# CYCLES OF SUMS OF INTEGERS

BRUNO DULAR

Abstract. We study the period of the linear map $T : \mathbb{Z}_m^n \to \mathbb{Z}_m^n : (a_0, \ldots, a_{n-1}) \mapsto (a_0 + a_1, \ldots, a_{n-1} + a_0)$ as a function of $m$ and $n$, where $\mathbb{Z}_m$ stands for the ring of integers modulo $m$. Because this map is a variant of the Ducci sequence, 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 also characterize the tuples that belong to a cycle when $m$ is prime.

## 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 an $n$-tuple of integers and iterates the *Ducci map* $(a_0, a_1, \ldots, a_{n-1}) \mapsto (|a_0 - a_1|, |a_1 - a_2|, \ldots, |a_{n-1} - a_0|)$ to generate a *Ducci sequence.* This process suggests the name *Cycles of differences of integers* [10], 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. Otherwise, a Ducci sequence will vanish or enter a periodic cycle. As several authors have pointed out [10, 5], 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 $\mathbb{Z}_2^n$. This map can be generalized as stated in Definition 1.1, performing sums modulo $m$ for some positive integer $m$.

This variant was introduced by Wong in [14] and was extensively studied by F. Breuer in [2], 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., $m = p^k$ with $p$ a prime and $n$ divisible by $p$. This is the object of section 5. There, we also see that our method does not generalize to certain special cases ($p = 2$ or $p$ a Wieferich prime), for which F. Breuer's method works.

Here, $\mathbb{N}$ denotes the set of positive integers (with the convention $0 \notin \mathbb{N}$).

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

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

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

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

For example, the T-sequence generated by the basic tuple of $\mathbb{Z}_{10}^4$ starts as shown below. Note 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 $P(10, 4) = 4$.

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

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

Because $x + y \equiv x - y \pmod 2$, 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 $\mathbf{a} \in \mathbb{Z}_m^n$ 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 $\mathbf{a}_{(i \mod n)}$.

Because $\mathbb{Z}_m^n$ is finite, a T-sequence must be eventually periodic. The goal of this paper is to study the maximal cycle length as a function of $m$ and $n$, that 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 $\boldsymbol{a} \in \mathbb{Z}_m^n$, a positive integer $L$ is the* cycle length *of the T-sequence $(T^r \boldsymbol{a})_{r \geq 0}$ if the following conditions hold:*

(1) *There exists a positive integer $N$ such that $T^{r+L}\boldsymbol{a} = T^r \boldsymbol{a}$ for all $r \geq N$.*
(2) *Every positive integer $L'$ satisfying $T^{r+L'}\boldsymbol{a} = T^r \boldsymbol{a}$ for large enough $r$ is a multiple of $L$.*

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

*In other words, the cycle length of the T-sequence $(T^r \boldsymbol{a})_{r\geq 0}$ is the smallest positive integer $L$ such that there exists some $N \in \mathbb{N}$ satisfying $T^{r+L}\boldsymbol{a} = T^r \boldsymbol{a}$ for all $r \geq N$.*

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

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

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

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

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

*This is called the* period *of T-sequences in $\mathbb{Z}_m^n$. This defines a function $P : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ 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. Ehrlich proved this result for Ducci sequences, but the proof is essentially the same for T-sequences.

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

In Section 2, we give basic results that are useful for studying more interesting properties of T-sequences. Among those, we prove a generalization that Ducci sequences of $2^n$-tuples eventually vanish.

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

**Theorem.** *Let $m, n \in \mathbb{N}$ with $m = p_1^{k_1} \ldots p_t^{k_t}$ the prime factorization of $m$. If $p_1, \ldots, p_t$ are odd and non-Wieferich*[1]*, then*

$$P(m,n) = \operatorname{lcm}\left(p_1^{k_1-1}P(p_1,n), \ldots, p_t^{k_t-1}P(p_t,n)\right).$$

[1] See definition 4.4.

## 2. Basic Results

The first result allows us to compute iterations of $T$ in a simple way. It will be used extensively throughout the paper.

