DUCCI-SEQUENCES AND PASCAL'S TRIANGLE

Herbert Glaser
Mathematisches Institut (Didaktik), Universität Würzburg, Germany

Gerd Schöffl
Korngasse 1, 97070 Würzburg, Germany

(*Submitted November 1993*)

INTRODUCTION

The so-called *Ducci-sequences* (or *n-number-game*) have recently been studied by several authors in this review (see [1] , [5], [6], [12], [17], and others). A Ducci-sequence is a sequence of n-tuples $A_i = (a_1, a_2, \ldots, a_n)$; the first n-tuple A_0 is any given n-tuple with nonnegative integer entries, $A_{i+1} := \mathcal{T}A_i$, where $\mathcal{T}$ is defined as follows:

$$\mathcal{T}A_i := (|a_1 - a_2|, |a_2 - a_3|, \ldots, |a_n - a_1|).$$

The n-tuple A_{i+1} is called the (direct) *successor* of A_i, whereas A_i is the *predecessor* of A_{i+1}. As the maximum entry of the n-tuples cannot increase under the application of $\mathcal{T}$ and therefore the number of successors of any A_0 is bounded, the sequence always leads to a cycle of repeating n-tuples or to the n-tuple $(0, \ldots, 0)$. If an n-tuple A_0 gives rise to the latter, it is usually called *vanishing.*

First, it will be shown in this article that the Ducci-sequences are closely related to *Pascal's triangle* and many properties of their cyclic structures can be found and proved considering Pascal's triangle modulo 2. In the second part we will examine whether, for a given $n \in \mathbb{N}$ there is such an M that $2^M \equiv -1 \bmod n$, which is crucial for some properties of the Ducci-sequences.

We would like to thank the referee for a number of valuable suggestions.

SOME BASIC PROPERTIES AND DEFINITIONS

It is a well-known fact that every n-tuple with integer entries vanishes if and only if n is a power of 2 (e.g., [4]). On the other hand, the n-tuples in the cycles of the Ducci-sequences are constant multiples of binary n-tuples ([6], [3]). As $\mathcal{T}(\lambda A) = \lambda \mathcal{T} A$ for every $\lambda \in \mathbb{N}_0$, we can limit any investigation of cycles to n-tuples over $\mathbb{Z}_2$. Since $|a-b| \equiv (a+b) \bmod 2$ for all integers a and b, we can use the linear operator $\mathcal{D}$ instead of $\mathcal{T}$, where $\mathcal{D}A := (a_1 + a_2, a_2 + a_3, \ldots, a_n + a_1) \bmod 2$ and A is a binary n-tuple. The operator $\mathcal{D}$ can be written as the sum of two linear operators over $\mathbb{Z}_2$: $\mathcal{D} = \mathcal{I} + \mathcal{H}$, where $\mathcal{I}$ is the identity and $\mathcal{H}A := (a_2, \ldots, a_n, a_1)$. Obviously, we get $\mathcal{H}^n = \mathcal{I}$ and $\mathcal{H}^{-1} = \mathcal{H}^{n-1}$, where $\mathcal{H}^{-1}$ is the inverse operator of $\mathcal{H}$.

We denote the k^{th} successor $\mathcal{D}^k A_0$ of a given binary n-tuple A_0 as A_k. If it is necessary to describe the entries of a certain successor A_k, we will use two indices and write $A_k = (a_{k,1}, \ldots, a_{k,n})$. Then we get:

$$A_{k+1,i} = a_{k,i} + a_{k,i+1}.$$

The subscripts denoting the place in the n-tuple are always reduced modulo n, using n instead of 0.

Ehrlich proved in [6] that the n-tuple $A_0 = (0, \dots, 0, 1)$ (and every cyclic permutation of A_0) produces a cycle of maximum length. The length of all other cycles of n-tuples of a given n divide this maximum. The sequence $\{A_k\}$ is called the *basic-Ducci-sequence* (*of n-tuples*) and the length of its periodic cycle is denoted as $\mathcal{P}(n)$. For every odd n, the first n-tuple in a cycle is $\mathcal{D}A_0 = A_1 = (0, \dots, 0, 1, 1)$. Further, Ehrlich stated the following theorems:

- If $2^m \equiv 1 \bmod n$, then $\mathcal{P}(n)$ divides $2^m - 1$. (1)
- If $2^M \equiv -1 \bmod n$, then $\mathcal{P}(n)$ divides $n(2^M - 1)$. (2)
- If n is not a power of 2, then n divides $\mathcal{P}(n)$. (3)
- If $n = 2^r \ell$, where ℓ is odd, then $\mathcal{P}(n) = 2^r \mathcal{P}(\ell)$. (4)

