CYCLES OF SUMS OF INTEGERS

BRUNO DULAR

ABSTRACT. We study the period of the linear map $T : \mathbf{Z}_m^n \to \mathbf{Z}_m^n : (a_0, \dots, a_{n-1}) \mapsto (a_0 + a_1, \dots, a_{n-1} + a_0)$ as a function of m and n, where $\mathbf{Z}_m$ stands for the ring of integers modulo m. This map being a variant of the Ducci map, several known results are adapted in the context of T. The main theorem of this paper states that the period modulo m can be deduced from the prime factorization of m and the periods of its prime factors. We give some other interesting properties.

CONTENTS

1. INTRODUCTION

The aim of this paper is to study a variant of the well-known *Ducci game of differences*. In this game, one starts with a n-tuple of integers and iterates the *Ducci map* $(a_0, a_1, \dots, a_{n-1}) \mapsto (|a_0 - a_1|, |a_1 - a_2|, \dots, |a_{n-1} - a_0|)$ to generate a *Ducci sequence*. This process suggests the name *Cycles of differences of integers* [6], which inspired the name of the present paper.

If n is a power of 2, we know that every Ducci sequence eventually vanishes, i.e., reaches the zero n-tuple. Else, a Ducci sequence will either vanish or enter a periodic cycle. As several authors pointed out [5, 6], studying the latter case comes down to considering n-tuples that consist only of 0 and 1's. Hence the Ducci map can be considered to be a linear map over $\mathbf{Z}_2^n$. This map can be generalized as stated in definition 1.1, performing sums modulo m for some positive integer m.

This variant has been introduced by Wong in [14] and has been extensively studied by F. Breuer in [3], who noticed a link between Ducci sequences and cyclotomic polynomials. The results we prove here are similar, but we use an elementary approach, which allows us to solve the inseparable case, i.e., $m = p^t$ with p a prime and n divisible by p. This is the object of section 5. There we also see that our method cannot generalize to special cases ($p = 2$ or p a Wieferich prime), for which F. Breuer's method works.

Date: May 2019.

Here $\mathbf{N}$ denotes the set of positive integers, 0 excluded.

Definition 1.1. Let $m,n \in \mathbf{N}$. Let

$$T : \mathbf{Z}_m^n \to \mathbf{Z}_m^n : \mathbf{a} = (a_0,\ldots,a_{n-1}) \mapsto T\mathbf{a} = (a_0+a_1, a_1+a_2,\ldots,a_{n-1}+a_0).$$

A *T-sequence* of $\mathbf{Z}_m^n$ is a sequence of the form $\left(T^k\mathbf{a}\right)_{k\geq 0}$ where $\mathbf{a} \in \mathbf{Z}_m^n$ and it is said to be generated by the tuple a.

The tuple $\mathbf{e} = (1,0,\ldots,0) \in \mathbf{Z}_m^n$ and the T-sequence it generates are respectively called the *basic tuple* and the *basic T-sequence* of $\mathbf{Z}_m^n$.

For example, the T-sequence generated by the basic tuple of $\mathbf{Z}_{10}^4$ starts as shown below. See that the tuple $(2,4,6,4)$ repeats, hence the T-sequence becomes periodic at that point, with a cycle length of 4. With the notations introduced later, we write $P(10,4) = 4$.

$$\begin{array}{cccccc}
1\,0\,0\,0 & \mapsto & 1\,0\,0\,1 & \mapsto & 1\,0\,1\,2 & \mapsto \\
1\,1\,3\,3 & \mapsto & 2\,4\,6\,4 & \mapsto & 6\,0\,0\,6 & \mapsto \\
6\,0\,6\,2 & \mapsto & 6\,6\,8\,8 & \mapsto & 2\,4\,6\,4 & \mapsto \quad \ldots
\end{array}$$

Remark 1.2. Let $\mathbf{a}$ be a tuple of $\mathbf{Z}_m^n$, where $m = dm'$ for some integers d and m'. We consider $\mathbf{a}$ as an element of $\mathbf{Z}_{m'}^n$ by identifying it to the element $\mathbf{a} \bmod m'$ of $\mathbf{Z}_{m'}^n$.

As $x + y = x - y \bmod 2$, note that T-sequences are Ducci sequences when $m = 2$. Several known results can then be generalized.

To simplify notation, the components of a tuple $\mathbf{a} \in \mathbf{Z}_m^n$ are indexed from 0 to $n-1$. We sometimes write $[\mathbf{a}]_i$ for $\mathbf{a}_i$. Note that addition and subtraction of the indices will always be performed modulo n. Thus, $\mathbf{a}_i$ should be understood as $\mathbf{a}_{(i \bmod n)}$.

Since $\mathbf{Z}_m^n$ is finite, a T-sequence must be eventually periodic. The goal of this paper is to study the period as a function of m and n, which we denote by $P(m,n)$. We shall detail what we mean by the length of the period.

Definition 1.3. Given m, n and $\mathbf{a} \in \mathbf{Z}_m^n$, a positive integer P is the *cycle length* of the T-sequence $\left(T^k\mathbf{a}\right)_{k\geq 0}$ if the following conditions hold:

(1) There exists a positive integer N such that $T^{k+P}\mathbf{a} = T^k\mathbf{a}$ for all $k \geq N$.
(2) Every positive integer satisfying (1) is a multiple of P.

The smallest such N is called the *pre-period*. If N is the pre-period, then the finite sequences $\left(\mathbf{a}, T\mathbf{a},\ldots,T^{N-1}\mathbf{a}\right)$ and $\left(T^N\mathbf{a},\ldots,T^{N+P-1}\mathbf{a}\right)$ are called *pre-cycle* and *cycle*, respectively.

In other words, the cycle length of the T-sequence $\left(T^k\mathbf{a}\right)_{k\geq 0}$ is the smallest positive integer P such that there exists some $N \in \mathbf{N}$ satisfying $T^{k+P}\mathbf{a} = T^k\mathbf{a}$ for all $k \geq N$.

We define $\mathscr{C}_m^n$ as the subset of $\mathbf{Z}_m^n$ of all tuples that belong to a cycle. It directly follows from remark 1.2 that $\mathscr{C}_m^n \subset \mathscr{C}_d^n$ whenever d divides m.

To simplify notation, cyclic permutations of a cycle are also called *cycles* and thus we rather refer to *a* cycle than *the* cycle.

In section 6, we give a characterization of $\mathscr{C}_m^n$ for some m and n.

Definition 1.4. Given m and n in $\mathbf{N}$, we define

$$P(m,n) = \max\left\{P \in \mathbf{N} : P \text{ is the cycle length of some T-sequence in } \mathbf{Z}_m^n\right\}.$$

It is called the *period* of T-sequences in $\mathbf{Z}_m^n$. This defines a function $P : \mathbf{N}\times\mathbf{N} \to \mathbf{N}$ called the *period function*.

As Ehrlich pointed out in [5], studying the cycle length of basic T-sequences suffices to determine the period of T-sequences. Actually, Ehrlich proved this result for Ducci sequences but the proof is essentially the same for T-sequences.

Proposition 1.5. *For all $m,n \in \mathbf{N}$, the cycle length of the basic T-sequence of $\mathbf{Z}_m^n$ equals $P(m,n)$. Cycle lengths of other T-sequences in $\mathbf{Z}_m^n$ divide $P(m,n)$.*

In section 2 we give basic results that are useful to study more interesting properties of T-sequences. Among those we prove a generalization of the known fact that Ducci sequences of 2^n-tuples eventually vanish.