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

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

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

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

which completes the proof. □

**Definition 2.2.** *A T-sequence $(T^r \boldsymbol{a})_{r \ge 0}$, where $\boldsymbol{a} \in \mathbb{Z}_m^n$, is said to* vanish*, if there exists a positive integer $r$ such that $T^r \boldsymbol{a} = 0$.*

Recall that T-sequences are Ducci sequences if $m = 2$. Thus, it is well-known that every T-sequence of $\mathbb{Z}_2^n$ vanishes if and only if $n$ is a power of 2. This result was first proved by Ciamberlini and Marengoni in [4], and it has been reproven many times since then [3, 5]. This result still holds when $m$ is any power of 2. This was proved by Wong in [14]. Here, we give a shorter proof, using the notation we introduced and proposition 2.1. In [1], C. Avart showed a converse to this theorem for the base case $m = 2$, 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 $m = 2^c$ and $n = 2^d$ for some positive integers $c$, $d$, then every T-sequence of $\mathbb{Z}_m^n$ vanishes, that is, $P(m, n) = 1$. Reciprocally, if every T-sequence of $\mathbb{Z}_m^n$ vanishes, then $m$ is a power of 2.*

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

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

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

We now proceed with a proof by induction. Assume the result holds for some integer $c$. We prove that the result holds for $c + 1$. Let $\mathbf{a} \in \mathbb{Z}_{2^{c+1}}^{2^d}$. If considered over $\mathbb{Z}_{2^c}^{2^d}$, the T-sequence generated by $\mathbf{a}$ vanishes. Let $r$ be an integer such that $T^r\mathbf{a} \equiv \mathbf{0} \pmod{2^c}$. Therefore, $T^r\mathbf{a} \equiv 2^c\mathbf{u} \pmod{2^{c+1}}$ 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 $r'$ such that $T^{r+r'}\mathbf{a} \equiv 2^c T^{r'}\mathbf{u} \equiv \mathbf{0} \pmod{2^{c+1}}$, which concludes the proof.

The reciprocal follows from the proof of Proposition 4.3. □

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

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

Thus, $T = I + H$, where $I$ is the identity map. The following lemma generalizes Lemma 1 in [5].

**Lemma 2.4.** *If $p$ is a prime and $k$ is a positive integer, then $T^{p^k} = I + H^{p^k}$ as linear maps from $\mathbb{Z}_p^n$ into itself.*

*Proof.* We have $T = I + H$, where $I$ is the identity map. The proof follows from Proposition 2.1 and 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].

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

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

*Proof.* By Lemma 2.4, we have

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 $\mathbb{Z}_n$, 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 $m = p_1^{k_1} \ldots p_t^{k_t}$, knowing $P(p_i, n)$ for $i = 1, \ldots, t$?

The next proposition suggests a positive answer. We will often use it without reference.

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

*Proof.* Let $r \in \mathbb{N}$ be large enough so that $\mathbf{a} = T^r\mathbf{e} \in \mathcal{C}_m^n \subset \mathcal{C}_d^n$. The congruence $T^{P(m,n)}\mathbf{a} \equiv \mathbf{a} \pmod{m}$ still holds modulo $d$ since $d \mid m$. The conclusion follows from Definition 1.3. □

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

**Theorem 3.2.** *If $m = \prod_{i=1}^t p_i$, with $p_1, \ldots, p_t$ pairwise coprime, then*

$$P(m, n) = \operatorname{lcm}\left(P(p_1, n), \ldots, P(p_t, n)\right).$$

*Proof.* We prove this for two coprime integers. The generalization for $t$ pairwise coprime integers follows by induction. By Proposition 1.5, we only need to consider the basic T-sequence.

Let $p$ and $q$ be two coprime integers. Here, we assume that $r$ is large enough for $T^r\mathbf{e}$ to be in different cycles. By Definition 1.3, we have

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

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

We now show that $L$ satisfies (2) of Definition 1.3. Suppose $Q$ is such that $T^{r+Q}\mathbf{e} \equiv T^r\mathbf{e} \pmod{pq}$. In particular, $T^{r+Q}\mathbf{e} \equiv T^r\mathbf{e} \pmod{p}$; 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 determine that this is (almost) the case.