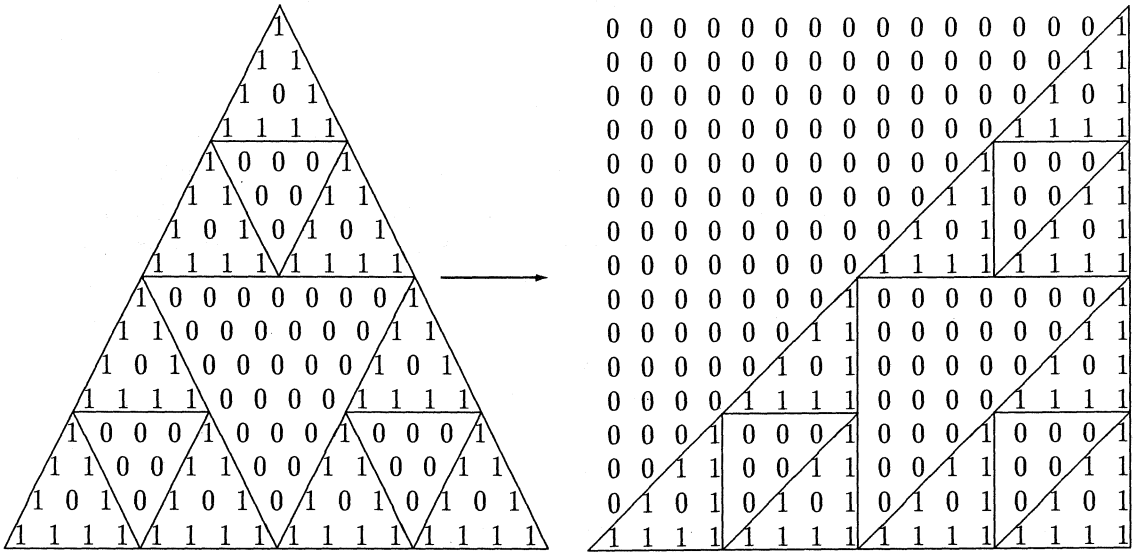
Before we take a closer look at the properties of Pascal's triangle, we will state a theorem that allows a new approach to our problem.

A NEW APPROACH TO AN OLD PROBLEM

In Pascal's triangle, we find the binomial coefficient $\binom{k}{i}$ of the i^{th} place in the k^{th} row. The 0^{th} row consists of a single one. When we place zeros left and right of the triangle, we can obtain any element by adding the two elements to the left and right above its place. This is easy to see, knowing the formula for adding the binomial coefficients:

$$\binom{k}{i} + \binom{k}{i+1} = \binom{k+1}{i+1}.$$

We will limit our investigation to $\mathbb{Z}_2$, and thus every binomial coefficient shall be considered modulo 2. Pascal's triangle modulo 2 with n rows (i.e., row 0 to row $n-1$) will be denoted as PT_n. The number of a chosen row shall be denoted as k. We fill up every k^{th} row of a PT_n with $n-k-1$ zeros on the left side. By shifting to the right and considering the rows as n-tuples, we obtain a square of n different n-tuples.



```
                1                              0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 1
               1 1                             0 0 0 0 0 0 0 0 0 0 0 0 0 0 1 1
              1 0 1                            0 0 0 0 0 0 0 0 0 0 0 0 0 1 0 1
             1 1 1 1                           0 0 0 0 0 0 0 0 0 0 0 0 1 1 1 1
            1 0 0 0 1                          0 0 0 0 0 0 0 0 0 0 0 1 0 0 0 1
           1 1 0 0 1 1                         0 0 0 0 0 0 0 0 0 0 1 1 0 0 1 1
          1 0 1 0 1 0 1                        0 0 0 0 0 0 0 0 0 1 0 1 0 1 0 1
         1 1 1 1 1 1 1 1                       0 0 0 0 0 0 0 0 1 1 1 1 1 1 1 1
        1 0 0 0 0 0 0 0 1          ------>     0 0 0 0 0 0 0 1 0 0 0 0 0 0 0 1
       1 1 0 0 0 0 0 0 1 1                     0 0 0 0 0 0 1 1 0 0 0 0 0 0 1 1
      1 0 1 0 0 0 0 0 1 0 1                    0 0 0 0 0 1 0 1 0 0 0 0 0 1 0 1
     1 1 1 1 0 0 0 0 1 1 1 1                   0 0 0 0 1 1 1 1 0 0 0 0 1 1 1 1
    1 0 0 0 1 0 0 0 1 0 0 0 1                  0 0 0 1 0 0 0 1 0 0 0 1 0 0 0 1
   1 1 0 0 1 1 0 0 1 1 0 0 1 1                 0 0 1 1 0 0 1 1 0 0 1 1 0 0 1 1
  1 0 1 0 1 0 1 0 1 0 1 0 1 0 1                0 1 0 1 0 1 0 1 0 1 0 1 0 1 0 1
 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1               1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
```

The i^{th} entry in the k^{th} row will be denoted as $a_{k,i}$. We obtain:

$$a_{k,i} = \begin{cases} 0 & : 1 \le i \le n-k-1, \\ \binom{k}{i-n+k} & : n-k \le i \le n. \end{cases}$$

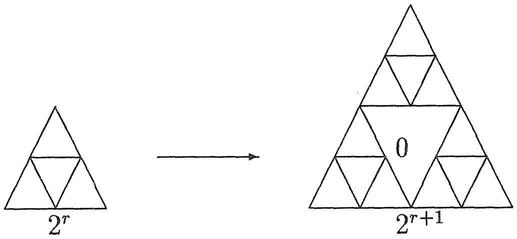
Adopting the above formula for the binomial coefficients, we get $a_{k+1,i} = a_{k,i} + a_{k,i+1}$:

- $1 \le i \le n-k-2: a_{k+1,i} = 0 = a_{k,i} + a_{k,i+1}$.
- $i = n-k-1: a_{k+1,i} = 1 = 0+1 = a_{k,i} + \binom{k+1}{0} = a_{k,i} + a_{k,i+1}$.
- $n-k \le i \le n: a_{k+1,i} = \binom{k+1}{i-n+k+1} = \binom{k}{i-n+k} + \binom{k}{i-n+k+1} = a_{k,i} + a_{k,i+1}$.