In sections 4 to 5 we give important theorems about the multiplicity of the period function, which are summed up in the following theorem. It is the main result of this paper.

Theorem 1.6. *Let $m,n \in \mathbf{N}$ with $m = p_1^{k_1} \dots p_r^{k_r}$ the prime factorization of m. If $p_1,\dots,p_r$ are odd and non-Wieferich*[1]*, then*

$$P(m,n) = \operatorname{lcm}\left(p_1^{k_1-1}P(p_1,n),\dots,p_r^{k_r-1}P(p_r,n)\right).$$

2. Basic results

The first result below allows us to compute iterations of T in a very simple way. It will be used without moderation in the rest of this paper.

Proposition 2.1. *Let $\boldsymbol{a} \in \mathbf{Z}_m^n$, with $m,n \in \mathbf{N}$. For all $k \in \mathbf{N}$ and i such that $0 \le i < n$,*

$$[T^k \boldsymbol{a}]_i \equiv \sum_{j=0}^{k} \binom{k}{j} \boldsymbol{a}_{i+j} \bmod m.$$

Proof. We prove this by induction on k. For $k=0$, the result is obvious. Suppose it holds for k, hence we show that it holds for $k+1$, by using Pascal's triangle formula and manipulating the sums as follows,

$$\begin{aligned}
[T^{k+1}\mathbf{a}]_i \equiv [T^k\mathbf{a}]_i + [T^k\mathbf{a}]_{i+1} &\equiv \sum_{j=0}^{k}\binom{k}{j}\mathbf{a}_{i+j} + \sum_{j=0}^{k}\binom{k}{j}\mathbf{a}_{i+j+1} \\
&\equiv \binom{k}{0}\mathbf{a}_i + \sum_{j=1}^{k}\left(\binom{k}{j}+\binom{k}{j-1}\right)\mathbf{a}_{i+j} + \binom{k}{k}\mathbf{a}_{i+k+1} \\
&\equiv \sum_{j=0}^{k+1}\binom{k}{j}\mathbf{a}_{i+j} \bmod m,
\end{aligned}$$

which completes the proof. □

Definition 2.2. We say that a T-sequence $(T^k\mathbf{a})_{k\ge 0}$, where $\mathbf{a} \in \mathbf{Z}_m^n$, *vanishes* if there exists a positive integer k such that $T^k\mathbf{a} = 0 \bmod m$.

Recall that T-sequences are Ducci sequences if $m=2$, thus it is well known that every T-sequence of $\mathbf{Z}_2^n$ vanishes if and only if n is a power of 2. It has first been proven by Ciamberlini and Marengoni in [4], and it has been reproven many times since then [2, 5]. Actually, this result still holds when m is any power of 2. This has been proven by Wong in [14]. We give here a shorter proof using the notations we introduced and proposition 2.1. In [1], C. Avart shows a converse to this theorem for

[1] See definition 4.4.

the base case $n = 2$, stating that the only tuples that vanish are the tuples obtained by concatenation of several copies of a tuple of length a power of 2.

Theorem 2.3. *If n and l are positive integers, then every T-sequence of $\mathbf{Z}_{2^n}^{2^l}$ vanishes, that is, $P(2^n, 2^l) = 1$. Reciprocally, if every T-sequence of $\mathbf{Z}_m^n$ vanishes, then m is a power of 2.*

Proof. We first prove the case $n = 1$. Let $\mathbf{a} \in \mathbf{Z}_2^{2^l}$. Since $\binom{2^l}{j}$ is even for $0 < j < 2^l$ and by proposition 2.1, we have

$$\left[T^{2^l}\mathbf{a}\right]_i = \sum_{j=0}^{2^l} \binom{2^l}{j} \mathbf{a}_{i+j} = 2\mathbf{a}_i = 0 \bmod 2$$

for all i between 0 and $n-1$.

We now proceed with a proof by induction. Assume the result holds for some integer n, we prove that it still holds for $n+1$. Let $\mathbf{a} \in \mathbf{Z}_{2^{n+1}}^{2^l}$. If considered over $\mathbf{Z}_{2^n}^{2^l}$, the T-sequence generated by $\mathbf{a}$ vanishes. Let k be an integer such that $T^k\mathbf{a} = \mathbf{0} \bmod 2^n$. Therefore $T^k\mathbf{a} = 2^n\mathbf{u} \bmod 2^{n+1}$ for some tuple $\mathbf{u}$, which we can assume to consist only of 0 and 1's. It follows from the base case and by linearity of T that there exists some integer k' such that $T^{k+k'}\mathbf{a} = 2^n T^{k'}\mathbf{u} = \mathbf{0} \bmod 2^{n+1}$, which conclude the proof.

The reciprocal follows from the remark below definition 4.2. □

We denote by H the *left-shift* map [5], defined as

$$H : \mathbf{Z}_m^n \to \mathbf{Z}_m^n : (a_0, a_1, \ldots, a_{n-1}) \mapsto (a_1, a_2, \ldots, a_0).$$

Thus $T = I + H$ where I is the identity map. We have the following lemma (it is a generalization of lemma 1 in [5]), whose proof is a direct application of proposition 2.1 and of the fact that a prime p divides $\binom{p^k}{j}$ for $0 < j < p^k$.

The next proposition is a generalization of Corollary 3 and Theorem 2 in [5].

Lemma 2.4. *If p is a prime and k is a positive integer, then $T^{p^k} = I + H^{p^k} \bmod p$.*

Proposition 2.5. *Let p be a prime and n, K positive integers.*

(1) *If $p^K \equiv 1 \bmod n$, then $P(p,n)$ divides $p^K - 1$.*
(2) *If $p^K \equiv -1 \bmod n$, then $P(p,n)$ divides $n(p^K - 1)$.*

Proof. The proof is a simple application of lemma 2.4:

(1) $T^{p^K} = I + H^{p^K} = I + H = T$.
(2) $T^{p^K} = I + H^{p^K} = I + H^{-1} = H^{-1}T$, hence $T^{np^K} = H^{-n}T^n = T^n$.

□

If p and n are coprime, then $K = O_p(n)$, the order of p in $\mathbf{Z}_n$, always satisfies (1).

3. Multiplicity of the period function

In the following sections, we focus on the main question of this paper: can we deduce $P(m,n)$ from the prime factorization of $m = p_1^{e_1} \ldots p_r^{e_r}$, knowing $P(p_i, n)$ for $i = 1, \ldots, r$?

The next proposition suggests that we can. Due to its simplicity, we will often use it without reference.

Proposition 3.1. *If $d \mid m$, then $P(d,n) \mid P(m,n)$ for all $n \in \mathbf{N}$.*

Proof. Let $r \in \mathbf{N}$ be large enough for having $\mathbf{a} = T^r\mathbf{e} \in \mathscr{C}_m^n \subset \mathscr{C}_d^n$. The congruence $T^{P(m,n)}\mathbf{a} \equiv \mathbf{a} \bmod m$ still holds modulo d since $d \mid m$. We use (2) of definition 1.3 to conclude. □

The goal of the next few sections is to study this relation more precisely.

Theorem 3.2. *If $p_1, \dots, p_r$ are pairwise coprime, then*

$$P(m,n) = \operatorname{lcm}(P(p_1,n), \dots, P(p_r,n))$$

where $m = \prod_{i=1}^r p_i$.

Proof. We prove this for two coprime integers, the generalization for r pairwise coprime integers follows easily by induction. By proposition 1.5, we only need to consider the basic T-sequence.