## 4. Order of 2 and Wieferich Primes

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

**Definition 4.2.** *For $m > 2$ odd, we use $O(m)$ to denote the order of 2 in $\mathbb{Z}_m$; that is, it is the smallest integer $k$ such that $2^k \equiv 1 \pmod{m}$. Its existence follows from Euler's theorem.*

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

*Proof.* Let $r$ be a positive integer and $\mathbf{a}$ be a tuple of $\mathbb{Z}_m^n$. By linearity, we have $|T^r\mathbf{a}| \equiv 2^r\,|\mathbf{a}| \pmod{m}$. If $L$ is the cycle length of the T-sequence generated by $\mathbf{a}$ and $r$ is greater than the pre-period, then we must have $\left|T^{r+L}\mathbf{a}\right| \equiv 2^L\,|T^r\mathbf{a}| \pmod{m}$. Hence, $2^L \equiv 1 \pmod{m}$ or $|T^r\mathbf{a}| \equiv 0 \pmod{m}$. Note that if $m$ is not a power of 2, then $|T^r\mathbf{e}| \not\equiv 0 \pmod{m}$ for all $r$. Considering the basic T-sequence, this implies that $2^{P(m,n)}$ must equal $1 \pmod{m}$. □

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

Wieferich primes occur in several number theoretical subjects [8]. It is believed that there are infinitely many such numbers. We only know two of them, 1093 and 3511, and there are no other Wieferich primes below $10^{17}$ [13]. We will see in Section 5 that Wieferich primes are 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 $O(p)$ or $pO(p)$. By definition, $2^{O(p^2)} \equiv 1 \pmod{p^2}$. It also holds modulo $p$, so $O(p^2)$ is a multiple of $O(p)$. We have

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

so $O(p^2)$ divides $pO(p)$. Thus, it equals $O(p)$ or $pO(p)$.

Suppose that $p$ is a Wieferich prime, i.e., $2^{p-1} \equiv 1 \pmod{p^2}$. Then, $O(p^2)$ divides $p-1$. Because we cannot have $O(p^2) = pO(p)$, we have $O(p^2) = O(p)$. Conversely, if $O(p^2) = O(p)$, then $O(p^2)$ divides $p-1$, so $2^{p-1} \equiv 1 \pmod{p^2}$. □

As the following proposition shows, the first part of the previous proof also holds for all primes $p > 2$ and positive integers $k$; that is, $O(p^{k+1})$ is $O(p^k)$ or $pO(p^k)$. 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 $k \in \mathbb{N}$, then we have*

(1) *$O(p^{k+1})$ is $O(p^k)$ or $pO(p^k)$.*

---

[2]If $a \equiv b \pmod{p}$ and $a \equiv b \pmod{q}$, then $a - b = cp = dq$ for some integers $c$, $d$. Hence, $q$ divides $cp$, so $q$ divides $c$ by Euclid's lemma and we get $a - b = c'pq$ for some integer $c'$.

(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 first part of the proof of Lemma 4.5 and (3) follows from (1) and (2) by induction. We show (2).

Suppose $O(p^{k+1}) = pO(p^k)$. Then, $2^{O(p^k)} \equiv 1 + lp^k \pmod{p^{k+1}}$, where $l \not\equiv 0 \pmod p$. Hence, $2^{O(p^k)} \equiv 1 + lp^k + l'p^{k+1} \equiv 1 + p^k(l + l'p) \pmod{p^{k+2}}$ for some $l'$. By the binomial theorem and that $p$ divides $\binom{p}{j}$ for $0 < j < p$, we have $2^{pO(p^k)} \equiv 1 + p^{k+1}(l + l'p) \equiv 1 + lp^{k+1} \pmod{p^{k+2}}$. Since $l \not\equiv 0 \pmod p$, we have $2^{pO(p^k)} \not\equiv 1 \pmod{p^{k+2}}$, so $O(p^{k+2})$ must equal $p^2O(p^k)$. This concludes the proof. □

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. Indeed, if $p$ is an odd prime and $n \in \mathbb{N}$, then $O(p^k) \mid P(p^k, n)$ for all positive integers $k$. That $(O(p^k))_{k\in\mathbb{N}}$ eventually grows as a geometric sequence forces $(P(p^k, n))_{k\in\mathbb{N}}$ to behave in the same way.