Considering that the n-tuple in the 0^{th} row is $(0, \ldots, 0, 1) = A_0$, the first n-tuple of the *basic-Ducci-sequence*, we have shown

Theorem 1: The n rows in the modified Pascal triangle (as shown above) are the n-tuples A_0, A_1, $\ldots$, A_{n-1} of the *basic-Ducci-sequence*.

We will now take a closer look at Pascal's triangle. This triangle shows an interesting geometry which is closely related to that of the Sierpinski gasket (cf. [14]). Therefore, the PT_{2^r} for $r \in \mathbb{N}$ can be constructed recursively. For a given PT_{2^r}, $r \in \mathbb{N}$, we get $PT_{2^{r+1}}$ by placing two PT_{2^r}'s at the corners of the base of the first PT_{2^r} and filling up the empty triangle with zeros:



This construction can be proved using a lemma of Hinz ([8], p. 541).

Lemma 1: For $0 \le k, i < 2^r$, and $r \in \mathbb{N}_0$, it follows that

$$\binom{2^r + k}{i} \equiv \binom{k}{i} \mod 2.$$

In [8] we can find some additional facts that have been stated by Lucas [10] and Glaisher (reference can be found in Stolarsky [16]) and can be proved with the help of the above lemma ([8], p. 539):

- For $0 \le i \le k$, the binomial coefficients $\binom{k}{i}$ are all odd if and only if $k = 2^r - 1$ for some $r \in \mathbb{N}_0$. (5)
- For $0 < i < k$, the binomial coefficients $\binom{k}{i}$ are all even if and only if k is a power of 2 (the outer elements are 1). (6)
- Let $\beta(k)$ be the number of ones in the 2-adic expansion of $k \in \mathbb{N}_0$. Then the number of odd binomial coefficients $\binom{k}{i}$ for $0 \le i \le k$ is $2^{\beta(k)}$. (7)

The advantage of using PT_n for examining the Ducci-sequences is the fact that many properties of the cycles can easily be seen. Regarding the fractal geometry of the triangle, the results can be observed for small n and generalized for higher ones. For example, if we take a look at the PT_{2^r}, we see that the row $2^r - 1$ contains only ones. This leads us to an easy proof of the well-known fact that every 2^r-tuple with integer entries vanishes (see [4], [7], [3], et al.).

In the same way, we can prove all the following new results. As some of the proofs are quite long when using exclusively Pascal's triangle, we will adopt other techniques as well.

CYCLES OF SOME DUCCI-SEQUENCES

Following Ehrlich [6], we say n **is with a** -1 if $n \in \mathbb{N}$ is odd and there exists an $M \in \mathbb{N}$ with $2^M \equiv -1 \bmod n$; otherwise, we call n **without a** -1. We will now give a lower bound for $\mathcal{P}(n)$ for every n with a -1 [for an upper bound, see (2)]. First, we have to state the following lemma.

Lemma 2: Let n be with a -1 and $k \in \mathbb{N}, k \geq 1$. Then

$$\mathcal{D}^{k(2^M-1)+1} = \mathcal{H}^{-k}\mathcal{D}.$$

Proof: We proceed by induction using Ehrlich's Lemma 1 ([6], p. 302):

$$2^m \equiv t \bmod n \Rightarrow \mathcal{D}^{2^m} = \mathcal{I} + \mathcal{H}^t.$$

Let $k = 1$. Then we get

$$\mathcal{D}^{(2^m-1)+1} = \mathcal{D}^{2^M} = \mathcal{I} + \mathcal{H}^{-1} = \mathcal{H}^{-1}\mathcal{D}.$$

Assume now that the statement is true for $k \in \mathbb{N}$. It follows by computation that

$$\begin{aligned}\mathcal{D}^{(k+1)(2^M-1)+1} &= \mathcal{D}^{k(2^M-1)+1}\mathcal{D}^{2^M-1} = \mathcal{H}^{-k}\mathcal{D}\mathcal{D}^{2^M-1}\\ &= \mathcal{H}^{-k}\mathcal{D}^{2^M} \qquad = \mathcal{H}^{-k}\,\mathcal{H}^{-1}\,\mathcal{D}\\ &= \mathcal{H}^{-(k+1)}\mathcal{D}. \quad \square\end{aligned}$$

This lemma leads to

Theorem 2: For n with a -1, every cyclic permutation of $A_1 = (0, \ldots, 0, 1, 1)$ can be found in the *basic-Ducci-sequence*.