Let p, q be two coprime integers. We assume here that k is large enough for $T^k\mathbf{e}$ to be in the different cycles. By definition 1.3, we have

$$\begin{cases} T^{k+L}\mathbf{e} \equiv T^k\mathbf{e} \bmod p \\ T^{k+L}\mathbf{e} \equiv T^k\mathbf{e} \bmod q \end{cases},$$

where $L = \operatorname{lcm}(P(p,n), P(q,n))$. Since p and q are coprime, it directly follows[2] that $T^{k+L}\mathbf{e} = T^k\mathbf{e} \bmod pq$, hence L is a multiple of the period $P(pq,n)$.

We now show that L satisfies (2) from definition 1.3. Suppose Q is such that $T^{k+Q}\mathbf{e} \equiv T^k\mathbf{e} \bmod pq$. In particular, $T^{k+Q}\mathbf{e} \equiv T^k\mathbf{e} \bmod p$, hence Q is a multiple of $P(p,n)$. Similarly, Q is a multiple of $P(q,n)$. Therefore, by definition of the least common multiple, $L \leq Q$, and $L = P(pq,n)$. □

With this theorem in our toolbox, we can restrict our attention to the periods modulo powers of primes. The question one may ask is whether we can deduce $P(p^k,n)$ from $P(p,n)$. We will shortly that it is (almost) the case.

4. Order of 2 and Wieferich primes

Definition 4.1. For a tuple $\mathbf{a} \in \mathbf{Z}_m^n$, we write $|\mathbf{a}|$ the *sum of components* of $\mathbf{a}$ modulo m.

Definition 4.2. For $m > 2$ odd, we write $O(m)$ the order of 2 in $\mathbf{Z}_m$, that is, the smallest integer k such that $2^k \equiv 1 \bmod m$. Its existence follow from Euler's theorem.

Let k be a positive integer and $\mathbf{a}$ be a tuple of $\mathbf{Z}_m^n$. By linearity, we have $\left|T^k\mathbf{a}\right| \equiv 2^k|\mathbf{a}| \bmod m$. If P is the cycle length of the T-sequence generated by $\mathbf{a}$ and k is greater than the pre-period, then we must have $\left|T^{k+P}\mathbf{a}\right| \equiv 2^P\left|T^k\mathbf{a}\right| \bmod m$, hence $2^P \equiv 1 \bmod m$ or $\left|T^k\mathbf{a}\right| \equiv 0 \bmod m$. Note that if m is not a power of 2, then $\left|T^k\mathbf{e}\right|$ is nonzero for all k, hence $2^{P(m,n)}$ must equal $1 \bmod m$. This implies the following proposition.

Proposition 4.3. *If $m > 2$ is odd, then $O(m)$ divides $P(m,n)$.*

Definition 4.4. A prime p is a *Wieferich prime* if $2^{p-1} \equiv 1 \bmod p^2$.

[2]If $a = b \bmod p$ and $a = b \bmod q$, then $a - b = kp = lq$ for some integers k, l. Hence q divides kp, so q divides k by Euclid's lemma and we get $a - b = k'pq$ for some integer k'.

Wieferich primes surprisingly pop out in several number theoretical subjects [9]. It is believed that there are infinitely many such numbers. What is extraordinary about these is that we only know two of them, 1093 and 3511, and there are no other Wieferich primes below 10^{17} [13]. Proposition 4.3 suggests that Wieferich primes shall be of considerable interest here.

We can characterize Wieferich primes by the order of 2 modulo p^2.

Lemma 4.5. *A prime $p > 2$ is a Wieferich prime if and only if $O(p) = O(p^2)$.*

Proof. We first show that $O(p^2)$ equals either $O(p)$ or $pO(p)$. By definition, $2^{O(p^2)} = 1 \bmod p^2$. It also holds modulo p, so $O(p^2)$ is a multiple of $O(p)$. For all positive integer k,

$$2^{pO(p)} - 1 \equiv \left(2^{O(p)} - 1\right)\left(2^{(p-1)O(p)} + 2^{(p-2)O(p)} + \cdots + 2^{O(p)} + 1\right) \equiv 0 \bmod p^2,$$

so $O(p^2)$ divides $pO(p)$, thus we can conclude.

Suppose that p is a Wieferich prime, that is, $2^{p-1} \equiv 1 \bmod p^2$. Then $O(p^2)$ divides $p-1$, so we cannot have $O(p^2) = pO(p)$. The proof of the other direction is direct. Indeed, $O(p^2) = O(p)$ divides $p-1$, so $2^{p-1} \equiv 1 \bmod p^2$. □

Actually, the first part of the previous proof also holds for all prime $p > 2$ and positive integer k, that is, $O(p^{k+1})$ is either $O(p^k)$ or $pO(p^k)$. In fact, as soon as it is the latter for one k, it is the latter for all subsequent k.

Proposition 4.6. *If $p > 2$ is a prime and $k \in \mathbf{N}$, then we have:*

1. *$O(p^{k+1})$ is either $O(p^k)$ or $pO(p^k)$.*
2. *If $O(p^{k+1}) = pO(p^k)$, then $O(p^{k+2}) = pO(p^{k+1})$.*
3. *If p is a non-Wieferich prime, then $O(p^k) = p^{k-1}O(p)$.*

Proof. The proof of (1) is similar to the one given above and (3) follows from (1) and (2) by induction. We show (2):

Suppose $O(p^{k+1}) = pO(p^k)$. Then $2^{O(p^k)} \equiv 1 + lp^k \bmod p^{k+1}$ where $l \not\equiv 0 \bmod p$, hence $2^{O(p^k)} \equiv 1 + lp^k + l'p^{k+1} \equiv 1 + p^k(l + l'p) \bmod p^{k+2}$ for some l'. By the binomial theorem and the fact that p divides $\binom{p}{j}$ for $0 < j < p$, we have $2^{pO(p^k)} \equiv 1 + p^{k+1}(l + l'p) \equiv 1 + lp^{k+1} \bmod p^{k+2}$. Since $l \not\equiv 0 \bmod p$, the proof is complete. □

For the known Wieferich primes, we have $O(p^3) = pO(p^2)$, hence by (3) of the previous proposition, it follows that $O(p^k) = p^{k-2}O(p)$ for all $k \geq 2$.

5. Period modulo powers of primes

Propositions 4.3 and 4.6 suggest a similar induction relation for the period function.

Theorem 5.1. *If p is a prime and $k, n \in \mathbf{N}$, then we have:*

1. *$P(p^{k+1}, n)$ is either $P(p^k, n)$ or $pP(p^k, n)$.*
2. *If $k \geq 2$ and $P(p^{k+1}, n) = pP(p^k, n)$, then $P(p^{k+2}, n) = pP(p^{k+1}, n)$.*
3. *If $P(p^{N+1}, n) = pP(p^N, n)$ for some $N \geq 2$, then $P(p^{N+k}, n) = p^kP(p^N, n)$ for all $k \in \mathbf{N}$.*

Proof. In (1) and (2), we choose r sufficiently large for $\mathbf{a} = T^r\mathbf{e}$ to be in a cycle of $\mathbf{Z}^n_{p^{k+1}}$ and $\mathbf{Z}^n_{p^{k+2}}$, respectively.

(1). Let $L = P(p^k, n)$. Since $\mathbf{a}$ is in a cycle modulo p^{k+1}, it is also in a cycle modulo p^k and $T^{P(p^{k+1},n)}\mathbf{a} \equiv \mathbf{a} \bmod p^k$. Hence L divides $P(p^{k+1}, n)$.

