(m)$,

2. $\ell(m)|p^{r-1}\ell(p)$.

Proof:

1. Obviously, $\mathcal{D}_m^{\ell(m)} A_1 = A_1$ and so $\mathcal{D}_p^{\ell(m)} A_1 = A_1$. Thus, $\ell(p) | \ell(m)$.

2. From $\mathcal{D}_p^{\ell(p)} A_1 = A_1$, we deduce, by induction, that $\mathcal{D}_{sp}^{s\ell(p)} A_1 = A_1$ for every odd s and, consequently, $\mathcal{D}_m^{p^{r-1}\ell(p)} A_1 = \mathcal{D}_{p^{r-1}p}^{p^{r-1}\ell(p)} A_1 = A_1$. Thus, $\ell(m) | p^{r-1}\ell(p)$. □

Remark: There are cases in which $\ell(p^r) < p^{r-1}\ell(p)$, e.g., for $p = 1093$,

$$\ell(p) = \frac{p-1}{3} = \ell(p^2).$$

We will end this section with a final observation.

Corollary 5: If m is odd, then $4 | \ell(m)$.

Proof: From Theorem 5, we deduce that $4 | \ell(p)$ for every prime p. Thus, $4 | \ell(p^r)$ by Theorem 6 and $4 | \ell(m)$ by Theorem 3. □

THE LIFE SPAN

As we have seen above, A_0 produces a cycle of maximum length. It also has the highest possible life span.

Lemma 6: Let B be a 4-tuple. Then $\mathcal{L}_m(B) \le \mathcal{L}_m(A_0)$.

Proof: B can be written as a linear combination of the cyclic permutations of A_0 (see the proof of Theorem 2). If $\mathcal{D}_m^k A_0 = (0, 0, 0, 0)$ for some k, then $\mathcal{D}_m^k C = (0, 0, 0, 0)$, where C is any cyclic permutation of A_0. Thus, $\mathcal{D}_m^k B = (0, 0, 0, 0)$. □

Therefore, we can limit our investigation to A_0. Before stating our last theorem, we need some further notations and a rather technical lemma.

Notations: Let $\mathcal{D}$ and $\mathcal{H}$ be the operators on 4-tuples over $\mathbb{Z}$ defined by $\mathcal{D}(a, b, c, d) = (a+b, b+c, c+d, d+a)$ and $\mathcal{H}(a, b, c, d) = (b, c, d, a)$. Obviously, $\mathcal{D}A \equiv \mathcal{D}_m A \bmod m$ for every 4-tuple A with entries from $\mathbb{Z}$. If every entry of A is divisible by $r \in \mathbb{N}$, we write $A \equiv 0 \bmod r$.

Lemma 7: Let $B = (b-2, b-1, b, b-1)$, where $b \ge 3$ is odd. Then $\mathcal{D}B \not\equiv 0 \bmod 2$ and $\mathcal{D}^2 B = 2\mathcal{H}C$, where $C = (c-2, c-1, c, c-1)$ and c is odd.

Proof:

$$\begin{aligned} \mathcal{D}^2 B &= \mathcal{D}(2b-3, 2b-1, 2b-1, 2b-3) \\ &= (4b-4, 4b-2, 4b-4, 4b-6) \\ &= 2(2b-2, 2b-1, 2b-2, 2b-3) \\ &= 2(c-1, c, c-1, c-2), \end{aligned}$$

where $c = 2b-1$. □

Theorem 7: Let $m \ge 2, m = 2^r k$ for some $r \in \mathbb{N}_0$ and k an odd natural number. Then

$$\mathcal{L}_m(A_0) = \begin{cases} 1 & : r = 0, \\ 2r+2 & : r \ge 1. \end{cases}$$

Proof:

- Let $r=0$, i.e., m is odd. Lemma 4 shows that $A_1=\mathcal{D}_m A_0$ is in a cycle and Lemma 6 completes the proof.
- Let $r \geq 1$, i.e., m is even. As in Theorem 3, we can compute over $\mathbb{Z}_{p_1^{t_1}} \oplus \cdots \oplus \mathbb{Z}_{p_s^{t_s}}$. Since $\mathcal{D}_{p^r} A_0$ is in a cycle for every odd prime p, we have to consider only the case $p_i^{t_i}=2^r$. We compute $\mathcal{D}^k A_0$:

$$\begin{aligned} A_0 &= (1, 0, 0, 0), \\ A_1 &= (1, 0, 0, 1), \\ A_2 &= (1, 0, 1, 2), \\ A_3 &= (1, 1, 3, 3), \\ A_4 &= (2, 4, 6, 4). \end{aligned}$$

Obviously, only the entries of A_4 are all divisible by 2. We can write A_4 as $A_4=2\cdot(3-2, 3-1, 3, 3-1)$. Thus, we can apply the preceding lemma, and it follows by induction that $A_{2r+2} \equiv 0 \bmod 2^r$ and $A_k \not\equiv 0 \bmod 2^r$ for $k<2r+2$. Therefore, $A_l \equiv 0 \bmod 2^r$ if and only if $\ell \geq 2r+2$ and $\mathcal{L}_m(A_0)=2r+2$. □

ACKNOWLEDGMENTS

I am indebted to Mr. Herbert Glaser for introducing me to this interesting problem and giving me a number of useful hints. I would also like to thank the referee for a number of valuable suggestions.

REFERENCES

1. C. Ciamberlini & A. Marengoni. "Su una interessante curiosità numerica." *Periodiche di Matematiche* **17** (1937):25-30.
2. A. Ehrlich. "Periods in Ducci's *N*-Number Game of Differences." *The Fibonacci Quarterly* **28.4** (1990):302-05.
3. A. Engel. *Mathematisches Experimentieren mit dem Computer* (Chapter 63, pp. 231-36). Stuttgart: Klett-Schulbuchverlag, 1991.
4. H. Glaser & G. Schöffl. "Ducci-Sequences and Pascal's Triangle." *The Fibonacci Quarterly* **33.4** (1995):313-24.
5. A. Ludington-Furno. "Cycles of Differences of Integers." *J. Number Theory* **13** (1981):255-61.
6. L. Meyers. "Ducci's Four-Number Problem: A Short Bibliography." *Crux Mathematicorum* **8** (1982):262-66.
7. F.-B. Wong. "Ducci Processes." *The Fibonacci Quarterly* **20.2** (1982):97-105.

AMS Classification Numbers: 00A08, 11B37, 11B65

❖❖❖