Proof: As n is odd, the n-tuple A_1 is the first n-tuple in the cycle of the *basic-Ducci-sequence* and $A_1 = \mathcal{D}(0, \ldots, 0, 1)$. Using Lemma 2 above, we obtain $\mathcal{D}^{k(2^M-1)+1}A_0 = \mathcal{H}^{-k}\mathcal{D}A_0$ and therefore $\mathcal{D}^{k(2^M-1)}A_1 = \mathcal{H}^{-k}A_1$ for every $k \in \mathbb{N}$. □

Obviously this result implies that, for every n with a -1, the cyclic permutations of $(0, \ldots, 0, 1)$ give rise to the same cycle, and so there exists only one cycle of maximum length.

Theorem 3: For n with a -1, we get $\mathcal{P}(n) \geq n(n-2)$.

Proof: We have to determine the minimum number of applications of $\mathcal{D}$ for obtaining the first cyclic permutation of A_1 in the *basic-Ducci-cycle*. We use Pascal's triangle. A permutation of A_1 consists of two adjacent ones (where $a_{1,1}$ and $a_{1,n}$ are considered as being adjacent as well). Since the last and the first entry of Pascal's triangle are always ones, the number of ones in every row is at least 2. Thus, we can (possibly) find a cyclic permutation of A_1 for the first time when the first and the last entry of Pascal's triangle can be considered as adjacent ones in an n-tuple, which is to say that $a_{k,1} = 1$. Regarding the construction of n-tuples from Pascal's triangle, it follows that $k = n-1$, that means after $n-2$ applications of $\mathcal{D}$ on A_1. We use the same argument for the successors of the first permutation of A_1, and the proof is complete. □

This theorem gives rise to an important result.

Theorem 4: For n with a –1, it follows that

$$\mathcal{P}(n) = n(n-2) \Leftrightarrow n = 2^r + 1, \ r \in \mathbb{N}.$$

Proof:

"$\Leftarrow$" If $n = 2^r + 1$, then $2^r = n - 1 \equiv -1 \bmod n$ and from Theorem 3 we get $\mathcal{P}(n) \geq n(n-2)$. On the other hand, $\mathcal{P}(n)$ divides $n(2^r - 1) = n(n-2)$ [see property (2)], and so $n(2^r - 1) = n(n-2)$.

"$\Rightarrow$" As n is with a –1, the proof of Theorem 3 shows that $\mathcal{P}(n) = n(n-2)$ if and only if the n-tuple A_{n-1} is a permutation of A_1. According to properties (6) and (7), we obtain exactly two ones in a row of Pascal's triangle if and only if the number of the row is of the form $2^r + 1$. Considering that the ones are adjacent if and only if the n-tuple that is formed from the row $2^r + 1$ of Pascal's triangle is not filled up by zeros, i.e., $n = 2^r + 1$, we have shown our statement. □

Furthermore, we can extend Theorem 4 for every even n with $n = 2^r + 2^s$.

Theorem 5: If $n = 2^r + 2^s$ for $r > s \geq 0$, then $\mathcal{P}(n) = \frac{n(n-2^{s+1})}{2^s}$.

Proof: By using Theorem 4 and Ehrlich's formula (4), we obtain

$$\begin{aligned}\mathcal{P}(2^r + 2^s) &= 2^s \mathcal{P}(2^{r-s} + 1) \\ &= 2^s (2^{r-s} + 1)(2^{r-s} - 1) \\ &= \frac{(2^r + 2^s)(2^r - 2^s)}{2^s} \\ &= \frac{n(n - 2^{s+1})}{2^s}. \quad \square\end{aligned}$$

As mentioned above, Ehrlich [6] was able to describe the first n-tuple in the cycle of the *basic-Ducci-sequence* if n is odd. Nothing is yet known about the case in which n is even. We will be able to give a partial solution at this time.

Theorem 6: For $n = 2^r + 2^s$, $r > s \geq 0$, the n-tuple

$$A_{2^s} = (\underbrace{0, \ldots, 0}_{n-2^s-1}, \underbrace{1, 0, \ldots, 0, 1}_{2^s+1})$$

is the first n-tuple in the cycle of the *basic-Ducci-sequence.*

Proof:

1. The n-tuple is contained in the cycle.

Pascal's triangle PT_n shows us that

$$A_{2^r} = (\underbrace{0, \dots, 0}_{2^2-1}, 1, \underbrace{0, \dots, 0}_{2^r+1}, 1)$$

is a successor of

$$A_{2^s} = (\underbrace{0, \dots, 0}_{2^{r-1}}, 1, \underbrace{0, \dots, 0}_{2^s-1}, 1).$$

Obviously, A_{2^r} is a cyclic permutation of A_{2^s}: $A_{2^r} = \mathscr{H}^{-2^s} A_{2^s}$. On the other hand, we have $A_{2^r} = \mathscr{D}^{2^r-2^s} A_{2^s}$. We can conclude that

$$\mathscr{D}^{\frac{(2^r-2^s)n}{2^s}} A_{2^s} = \mathscr{H}^{-n} A_{2^s} = A_{2^s}$$

and, therefore, A_{2^s} is contained in the cycle. Keeping in mind that the first and the last entry of PT_n are always 1, and counting the consecutive zero-entries, we obtain that A_{2^r} is the only cyclic permutation of A_{2^s} among its successors $A_{2^s+1}, \dots, A_n$, which are contained in the (modified) PT_n. Therefore, we have even shown that A_{2^r} is the first of the cyclic permutations of A_{2^s} that appears in the cycle.