We have $T^L\mathbf{a} \equiv \mathbf{a} \bmod p^k$, so $T^L\mathbf{a} = \mathbf{a} + p^k\mathbf{u}$ for some tuple $\mathbf{u}$, that we can consider to be in $\mathbf{Z}_p^n$. By linearity of T, the tuple $p^k\mathbf{u} = T^L\mathbf{a} - \mathbf{a}$ is in a cycle modulo p^{k+1}. It implies that $\mathbf{u}$ is in a cycle in $\mathbf{Z}_p^n$, hence $T^L\mathbf{u} = \mathbf{u} + p\mathbf{v}$ for some tuple $\mathbf{v}$. Then, by linearity,

$$T^{2L}\mathbf{a} \equiv T^L\mathbf{a} + p^kT^L\mathbf{u} \equiv \mathbf{a} + p^k\mathbf{u} + p^k(\mathbf{u} + p\mathbf{v}) \equiv \mathbf{a} + 2p^k\mathbf{u} \bmod p^{k+1}.$$

By iterating T^L on $\mathbf{a}$, we then obtain $T^{pL}\mathbf{a} \equiv \mathbf{a} + pp^k\mathbf{u} \equiv \mathbf{a} \bmod p^{k+1}$. Hence $P(p^{k+1}, n)$ divides pL.

Therefore, $P(p^{k+1}, n)$ is either L or pL.

(2). Let $L = P(p^k, n)$, $L_1 = P(p^{k+1}, n)$ and $L_2 = P(p^{k+2}, n)$. Suppose $L_1 = pL$. By (1), we know that L_2 is either L_1 or pL_1. We show that it equals the latter.

Since $\mathbf{a}$ is in a cycle modulo p^{k+2}, it is also in a cycle modulo p^{k+1} and p^k. Then $T^L\mathbf{a} \equiv \mathbf{a} \bmod p^k$, but this congruence does not hold $\bmod p^{p+1}$, for we assumed that $L_1 = pL$. This implies that $T^L\mathbf{a} = \mathbf{a} + p^k\mathbf{u}$ where $\mathbf{u} \not\equiv 0 \bmod p$.

By linearity of T, the tuple $p^k\mathbf{u} = T^L\mathbf{a} - \mathbf{a}$ is in a cycle modulo p^{k+2}, hence $\mathbf{u}$ is in a cycle modulo p^2. The condition $k \geq 2$ implies that $P(p^2, n)$ divides $L = P(p^k, n)$. We then have, by the same argument as in (1),

$$T^{L_1}\mathbf{a} \equiv T^{pL}\mathbf{a} \equiv \mathbf{a} + p^{k+1}\mathbf{u} \not\equiv \mathbf{a} \bmod p^{k+2}.$$

Therefore, $L_2 \neq L_1$, so $L_2 = pL_1$.

(3). This follows directly from (1) and (2) by induction. □

The following proposition exhibits the fact that the condition $k \geq 2$ is needed for (2) to hold.

Proposition 5.2. *We have $P(2,3) = 3$ and $P(2^k, 3) = 6$ for all positive integer $k > 1$.*

Proof. By theorem 1.5, it suffices to compute the first iterations of the basic T-sequence to get $P(2,3) = 3$.

We prove that $P(2^k, 3) = 6$ for all positive integer $k > 1$ by induction. For the base case, we simply proceed as above. The cycle of the basic T-sequence is

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

Suppose that the basic T-sequence of $\mathbf{Z}_{2^k}^3$ has a cycle of the form

$$\big((a,a,b),(d,c,c),(a,b,a),(c,c,d),(b,a,a),(c,d,c)\big)$$

where $a,b,c,d \in \mathbf{Z}_{2^k}$, with $a,b \leq 2^{k-1}$ and $c,d \geq 2^{k-1}$. Then we show that the basic T-sequence of $\mathbf{Z}_{2^{k+1}}^3$ has a cycle of form

$$\big((d,c,c),(a',b',a'),(c,c,d),(b',a',a'),(c,d,c),(a',a',b')\big)$$

where $a',b' \in \mathbf{Z}_{2^{k+1}}$ and $a,b \geq 2^k$. Indeed, $(d,c,c) = 2^{k-1}(1,1,1)+(d',c',c')$ with $c',d' \leq 2^{k-1}$, hence $T(d,c,c) = 2^k(1,1,1) + (a,b,a) \bmod 2^{k+1}$ by linearity. Thus $T^2(d,c,c) = (c,c,d)$ and we can apply the exact same argument two more times.

Since the cycle of the basic T-sequence of $\mathbf{Z}_4^3$ is of that form and the above argument also works for cyclic permutations of these sequences, the proof is complete. □

We now try to show that $P(p^2,n) = pP(p,n)$ for any non-Wieferich prime $p > 2$. Theorem 5.1 will permit us to conclude.

Proposition 5.3. *Let $p > 2$ be a non-Wieferich prime and $n \in \mathbf{N}$. If n is not a multiple of p, then $P(p^2,n) = pP(p,n)$ and $P(p^3,n) = p^2P(p,n)$.*

Proof. By theorem 5.1, we know that $P(p^2,n)$ is either $P(p,n)$ or $pP(p,n)$. Given p and n are coprime, Proposition 2.5 tells us that $P(p,n)$ divides $p^{O_p(n)} - 1$, so it cannot be a multiple of p. However, by proposition 4.3, $P(p^2,n)$ is a multiple of $O(p^2)$, which equals $pO(p)$ for p is non-Wieferich (proposition 4.6). Therefore, since p divides $P(p^2,n)$, we must have $P(p^2,n) = pP(p,n)$.

The proof that $P(p^3,n) = p^2P(p,n)$ is very similar. □

Corollary 5.4. *If $p > 2$ is a non-Wieferich prime and n is not a multiple of p, then $P(p^k,n) = p^{k-1}P(p,n)$ for all $k \in \mathbf{N}$.*

To generalize proposition 5.3 for any $n \in \mathbf{N}$, we first need to prove a few lemmas.

The *p-adic valuation* of an integer n is the largest power of p that divides n. It is denoted by $v_p(n)$. We write $s_p(n)$ the sum of the digits of n when written in base p. If p is a prime, *Legendre's formula* [11] states that

$$v_p(n!) = \frac{n - s_p(n)}{p-1}.$$

Note that $v_p(ab) = v_p(a) + v_p(b)$ and $v_p(a/b) = v_p(a) - v_p(b)$ for all integers a, b.