**Theorem 5.1.** *If* $p$ *is a prime and* $k, n \in \mathbb{N}$*, then we have*
(1) $P(p^{k+1}, n)$ *is* $P(p^k, n)$ *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* $k \in \mathbb{N}$.

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

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

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

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

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

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

(2). Suppose $k \geq 2$ and 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 $L_1$ or $pL_1$. We show that it equals the latter.

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

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 $L = P(p^k, n)$. Then, we have, by the same argument as in (1),

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

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 that the condition $k \geq 2$ is needed for (2) in the previous theorem to hold.

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

*Proof.* By Theorem 1.5, computing the first iterations of the basic T-sequence gives $P(2,3) = 3$.

We prove that $P(2^k, 3) = 6$ for all positive integers $k > 1$ by induction. The idea of the argument is to show that, for all $k > 1$:

(1) The pre-period of the basic T-sequence of $\mathbb{Z}_{2^k}^3$ is $N_k = k + 1$ and it has a cycle of the form

$$\big((a,a,b),(d,c,c),(a,b,a),(c,c,d),(b,a,a),(c,d,c)\big), \tag{5.1}$$

where $a,b,c,d \in \mathbb{Z}_{2^k}$, with $a,b \leq 2^{k-1} \leq c,d$.

(2) The pre-period of the basic T-sequence of $\mathbb{Z}_{2^{k+1}}^3$ is $N_{k+1} = k + 2$ and it has a cycle of the form

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

where $a',b' \in \mathbb{Z}_{2^{k+1}}$ and $c,d \leq 2^k \leq a',b'$ (Note that $c$ and $d$ are those from (1)). In other words, it means that the cycle in $\mathbb{Z}_{2^{k+1}}^3$ starts at the second tuple of the cycle in $\mathbb{Z}_{2^k}^3$.

For the base cases, $k = 2$ and $k = 3$, the cycles of the basic T-sequences are respectively,

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

and

$$\big((2,3,3),(5,6,5),(3,3,2),(6,5,5),(3,2,3),(5,5,6)\big),$$

so (1) and (2) are satisfied.

Now, let $k > 1$ and suppose (1) is satisfied. Since $c,d \geq 2^{k-1}$, we have $(d,c,c) = 2^{k-1}(1,1,1) + (d',c',c')$ for some $c',d' < 2^{k-1}$. Then by linearity,

$$2^k(1,1,1) + (d'+c', c'+c', d'+c') = T(d,c,c) \equiv (a,b,a) \pmod{2^k}.$$

Hence, $(d'+c', c'+c', d'+c') = (a,b,a)$ because $a, b, c'+c', c'+d'$ are smaller than $2^k$. If we let $a' = 2^k + a$ and $b' = 2^k + b$, we have $T(d,c,c) = (a',b',a')$ and $T^2(d,c,c) \equiv (c,c,d) \pmod{2^{k+1}}$. By symmetry of this argument under cyclic permutations, we have $T^3(d,c,c) \equiv (b',a',a')$, $T^4(d,c,c) \equiv (c,d,c)$, $T^5(d,c,c) \equiv (a',a',b')$, and $T^6(d,c,c) \equiv (d,c,c)$, as desired. Then, $N_{k+1} = N_k + 1$ and (2) holds. □

The goal of the rest of this section is to show the main theorem of this paper, stated in the Introduction. To do that, we need to find *base cases* to use (3) of Theorem 5.1. We first prove the case $p \nmid n$ in Proposition 5.3. Then, we will use combinatorial congruences to deduce the case $p \mid n$.