2. A_{2^s} is the first n-tuple in the cycle.

The n-tuple A_{2^s-1} is the predecessor of A_{2^s}. We suppose that A_{2^s-1} is contained in the cycle. It follows from above that the predecessor A_{2^r}, i.e., A_{2^r-1}, is in the cycle. Therefore, A_{2^r-1} must be a cyclic permutation of A_{2^s-1}. A look at PT_n shows that A_{2^s-1} contains 2^s ones, and in A_{2^r-1} we can find 2^r ones [see property (7)]. This is a contradiction to the assertion, as $r > s$. □

Corollary 1: If $n = 2^r + 2^s$, $r > s \geq 0$, then there are 2^s different cycles of maximum length that are produced by the cyclic permutations of the n-tuple A_0.

Proof: The operators $\mathscr{D}$ and $\mathscr{H}$ commute, so

$$\begin{aligned} \mathscr{D}^{2^r-2^s} A_{2^r} &= \mathscr{D}^{2^r-2^s} \mathscr{H}^{-2^s} A_{2^s} \\ &= \mathscr{H}^{-2^s} \mathscr{D}^{2^r-2^s} A_{2^s} = \mathscr{H}^{-2\cdot 2^s} A_{2^s}. \end{aligned}$$

By induction, every n-tuple $\mathscr{H}^{-\ell 2^s} A_{2^s}$, $\ell \in \mathbb{N}$, appears in the cycle of the successors of $(0, \dots, 0, 1)$.

Using the same argument as in the proof of Theorem 6, we conclude that for every ℓ the n-tuple $\mathscr{H}^{-(\ell+1)2^s} A_{2^s}$ is the first cyclic permutation of $\mathscr{H}^{-\ell 2^s} A_{2^s}$ among the successors of the latter. As $2^s \,|\, \mathscr{P}(n)$, no other cyclic permutation than the ones described above can be found in the cycle produced by $(0, \dots, 1)$.

We use the same technique for the successors of $\mathscr{H}^{-1} A_0$, $\mathscr{H}^{-2} A_0, \dots, \mathscr{H}^{-2^s+1} A_0$. □

We will now consider $2^r - 1$-tuples. Using Pascal's triangle, we can determine $\mathscr{P}(n)$ for $n = 2^r - 1$.

Theorem 7: If $r \in \mathbb{N}$ and $n = 2^r - 1$, then $\mathscr{P}(n) = n$.

Proof: Using the proof of Theorem 3, we see that no cyclic permutation of A_1 can be found in fewer than $(n-2)$ steps. Pascal's triangle shows that

$$A_{n-1} = \mathscr{D}^{n-2} A_1 = (1, 0, 1, 0, \ldots, 1, 0, 1).$$

Then $A_n = (1, 1, \ldots, 1, 0)$ and $A_{n+1} = (0, 0, \ldots, 1, 1) = A_1$. □

Corollary 2: For $r \geq 2$ and $n = 2^r - 1$, no cyclic permutation of A_1 can be found in the *basic-Ducci-sequence*, and there are n different cycles of maximum length.

Again, we can extend the last theorem.

Theorem 8: If $n = 2^r - 2^s$, $r > s \geq 0$, then $\mathscr{P}(n) = n$.

Proof: We prove this theorem using Ehrlich's formulas:

$$\mathscr{P}(2^r - 2^s) = 2^s \mathscr{P}(2^{r-s} - 1) = 2^s(2^{r-s} - 1) = n. \quad □$$

It can be shown that only for such an n does the length of the cycle of the *basic-Ducci-sequence* equal n.

Theorem 9: If $\mathscr{P}(n) = n$, then $n = 2^r - 2^s$, where $n \geq 2$ and $r > s \geq 0$.

Proof: Using properties (3) and (4), we can limit our investigation to odd numbers. Then the first n-tuple in the cycle is $A_1 = (0, \ldots, 0, 1, 1)$. There are only two different (possible) predecessors of A_1: the n-tuple $(0, \ldots, 0, 1)$ or the n-tuple $B := (1, \ldots, 1, 0)$ (see [11]). As the first n-tuple is not in the cycle, the predecessor of A_1 in the cycle must be B. As $\mathscr{P}(n) = n$, it follows that $B = A_n$. Since every binary n-tuple has exactly two predecessors, the predecessor of B is either $C := (1, 0, 1, 0, \ldots, 1, 0, 1)$ or $D := (0, 1, 0, 1, \ldots, 0, 1, 0)$. We consider PT_n. The last row represents A_{n-1}, i.e., C or D. It follows from Theorem 1 that the first entry of A_{n-1} must be 1; thus, the predecessor of B in the cycle is C. If we consider PT_{n+1}, then its last row must consist entirely of ones because C is the second to last row of PT_{n+1}. Property (5) shows that all the entries are ones if and only if $n+1$ is a power of 2 and $n = 2^r - 1$ for some $r \geq 2$. (For $n = 2^1 - 1$, the Ducci-problem makes no sense). □

As above, we can answer the question: Which n-tuple is the first one in the cycle?