Lemma 5.5. *Let p be a prime and $k, s \in \mathbf{N}$ with $0 \le s \le k$. We have*

$$\left\{ j \in \left\{0,\dots,p^k\right\} : p^s \nmid \binom{p^k}{j} \right\} = \left\{ mp^{k-s+1} : 0 \le m \le p \right\}.$$

Proof. It is clear that 0 and p^k belong to both sets. Let $0 < n < p^k$ and $\sum_{i=0}^{k-1} n_i p^i$ its decomposition in base p. We first show that $v_p\left(\binom{p^k}{n}\right) = k - r$ where $r = \min\{i : n_i \neq 0\}$. Since $0 < n < p^k$, we have $0 < r < k$

By Legendre's formula, we have $v_p(p^k!) = \frac{p^k-1}{p-1}$ and $v_p(n) = \frac{n-s_p(n)}{p-1}$ where $s_p(n) = \sum_i n_i$. We also have

$$p^k - n = 1 + \sum_{i=0}^{k-1} (p-1-n_i)p^i = (p-n_r)p^r + \sum_{i=r+1}^{k-1} (p-1-n_i)p^i.$$

Thus,

$$v_p((p^k-n)!) = \frac{p^k - n - \sum_{i=r+1}^{k-1}(p_i - 1 - n_i) - (p-n_r)}{p-1},$$

and

$$\begin{aligned}
v_p(n!(p^k-n)!) = v_p(n!) + v_p((p^k-n)!) &= \frac{1}{p-1}\left(p^k - \sum_{i=r+1}^{k-1}(p-1) - p\right) \\
&= \frac{p^k - (k-r-1)(p-1) - p}{p-1} = \frac{p^k - 1 - k(p-1) + r(p-1)}{p-1} \\
&= \frac{p^k-1}{p-1} + r - k.
\end{aligned}$$

Therefore, we obtain $v_p\left(\binom{p^k}{n}\right) = k - r$, hence an integer $0 < n < p^k$ belongs to the first set if and only if $k - r < s$, i.e., $s \geq k - 1 + 1$, which happens if and only if n is a multiple of p^{k-s+1}. This concludes the proof. □

The proof of the following lemma is due to Darij Grinberg and Victor Reiner ((12.69.3) in [8]).

Lemma 5.6. *Let $n \in \mathbf{N}$ and p be a prime factor of n. For all $q \in \mathbf{N}$ and $r \in \mathbf{Q}$ such that rn is an integer, we have*

$$\binom{qn}{rn} \equiv \binom{qn/p}{rn/p} \bmod p^{v_p(n)}.$$

Proof. The argument consists in counting the (rn)-elements subsets of the set $\mathbf{Z}_{qn}$. It is clearly $\binom{qn}{rn}$.

At the same time, the subsets fall into two classes:

(1) The subsets which are invariant under the permutation $i \mapsto i + qn/p$ of $\mathbf{Z}_{qn}$.
(2) The other ones.

Say there are N_1 and N_2 subsets in the first and second class, respectively.

If a (rn)-elements subset S belongs to the first class, then the intersection $S \cap \{0, 1, \ldots, qn/p - 1\}$ must have rn/p elements, which uniquely determine all of S by iterating the permutation given above. Thus the first class contains $N_1 = \binom{qn/p}{rn/p}$ elements.

Besides, the permutation $\phi : i \mapsto i + qn/p^{v_p(n)}$ of $\mathbf{Z}_{qn}$ acts on the subsets of the second class, splitting them into orbits. Since $\phi^{v_p(n)}$ acts trivially, the size of each orbit divides $p^{v_p(n)}$. Suppose that the size $|\mathcal{O}|$ of an orbit $\mathcal{O}$ is a proper divisor of $p^{v_p(n)}$. Then $p^{v_p(n)-1}$ divides $|\mathcal{O}|$, so $\phi^{p^{v_p(n)-1}}$ acts trivially on $\mathcal{O}$, hence elements of this orbit are subsets of the first class, which is a contradiction. Then every orbit has size $p^{v_p(n)}$.

Since the set of all second class subsets is the union of these orbit, it has size N_2 divisible by $p^{v_p(n)}$.

Therefore, we have $\binom{qn}{rn} = N_1 + N_2 \equiv \binom{qn/p}{rn/p} \bmod p^{v_p(n)}$ and the proof is complete. □

To prove the following lemma, we shall introduce *Babbage's theorem* (theorem 1.12 in [7]). It states that for any prime p and integers $a, b \geq 0$, we have $\binom{ap}{bp} \equiv \binom{a}{b} \bmod p^2$. Note that if $p \geq 5$, we can replace $\bmod p^2$ by $\bmod p^3$, thus reinforcing the result. This case is known as *Wolstenholme's theorem*.

Lemma 5.7. *If p is a prime, $k \geq 1$ and $0 \leq m \leq p$, then*

$$\binom{p^k}{mp^{k-1}} \equiv \binom{p}{m} \bmod p^2$$

Proof. It follows directly from Babbage's theorem by induction, or from lemma 5.6. □

Lemma 5.8. *If p is a prime, $k \geq 2$ and $0 \leq m \leq p^2$, then*

$$\binom{p^k}{mp^{k-2}} \equiv \binom{p^2}{m} \bmod p^3$$

Proof. For $p \geq 5$, the proof follows from Wolstenholme's theorem by induction.
For $p = 2$ and $p = 3$, it follows from lemma 5.6. □

Proposition 5.9. *Let p be a prime and $n \in \mathbf{N}$ with $n = p^k n'$, where $k = v_p(n)$. Then we have*

(1) $P(p,n) = p^k P(p,n')$. *If $p = 2$, it holds only if $n' \neq 0$*
(2) *If $p > 2$ is a non-Wieferich prime, then $P(p^2,n) = p^k P(p^2,n')$.*
(3) *If $p > 2$ is a non-Wieferich prime, then $P(p^3,n) = p^k P(p^3,n')$.*

Proof. The idea of this proof is to study the behavior of a T-sequence $(T^i\mathbf{a})_{i\in\mathbf{N}}$ of $\mathbf{Z}_m^n$ (where $m = p, p^2, p^3$, respectively) by studying the behavior of the T-sequence generated by a *subtuple* of $\mathbf{a}$, which is a T-sequence of smaller tuples that we better understand.

For that purpose, we introduce a family of functions S_r, $0 \leq r \leq k$, that extract an interesting subtuple from a given tuple. For $0 \leq r \leq k$, let

$$S_r : \mathbf{Z}_m^n \to \mathbf{Z}_m^{p^r n'} : (a_0, \dots, a_{n-1}) \mapsto (a_0, a_{p^{k-r}}, a_{2p^{k-r}}, \dots, a_{(p^r n'-1)p^{k-r}}).$$

(1). Here we use S_0. For $\mathbf{a} \in \mathbf{Z}_p^n$, the subtuple $S_0(\mathbf{a})$ is in $\mathbf{Z}_p^{n'}$.

By Lemma 2.4, we have $T^{p^k} \equiv I + H^{p^k} \bmod p$, hence $S_0(T^{p^k}\mathbf{a}) \equiv TS_0(\mathbf{a}) \bmod p$ for any tuple $\mathbf{a} \in \mathbf{Z}_p^n$. Considering the basic tuple $\mathbf{e}$ of $\mathbf{Z}_p^n$, it gives $S_0(\mathbf{e}) = \mathbf{e'}$ where $\mathbf{e'}$ is the basic tuple of $\mathbf{Z}_p^{n'}$. Note that components of $\mathbf{e}$ that are not components of $\mathbf{e'}$ remain zero after any number of iterations of T^{p^k}, hence the behavior of the T-sequence $(T^{rp^k}\mathbf{e})_{r\geq 0}$ is entirely determined by the behavior of $(T^r\mathbf{e'})_{r\geq 0}$. The cycle length of the latter being $P(p,n')$, the cycle length of the former is $p^k P(p,n')$.

If $p = 2$, note that this argument only holds if the T-sequences do not vanish. This explains the additional condition $n' \neq 0$ in this case.

If $p = 2$, this argument only holds if the T-sequences do not vanish. This explains the additional condition in this case.

(2). Here we suppose $p > 2$ is a non-Wieferich prime. We first show that $P(p^2, pn') = pP(p^2,n')$ and then that $P(p^2,n) = p^{k-1}P(p^2,pn')$.

To prove the first part, we use $S_0 : \mathbf{Z}_{p^2}^{pn'} \to \mathbf{Z}_{p^2}^{n'}$. By lemmas 5.5 and 5.7, we have

$$[T^{p^2}\mathbf{a}]_i \equiv \sum_{j=0}^{p^2} \binom{p^2}{j} \mathbf{a}_{i+j} \equiv \sum_{j=0}^{p} \binom{p^2}{jp} \mathbf{a}_{i+jp} \equiv \sum_{j=0}^{p} \binom{p}{j} \mathbf{a}_{i+jp} \bmod p^2,$$

which implies that $S_0(T^{p^2}\mathbf{a}) \equiv T^p S_0(\mathbf{a}) \bmod p^2$. Since p is a non-Wieferich prime, p divides $P(p^2,n')$. Thus we obtain $P(p^2,pn') = p^2 p^{-1} P(p^2,n') = pP(p^2,n')$.

We now use S_1. For $\mathbf{a} \in \mathbf{Z}_p^n$, the subtuple $S_1(\mathbf{a})$ is in $\mathbf{Z}_{p^2}^{pn'}$. We also have

$$[T^{p^k}\mathbf{a}]_i \equiv \sum_{j=0}^{p^k} \binom{p^k}{j} \mathbf{a}_{i+j} \equiv \sum_{j=0}^{p} \binom{p^k}{jp^{k-1}} \mathbf{a}_{i+jp^{k-1}} \equiv \sum_{j=0}^{p} \binom{p}{j} \mathbf{a}_{i+jp^{k-1}} \bmod p^2,$$

where the second and third equalities follow from lemmas 5.5 and 5.7, respectively. Thus, $S_1(T^{p^k}\mathbf{a}) \equiv T^p S_1(\mathbf{a}) \bmod p^2$. Therefore we obtain $P(p^2,n) = p^k p^{-1} P(p^2,pn') = p^{k-1}P(p^2,pn') = p^k P(p^2,n')$ as expected, where the last equality follows from the first part.

(3). Suppose $p > 2$ is a non-Wieferich prime. The proof of this case is quite similar to the proof of (2). We first show that $P(p^3, p^2n') = p^2P(p^3, n')$ and then that $P(p^3, n) = p^{k-2}P(p^3, p^2n')$. To begin with, we suppose $k > 1$. We prove the case $k = 1$ separately.

First, we use S_0 again. For $\mathbf{a} \in \mathbf{Z}_{p^3}^{p^2n'}$, the subtuple $S_2(\mathbf{a})$ is in $\mathbf{Z}_{p^3}^{n'}$., and

$$[T^{p^4}\mathbf{a}]_i \equiv \sum_{j=0}^{p^4} \binom{p^4}{j} \mathbf{a}_{i+j} \equiv \sum_{j=0}^{p^2} \binom{p^4}{jp^2} \mathbf{a}_{i+jp^2} \equiv \sum_{j=0}^{p^2} \binom{p^2}{j} \mathbf{a}_{i+jp^2} \bmod p^3,$$

hence $S_0(T^{p^4}\mathbf{a}) \equiv T^{p^2}S_0(\mathbf{a}) \bmod p^3$. By proposition 5.3 (it is why we consider $p > 2$), p^2 divides $P(p^3, n')$, thus we obtain $P(p^3, p^2n') = p^4p^{-2}P(p^3, n')$

Now we use S_2. For $\mathbf{a} \in \mathbf{Z}_p^n$, the subtuple $S_2(\mathbf{a})$ is in $\mathbf{Z}_p^{p^2n'}$. First, using lemma 5.5 and 5.8, we obtain

$$[T^{p^k}\mathbf{a}]_i \equiv \sum_{j=0}^{p^k} \binom{p^k}{j} \mathbf{a}_{i+j} \equiv \sum_{j=0}^{p^2} \binom{p^k}{jp^{k-2}} \mathbf{a}_{i+jp^{k-2}} \equiv \sum_{j=0}^{p^2} \binom{p^2}{j} \mathbf{a}_{i+jp^{k-2}} \bmod p^3,$$

hence $S_2(T^{p^k}\mathbf{a}) \equiv T^{p^2}S_2(\mathbf{a}) \bmod p^3$. Together with the first part, we get $P(p^3, n) = p^kp^{-2}P(p^3, p^2n') = p^kP(p^3, n')$ as expected.

To conclude the proof, we consider $k = 1$. We have to show that $P(p^3, pn') = pP(p^3, n')$. We use S_0. For $\mathbf{a} \in \mathbf{Z}_{p^3}^{pn'}$, the subtuple $S_0(\mathbf{a})$ is in $\mathbf{Z}_{p^3}^{n'}$. As above, using lemmas 5.5 and 5.8, we have $[T^{p^3}\mathbf{a}]_i \equiv \sum_{j=0}^{p^2} \binom{p^2}{j} \mathbf{a}_{i+jp} \bmod p^3$, hence $S_0(T^{p^3}\mathbf{a}) \equiv T^{p^2}S_0(\mathbf{a}) \bmod p^3$. By proposition 5.3, p^2 divides $P(p^3, n')$. Thus we obtain $P(p^3, pn') = p^3p^{-2}P(p^3, n') = pP(p^3, n')$, which conludes. □

Theorem 5.10. *If $p \geq 3$ is a non-Wieferich prime, we have $P(p^k, n) = p^{k-1}P(p, n)$ for all positive integers k and n.*

Proof. Let $k, n \in \mathbf{N}$. Write $n = p^sn'$ where $s = v_p(n)$. We show that (1) $P(p^2, n) = pP(p^2, n)$ and (2) $P(p^3, n) = p^2P(p, n)$.

(1). Points (1) and (2) of proposition 5.9 yield $P(p, n) = p^sP(p, n')$ and $P(p^2, n) = p^sP(p^2, n')$, respectively. Since p is non-Wieferich and coprime with n', we have $P(p^2, n') = pP(p, n')$ by proposition 5.3. The conclusion follows directly.

(2). The argument is the same, using (3) of proposition 5.9 instead of (2).

Therefore, we complete the proof by theorem 5.1. □

With theorems 3.2 and 5.10, we are now able to prove theorem 1.6.

At this point, a question one may ask is whether we can generalize this result for 2 and Wieferich primes. The proofs above are considerably dependant on proposition 5.3, which itself is dependant on proposition 4.6. Therefore, it would not be possible to use the same method to obtain similar results for these special primes.

However, F. Breuer shows in theorem 8.2 of [3] that a variant of theorem 5.10 holds for 2 and Wieferich primes, namely that $P(p^k, n) = p^{max(0,k-1-t)}P(p, n)$ for some integer t. That is, these special cases eventually behaves as we would expect. Whether it is possible or not to derive such results with an elementary method, similar to the ones used here, remains an open question.

6. Characterization of tuples in a cycle

In this section we try to characterize tuples of $\mathbf{Z}_m^n$ that belong to $\mathscr{C}_m^n$. By theorem 2.3, we already know that $\mathscr{C}_m^n = \{\mathbf{0}\}$ if m and n are powers of 2.

The linear map T is represented in the standard basis by the matrix

$$\begin{pmatrix} 1 & 1 & 0 & \dots & 0 \\ 0 & 1 & 1 & \dots & 0 \\ & \vdots & & \ddots & \vdots \\ 1 & 0 & 0 & \dots & 1 \end{pmatrix},$$

to which we identify T. Note that $\det(T) = 0$ when n is even and $\det(T) = 2$ when n is odd. This simple fact yields the following proposition.