Theorem 10: The $2^r - 2^s$-tuple A_2, where $n \geq 2$ and $r > s \geq 0$, is the first one in the cycle of the *basic-Ducci-sequence.*

Proof:

1. The n-tuple is contained in the cycle.

From Pascal's triangle, we can conclude (using the recursive construction given above):

$$A_{n-1} = (\underbrace{1, \ldots, 1}_{2^s}, \underbrace{0, \ldots, 0}_{2^s}, \ldots, \underbrace{1, \ldots, 1}_{2^s}).$$

We obtain alternating blocks of 2^s ones and 2^s zeros, the first and the last block consisting of ones. For A_n, we conclude:

$$A_n = (\underbrace{0, \ldots, 0, 1}_{2^s}, \ldots, \underbrace{0, \ldots, 0, 1}_{2^s}, \underbrace{0, \ldots, 0}_{2^s}).$$

As the first $n/2^2-1$ blocks can be considered as the first elements of a *basic-Ducci-sequence* of 2^s-tuples, the next successors are easy to determine. After 2^s-1 applications of $\mathcal{D}$, we find

$$A_{n+2^s-1}=(\underbrace{1,1,\dots,1,1}_{n-2^s},\underbrace{0,\dots,0}_{2^s}).$$

It follows that

$$A_{n+2^s}=(\underbrace{0,\dots,0}_{n-2^s-1},\underbrace{1,0,\dots,0,1}_{2^s+1})=A_{2^s},$$

and the n-tuple A_{2^s} is contained in the cycle.

2. A_{2^s} is the first n-tuple in the cycle.

Using $\mathcal{P}(n)=n$, we can conclude: If A_{2^s-1} is contained in the cycle, then $A_{2^s-1}=A_{n+2^s-1}$. The first entry of A_{2^s-1} must be 0 (see construction of n-tuples from Pascal's triangle). On the other hand, we have shown above that $a_{n+2^s-1,1}=1$, which is a contradiction. □

THE PROBLEM "WITH" OR "WITHOUT" A –1

The question whether a given n is with or without a –1 is important for different theorems and properties of Ducci-sequences [see Theorem 4, properties (1) and (2)].

As every integer n can be considered as a product of prime numbers p, the problem can be divided into two separate questions:

- Which prime numbers are with a –1, which are without? and
- If $m,n\in\mathbb{N}$ and with (-out) a –1, is the product with (-out) a –1?

Prime numbers will be treated first. In the following, p shall denote an odd prime number and $O_p(2)$ shall denote the order of 2 in a cyclic group of unities of the Galois-field $\mathbb{Z}_p$. We keep in mind that $O_p(2)$ is a divisor of $\varphi(p)$—Euler's φ-function—and $\varphi(p)=p-1$.

The case $p\equiv-1 \bmod 4$ is easier to examine.

Lemma 3: Let $p\equiv-1 \bmod 4$, then $O_p(2)$ is odd if and only if $\frac{p+1}{4}$ is even.

Proof: We consider $p\equiv-1 \bmod 4$ first and show the equivalence of three statements:

1. $O_p(2)$ is odd if and only if 2 is a square number in $\mathbb{Z}_p$.

"$\Rightarrow$" Since, by assertion, $O_p(2)$ is odd, we obtain

$$2^{O_p(2)+1}=2=\left(2^{\frac{O_p(2)+1}{2}}\right)^2,$$

and 2 is a square number in $\mathbb{Z}_p$.

"$\Leftarrow$" $2\equiv a^2 \bmod p$ for some $a\in\mathbb{Z}_p$. By Fermat's theorem, $a^{p-1}\equiv 1 \bmod p$ and, as $2|p-1$ (p odd!), we conclude:

$$a^{p-1}=(\underbrace{a^2}_{=2})^{\frac{p-1}{2}}\equiv 1 \bmod p$$

and, further, $2^{\frac{p-1}{2}}\equiv 1 \bmod p$.

Using $p \equiv -1 \bmod 4$, we get $p-1 \equiv -2 \bmod 4$, and $\frac{p-1}{2}$ must be odd.

2. 2 is a square number in $\mathbb{Z}_p$ if and only if $(\frac{2}{p}) = 1$ (Legendre-symbol), which is equivalent to

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = 1.$$

3. $\frac{p+1}{4}$ is even if and only if $\frac{p^2-1}{8}$ is even. We can write p as $p = -1+4k, k \in \mathbb{N}$. Then it follows that $p^2 = 16k^2 - 8k + 1$ or $\frac{p^2-1}{8} = 2k^2 - k$.

As $2k^2$ is always even, we conclude that $\frac{p^2-1}{8}$ is even if and only if k is even. □

Theorem 11: Let $p \equiv -1 \bmod 4$. Then p is with a -1 if and only if $\frac{p+1}{4}$ is odd.