Proposition 6.1. *Let $m > 2$ and $n > 0$ be two odd integers. Then $\mathscr{C}_m^n = \mathbf{Z}_m^n$.*

Proof. Since $\det(T) = 2$ is invertible[3] modulo m, the matrix T is invertible[4], hence T is bijective. Consequently, we can unambiguously move backward in the eventually periodic T-sequence determined by a tuple $\mathbf{a}$ of $\mathbf{Z}_m^n$, so $\mathbf{a}$ belongs to a cycle. □

For n even, things are a bit more complicated and require the introduction of a few new notations. We denote the alternating sum of components of a tuple $\mathbf{a} \in \mathbf{Z}_m^n$ by

$$\sigma(\mathbf{a}) = \sum_{i=0}^{n-1} (-1)^i a_i \bmod m.$$

Proposition 6.2. *Let $m > 2$ be odd and $n > 0$ be even. If n and m are coprime, then a tuple $\boldsymbol{a} \in \mathbf{Z}_m^n$ belongs to a cycle if and only if $\sigma(\boldsymbol{a}) = 0$.*

Proof. We first show that the condition is sufficient. Let $\mathbf{a} \in \mathbf{Z}_m^n$ be such that $\sigma(\mathbf{a}) \equiv 0 \bmod m$. Finding a preimage $\mathbf{x}$ of $\mathbf{a}$ is equivalent to solving the system

$$\begin{cases} x_0 + x_1 \equiv a_0, \\ x_1 + x_2 \equiv a_1, \\ \quad\vdots \\ x_{n-1} + x_0 \equiv a_{n-1}, \end{cases} \quad \text{which is equivalent to} \quad \begin{cases} x_1 \equiv a_0 - x_0, \\ x_2 \equiv a_1 - a_0 + x_0, \\ x_3 \equiv a_2 - a_1 + a_0 - x_0, \\ \quad\vdots \\ x_{n-1} \equiv a_{n-2} - a_{n-3} + \dots + a_0 - x_0, \\ x_0 \equiv a_{n-1} - a_{n-2} + \dots + a_1 - a_0 + x_0. \end{cases} \tag{1}$$

All components of $\mathbf{x}$ are determined by the value chosen for x_0 and the last equation is satisfied since $\sigma(\mathbf{a}) \equiv 0 \bmod m$. Thus, $\mathbf{a}$ has exactly m preimages. Moreover, n and m are coprime, so n is invertible, hence the equation $\sigma(\mathbf{x}) \equiv nx_0 - (n-1)a_0 + (n-2)a_1 - \dots + 2a_{n-3} - a_{n-2} \equiv 0 \bmod m$ has exactly one solution x_0. Thus, $\mathbf{a}$ has exactly one preimage $\mathbf{x}$ with $\sigma(\mathbf{x}) \equiv 0 \bmod m$.

Therefore, the map T restricted to the set $\{\mathbf{a} \in \mathbf{Z}_m^n : \sigma(\mathbf{a}) \equiv 0 \bmod m\}$ is a one-to-one correspondence and we can conclude as in proposition 6.1.

The last equation of system 1 shows that the condition is necessary. □

The following result, concerning $\mathbf{Z}_2^n$, is shown in [6] and in [12] for the Ducci map, which is the same as our map in this case since.

[3] An integer x is invertible modulo m if and only if x and m are coprime.

[4] A matrix is invertible if and only if its determinant is invertible.

Proposition 6.3. *In $\mathbf{Z}_2^n$, we have* $\operatorname{im}(T) = \{\boldsymbol{a} \in \mathbf{Z}_2^n : |\boldsymbol{a}| = 0\}$ *and every* $\boldsymbol{a} \in \operatorname{im}(T)$ *has exactly two preimages. For odd n, a tuple $\boldsymbol{a} \in \mathbf{Z}_2^n$ belongs to a cycle if and only if* $|\boldsymbol{a}| = 0$.

If n is even, the two preimages of a tuple $\mathbf{a} \in \operatorname{im}(T)$ are either both in $\operatorname{im}(T)$ or both in $\mathbf{Z}_2^n \setminus \operatorname{im}(T)$. Thus we have to find a way to characterize tuples of $\operatorname{im}(T)$ that have preimages in $\operatorname{im}(T)$.

That has actually already been done by Ludington-Young in [6, 10], where the following definition and theorem 6.4 come from. We only consider here tuples of $\mathbf{Z}_2^n$. A tuple $\mathbf{a}$ is *even* if $|\mathbf{a}| = 0$. Suppose $n = 2^r k$ where k is odd, we say a tuple $\mathbf{a} \in \mathbf{Z}_2^n$ is *r-even* if

$$\sum_{i=0}^{k-1} a_{2^r i+j} \equiv 0 \bmod 2$$

for $j = 0, \dots, 2^r - 1$. For example, if $n = 12$, then $\mathbf{a}$ is 2-even if

$$a_0 + a_4 + a_8 \equiv 0, \quad a_1 + a_5 + a_9 \equiv 0, \quad a_2 + a_6 + a_{10} \equiv 0 \quad \text{and} \quad a_3 + a_7 + a_{11} \equiv 0.$$

Theorem 6.4. *Let $n = 2^r k$ with k odd. A tuple of $\mathbf{Z}_2^n$ belongs to a cycle if and only if it is r-even.*

Proposition 6.3 turns out to be the special case $r = 0$ of this theorem. Indeed, a tuple $\mathbf{a}$ is 0-even if and only if $|\mathbf{a}| = 0$.

We now generalize this characterization to odd primes. We say a tuple $\mathbf{a}$ of $\mathbf{Z}_p^n$, where $n = p^r k$, is *even* if $\sigma(\mathbf{a}) = 0$. We note

$$\sigma_j(\mathbf{a}) \equiv \sum_{i=0}^{k-1} (-1)^i a_{p^r i+j} \bmod p$$

for $j = 0, \dots, p^r - 1$. We say $\mathbf{a}$ is *r-even* if $\sigma_j(\mathbf{a}) = 0$ for all j.

Theorem 6.5. *Let $p > 2$ be a prime and $n = p^r k$ even with $r = v_p(n)$ (i.e., $k \not\equiv 0 \bmod p$). A tuple of $\mathbf{Z}_p^n$ belongs to a cycle if and only if it is r-even.*

Proof. First, note that $T\mathbf{a}$ is r-even if $\mathbf{a}$ is r-even. Since lemma 2.4 implies that $T^{p^r}\mathbf{e} \equiv \mathbf{e} + H^{p^r}\mathbf{e}$ is r-even, every tuple of a cycle must be r-even by proposition 1.5, hence the condition is necessary. We now show that it is sufficient.

Let $\mathbf{a} \in \mathbf{Z}_p^n$ be r-even. By proposition 6.2, r-evenness implying evenness, the tuple $\mathbf{a}$ has p preimages. Let $\mathbf{b}^{(0)}$ be one of these, hence all preimages are given by $\mathbf{b}^{(l)} = \mathbf{b}^{(0)} + (l, -l, \dots, l, -l)$ for $l = 0, \dots, p-1$. To simplify notation, we write σ_j for $\sigma_j\left(\mathbf{b}^{(0)}\right)$.

Since $a_i \equiv b_i^{(0)} + b_{i+1}^{(0)}$,

$$0 \equiv \sigma_0(\mathbf{a}) \equiv \sum_{i=0}^{k-1} (-1)^i a_{p^r i} \equiv \sum_{i=0}^{k-1} (-1)^i \left(b_{p^r i}^{(0)} + b_{p^r i+1}^{(0)}\right) \equiv \sigma_0 + \sigma_1$$

and, similarly, $\sigma_1 + \sigma_2$, $\sigma_2 + \sigma_3, \dots, \sigma_{p^r-2} + \sigma_{p^r-1}$ all equal $0 \bmod p$ and $\sigma_{p^r-1} - \sigma_0$ too[5]. Hence,

$$\sigma_0 \equiv -\sigma_1 \equiv \sigma_2 \equiv -\sigma_3 \equiv \cdots \equiv -\sigma_{p^r-2} \equiv \sigma_{p^r-1}.$$

Since k is invertible modulo p, the equation $\sigma_0\left(\mathbf{b}^{(l)}\right) \equiv \sigma_0 + kl \equiv 0 \bmod p$ has exactly one solution $l \equiv -\sigma_0/k \bmod p$, hence $\mathbf{b}^{(l)}$ is the only r-even preimage of $\mathbf{a}$.

Therefore, the map T restricted to the set of r-even tuples of $\mathbf{Z}_p^n$ is bijective and the proof is complete. $\square$

[5]The negative sign comes from the equality $(-1)^i b_{p^r i+p^r-1+1}^{(0)} = (-1)^i b_{p^r(i+1)}^{(0)}$.

Corollary 6.6. *Let p be a prime and $n = p^r k$ even with $r = v_p(n)$. Assume $k > 1$ if $p = 2$. Otherwise assume k is even. Then* $\left|\mathscr{C}_p^n\right| = p^{n-p^r}$.

7. More properties

In this section we establish some explicit formulas for $P(p,n)$ where p is a prime.

Proposition 7.1. *If $m > 2$ is odd, then $P(m,1) = P(m,2) = O(m)$.*

Proof. It follows directly from the definition of $O(m)$. □

Proposition 7.2. *If $p > 2$ is a prime, then $P(p,2p) = P(p,p) = pO(p)$.*

Proof. By (1) of proposition 5.9, we have $P(p,2p) = pP(p,2)$ and $P(p,p) = P(p,1)$. We conclude with proposition 7.1. □

Proposition 7.3. *If $p > 2$ is prime, then $P(p,3) = \gcd(O(p),6)$.*

Proof. Let $p > 2$ be a prime and $\mathbf{e} = (1,0,0)$ the basic tuple of $\mathbf{Z}_p^3$. By proposition 6.1, $\mathbf{e}$ belongs to a cycle and by proposition 4.3, $P(p,3)$ is a multiple of $O(p)$. In order to prove this proposition, we first establish a few facts.
(1). If r is even, then $T^r\mathbf{e}$ is a circular permutation of a tuple $(k+1,k,k)$ with $k \in \mathbf{Z}_p$. If r is odd, then $T^r\mathbf{e}$ is a circular permutation of a tuple $(k+1,k+1,k)$ with $k \in \mathbf{Z}_p$. This fact is easily provable by induction on r. We call the component that does not repeat the *lone component*. The proofs of (2) and (3) follow easily from this fact.
(2). The only tuples that belong to the cycle of the basic T-sequence and have component sum 1 are circular permutations of $(1,0,0)$ or $(-3^{-1}+1,-3^{-1}+1,-3^{-1})$. If $p = 3$, then they are circular permutations of $(1,0,0)$.
(3). Each iteration of T moves the lone component one step to the right. Thus $P(p,3)$ is a multiple of 3.

Now come the conclusions. If $O(p)$ is even, then by (1) and (2), $T^{rO(p)}\mathbf{e}$ is a circular permutation of $(1,0,0)$ for all integer $r > 0$, hence we can conclude with (3). If $O(p)$ is odd, then $T^{rO(p)}$ is a circular permutation of $(1,0,0)$ only if r is even, and again we conclude with (3). □

Proposition 7.4. *If p is a prime, $k \geq 0$ and $n \geq 1$ ($n > 1$ in the case $p = 2$), then*

1. $P(p,p^k(p^n-1)) = p^k(p^n-1)$,
2. $P(p,p^k(p^n+1)) = p^k(p^{2n}-1)$.

Proof. By (1) proposition 5.9, we only need to show the case $k = 0$.
(1). It follows from lemma 2.4 that $T^{p^n} = I + H^{p^n} = T$, hence $p^n - 1$ is a multiple of the period. A direct application of proposition 2.1 shows that it is actually the period.
(2). As above, $T^{p^n} = I + H^{p^n} = H^{-1}T$. Thus, $T^{p^n-1}T = H^{-1}T$ and for all positive integer r,

$$T^{r(p^n-1)}T = H^{-r}T.$$

Since the least r such that $H^{-r} = I$ is $p^n + 1$, the proof is complete. □

8. Open questions

We can see the iterations of the map T on the set $\mathscr{C}_m^n$ (which is bijective when restricted to $\mathscr{C}_m^n$) as the action of the group $\{T^k : k \in \mathbf{Z}\}$ on this set, splitting it into orbits. What are the possible sizes for these orbits? The tuple $(0,\ldots,0)$ has an orbit of size 1, whereas the basic tuple, after enough iterations, generates an orbit of size $P(m,n)$. What are the values between 1 and $P(m,n)$ that are the size of some orbit?

Further questions arise naturally. What is the largest pre-period that can happen? How all the results of this paper could be generalized to any linear map of $\mathbf{Z}_m^n$? Do there exist explicit formulas to find $P(p,n)$ for every prime p and positive integer n?

References

[1] Christian Avart. "A characterization of converging Ducci sequences over Z2". In: *The Fibonacci Quarterly* 49 (May 2011).

[2] Florian Breuer. "Ducci sequences in higher dimensions". In: *INTEGERS: Electronic journal of combinatorial number theory* 7.24 (2007).

[3] Florian Breuer. "Ducci sequences and cyclotomic fields". In: *Journal of Difference Equations and Applications* 16.7 (July 2010), pp. 847–862.

[4] C. Ciamberlini and A. Marengoni. "Su una interessante curiosita‘ numerica". In: *Periodiche di Matematiche* 17 (1937), pp. 25–30.

[5] Amos Ehrlich. "Periods in Ducci's n-number game of differences". In: *The Fibonacci Quaterly* 28.4 (Nov. 1990), pp. 302–305.

[6] Anne Ludington Furno. "Cycles of Differences of Integers". In: *Journal of number theory* 13.2 (May 1981), pp. 255–261.

[7] Darij Grinberg. *The Lucas and Babbage congruences*. `http://www.cip.ifi.lmu.de/~grinberg`
Accessed: 2019-03-09. Jan. 2019.

[8] Darij Grinberg and Victor Reiner. *Hopf Algebras in Combinatorics*. `https://arxiv.org/abs/1`
Ancillary file. Sept. 2014.

[9] G.H. Hardy and E.M. Wright. *An Introduction to the Theory of Numbers*. 5th. Oxford University Press, 1979, p. 202.

[10] Anne L. Ludington-Young. "Even Ducci-sequences". In: *The Fibonacci Quarterly* 37 (May 1999).

[11] A. M. Legendre. *Théorie des nombres*. Paris: Firmin Didot frères, 1830.

[12] Michał Misiurewicz, John G. Stevens, and Diana M. Thomas. "Iterations of linear maps over finite fields". In: *Linear Algebra and its Application* 413.1 (Feb. 2006), pp. 218–234.

[13] N.J.A. Sloane. *The On-Line Encyclopedia of Integer Sequences, Sequence A001220*. published electronically at https://oeis.org. 2017.

[14] Fook-Bun Wong. "Ducci Processes". In: *The Fibonacci Quaterly* 20.2 (May 1982), pp. 97–105.

E-mail address: `bruno.dular@epfl.ch`