Proof:

"$\Leftarrow$" We consider the equation $x^2 \equiv 1 \bmod p$. As $\mathbb{Z}_p$ is a Galois-field, the equation has exactly two solutions: $x \equiv 1 \bmod p$ and $x \equiv -1 \bmod p$. $2^{\frac{O_p(2)}{2}}$ is an integer solution of this equation if and only if $O_p(2)$ is even, i.e., $\frac{p+1}{4}$ is odd for $p \equiv -1 \bmod 4$ (Lemma 3). As, by definition, $2^{\frac{O_p(2)}{2}}$ cannot be congruent to 1 mod p, we have $2^{\frac{O_p(2)}{2}} \equiv -1 \bmod p$ and p is with a -1.

"$\Rightarrow$" If $2^M \equiv -1 \bmod p$, then it follows that $2M | O_p(2)$, and so the order of 2 is even. From Lemma 3, it follows that $\frac{p+1}{4}$ is odd. □

Let p be with a -1 and M be the least integer number with $2^M \equiv -1 \bmod p$, $M = 2^k \ell$ where $k \geq 0$ and ℓ is odd. For our further examination, we need to know that $k = 0$. We will use a well-known theorem from number theory.

Theorem 12: The congruence $x^2 \equiv -1 \bmod p$ has a solution in $\mathbb{Z}_p$ if and only if $p \equiv 1 \bmod 4$.

This theorem leads us at once to the following corollary.

Corollary 3: M is odd for every $p \equiv -1 \bmod 4$.

Proof: We assume that M is even. Then $a = 2^{\frac{M}{2}}$ satisfies the equation $x^2 \equiv -1$ in contradiction to the above theorem. □

The case $p \equiv 1 \bmod 4$ is harder to treat because the above argument cannot be used in this case. We will give only a partial solution.

Theorem 13: Let $p \equiv 1 \bmod 4$ and $\frac{p+1}{4}$ be odd. Then p is with a -1.

Proof: We again use

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = 1.$$

Since $\frac{p+1}{4}$ is odd ($p \equiv 1 \bmod 4$) as well as $\frac{p+1}{4}$ (by assumption), we conclude that 2 is not a square number in $\mathbb{Z}_p$. Using $2^{O_p(2)+1} \equiv 2 \bmod p$, we see that $O_p(2)+1$ must be odd and $O_p(2)$ is even. By definition, $2^{\frac{O_p(2)}{2}}$ cannot be congruent to 1, so p must be with a -1. □

If $\frac{p+1}{4}$ is even, both cases are possible:

- 17, 41, 97, 113 are with a –1;
- 73, 89, 233 are without a –1.

As the problem is linked to the still unsolved *Artin's Problem* (see [2], p. 113), the complete solution seems to be very difficult but interesting.

We also cannot determine whether M is even or odd. In most cases, M is even; however, for 281, we obtain $M = 35$. This question will be important in our further examination.

We will now treat products of prime numbers.

Lemma 4: Let p be with a –1. Then p^n is with a –1 for every $n \in \mathbb{N}$.

Proof: By induction. Let p^n be with a –1 for some n and $2^M \equiv -1 \bmod p^n$. Then $2^M = -1 + kp^n$ for some k. We compute:

$$2^{pM} = (2^M)^p = (-1+kp^n)^p = -1 + kp^{n+1} + \sum_{i=2}^{p-1} (-1)^{i+1} \binom{p}{i} k^i p^{ni} + p^{np} k^p.$$

As $\binom{p}{i}$ is divisible by p for $2 \le i \le p-1$, we obtain $2^{pM} \equiv -1 \bmod p^{n+1}$. As the lemma holds for $n = 1$, the proof is complete. □

(For a similar problem, see [13], pp. 364 ff.)

Theorem 14: Let $n = p_1 p_2 \dots p_\ell$, the product of odd prime numbers p_i (not necessarily different from each other) and (at least) one of the p_i without a –1, Then the product n is without a –1.

Proof: Without loss of generality, let p_1 be without a –1. We assume that n is with a –1, which means that there exists an $M \in \mathbb{N}$ with $2^M \equiv -1 \bmod n$. This implies that $2^M \equiv -1 \bmod p_1$ in contradiction to the choice of p_1. □

Theorem 15: Let ℓ and m be odd integers with a –1, $(\ell, m) = 1$, $2^L \equiv -1 \bmod \ell$ and $2^M \equiv -1 \bmod m$ (L and M minimal). Then $n = \ell m$ is with a –1 if and only if, for some $k \in \mathbb{N}_0$, 2^k divides L and M, and 2^{k+1} divides neither of them.

Proof:

"$\Leftarrow$" Obviously $L/2^k$ and $M/2^k$ are odd numbers. We compute:

$$(2^L)^{\frac{M}{2^k}} \equiv (-1)^{\frac{M}{2^k}} \bmod \ell \equiv -1 \bmod \ell;$$

$$(2^M)^{\frac{L}{2^k}} \equiv (-1)^{\frac{L}{2^k}} \bmod m \equiv -1 \bmod m.$$

It follows that $2^{\frac{LM}{2^k}} \equiv -1 \bmod n$ as $n = \ell m$.

"$\Rightarrow$" By contradiction:

Assume, without loss of generality, that $2^N \equiv -1 \bmod n$, $2^k | L$, $2^{k+1} \nmid L$, and $2^{k+1} | M$ and N is minimal. This implies that $2^N \equiv -1 \bmod m$, $2^N \equiv -1 \bmod \ell$, and that N is the least common multiple of L and M. Therefore, N is divisible by 2^{k+1} and $N = 2LR$ for some $R \in \mathbb{N}$. It follows by computation that

$$\begin{aligned} 2^N = 2^{2LR} \qquad &= (2^L)^{2R} \\ &\equiv (-1)^{2R} \bmod \ell \equiv 1 \bmod \ell, \end{aligned}$$

which is a contradiction to $2^N \equiv -1 \bmod \ell$ as $\ell \neq 2$. □

Corollary 4: If $p_1, \ldots, p_\ell$ are prime numbers, $p_i \equiv -1$ mod 4, and $\frac{p_i+1}{4}$ is odd for every $1 \le i \le \ell$, then $n = p_1^{k_1} \ldots p_\ell^{k_\ell}$ is with a -1.

Proof: Since $\frac{p+1}{4}$ is odd, p is with a -1 by Theorem 11. By Lemma 4, p^k is with a -1. By Corollary 3, M is odd, where $2^M \equiv -1 \bmod p$. By the proof of Lemma 4, $2^{p^{k-1}M} \equiv -1 \bmod p^k$; of course, the exponent $p^{k-1}M$ is odd. This is true for each prime p. The result now follows by Theorem 15. □

(For a similar result, see [13], p. 364.)

REMAINING QUESTIONS

During our investigation, we have seen that the Ducci-problem is closely linked to the problem of finding the order of 2 in a given field $\mathbb{Z}_p$. It seems that this problem is not yet completely solved.

Going back to the Ducci-sequences, it is interesting to ask how many different orbits the operator $\mathcal{D}$ (and therefore $\mathcal{T}$) produces if *all* Ducci-sequences are considered. If n is not a power of 2, let k be the number of divisors m of n (where $m < n$). Then we can find at least $k+2$ different cycles: the cycle that contains only the n-tuple $(0, \ldots, 0)$, the cycle of the *basic-Ducci-sequence* of n-tuples and the cycle of n-tuples that are formed of the n/m-fold repetition by the m-tuples of the corresponding *basic-Ducci-sequence*.

A whole range of new problems can be obtained using a variation of the process of forming the Ducci-sequence (first done by Wong [17]), for example:

$$\mathcal{T}(a_1, \ldots, a_n) := ((a_1 + a_2) \bmod k, \ldots, (a_n + a_1) \bmod k), \;\; k \in \mathbb{N}.$$

Many interesting results on that topic can be found in [17], but the length of cycles of so-called *Ducci-processes* has not been treated yet (except the above variation in [15]).

REFERENCES

1. K. D. Boklan. "The n-Number Game." *The Fibonacci Quarterly* **22.2** (1984):152-55.
2. P. Bundschuh. *Einführung in die Zahlentheorie*. 2. Auflage. Berlin, Heidelberg, New York: Springer-Verlag, 1992.
3. M. Burmester, R. Forcade, & E. Jacobs. "Circles of Numbers." *Glasgow Mathematical Journal* **19** (1978):115-19.
4. C. Ciamberlini & A. Marengoni. "Su una interessante curiosità numerica." *Periodiche di Matematiche* **17** (1937):25-30.
5. J. W. Creely. "The Length of a Three-Number Game." *The Fibonacci Quarterly* **26.2** (1988):141-43.
6. A. Ehrlich. "Periods in Ducci's N-Number Game of Differences." *The Fibonacci Quarterly* **28.4** (1990):302-05.
7. B. Freedman. "The Four Number Game." *Scripta Mathematica* **14** (1948):35-47.

8. A. Hinz. "Pascal's Triangle and the Tower of Hanoi." *Amer. Math. Monthly* **99** (1992):538-44.
9. M. Lotan. "A Problem in Difference Sets." *Amer. Math. Monthly* **56** (1949):535-41.
10. E. Lucas. *Théeorie des nombres.* 1891, p. 420.
11. A. Ludington Furno. "Cycles of Differences of Integers." *J. Number Theory* **13** (1981):255-61.
12. A. Ludington-Young. "Length of the *n*-Number Game." *The Fibonacci Quarterly* **28.3** (1990):259-65.
13. D. P. Parent. *Exercises in Number Theory.* New York: Springer-Verlag, 1984.
14. H.-O. Peitgen, et al. *Fractale: Selbstähnlichkeit, Chaosspiel, Dimension; ein Arbeitsbuch.,* Ernst Klett Schulbuchverlag, Stuttgart. Berlin, Heidelberg, New York: Springer-Verlag, 1992.
15. G. Schöffl. "Duccifolgen und ihre Behandlung im Unterricht, Zulassungsarbeit zur Wissenschaftlichen Prüfung für das Lehramt an den Gymnasien in Bayern." Unpublished thesis, Mathematisches Institut der Universität Würzburg, 1993.
16. K. B. Stolarsky. "Power and Exponential Sums of Digital Sums Related to Binomial Coefficient Parity." *SIAM J. Appl. Math.* **32** (1977):717-30.
17. F.-B. Wong. "Ducci Processes." *The Fibonacci Quarterly* **20.2** (1982):97-105.

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

❖❖❖