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

*Proof.* By Theorem 5.1, we know that $P(p^2, n)$ is $P(p, n)$ or $pP(p, n)$. Because $p$ 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 $pO(p)$, because $p$ is non-Wieferich (Proposition 4.6). Therefore, $p$ divides $P(p^2, n)$ and we must have $P(p^2, n) = pP(p, n)$.

Similarly, $P(p^3, n)$ is $pP(p, n)$ or $p^2P(p, n)$. Because $O(p^3) = p^2O(p)$ divides $P(p^3, n)$ and $pP(p, n)$ is not divisible by $p^2$, we must have $P(p^3, n) = p^2P(p, n)$. □

**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 $k \in \mathbb{N}$.*

*Proof.* It follows from Proposition 5.3 and (3) in Theorem 5.1. □

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

The *p-adic valuation* of an integer $n$ is the exponent of the largest power of $p$ that divides $n$. We denote this by $v_p(n)$. We write $s_p(n)$ for the sum of the digits of $n$ when written in base $p$. If $p$ is a prime, *Legendre's formula* [9] 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 $a$ and $b$.

The following Lemma generalizes the following: $p$ divides $\binom{p^v}{n}$ for all $0 < n < p^v$, but not for $n = 0$ and $p^v$. We will make use of the cases $s = 2$ and 3 later in Proposition 5.9.

**Lemma 5.5.** *Let $p$ be a prime and $v, s \in \mathbb{N}$ with $1 \leq s \leq v$. We have*

$$\left\{n \in \{0, \dots, p^v\} : p^s \nmid \binom{p^v}{n}\right\} = \left\{mp^{v-s+1} \colon 0 \leq m \leq p^{s-1}\right\}.$$

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

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

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

Thus,

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

and

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

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

The following lemma was proved by Darij Grinberg and Victor Reiner ((12.69.3) in [6]).

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

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

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

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

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

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

If a $(rn)$-element 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.

On the other hand, the permutation $\phi : i \mapsto i + qn/p^{v_p(n)}$ of $\mathbb{Z}_{qn}$ acts on the subsets of the second class, splitting them into orbits. Their $p^{v_p(n)}$-power acts trivially on the subsets of the second class. Then, 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 $|\mathcal{O}|$ divides $p^{v_p(n)-1}$, so $\phi^{p^{v_p(n)-1}}$ acts trivially on $\mathcal{O}$. Hence, elements of this orbit are subsets of the first class, a contradiction. Thus, every orbit has size $p^{v_p(n)}$.

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

Therefore, we have $\binom{qn}{rn} = N_1 + N_2 \equiv \binom{qn/p}{rn/p} \pmod{p^{v_p(n)}}$ 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 $\binom{ap}{bp} \equiv \binom{a}{b} \pmod{p^2}$. Note that if $p \geq 5$, we can replace $\pmod{p^2}$ by $\pmod{p^3}$, thus strengthening the result. This case is known as *Wolstenholme's theorem*.

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

$$\binom{p^v}{jp^{v-1}} \equiv \binom{p}{j} \pmod{p^2}.$$

*Proof.* The proof follows directly from Babbage's theorem by induction. □

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

$$\binom{p^v}{jp^{v-2}} \equiv \binom{p^2}{j} \pmod{p^3}.$$

*Proof.* For $p \geq 5$, the proof follows from Wolstenholme's theorem by induction.

Now we consider the cases $p = 2$ and $p = 3$. If $v = 2$, the result follows directly. If $v > 2$, then Lemma 5.6 with $q = 1$, $n = p^v$ (then $v_p(n) = v$), and $r = j/p^2$ gives

$$\binom{p^v}{jp^{v-2}} = \binom{qn}{rn} \equiv \binom{qn/p}{rn/p} \equiv \binom{p^{v-1}}{jp^{v-3}} \pmod{p^v}.$$

The congruence holds modulo $p^3$ since $v \geq 3$. Then, the proof proceeds by induction. □

Now, we can apply these lemmas to prove the following proposition, which gives us base cases to apply Theorem 5.1.

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

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

*Proof.* The idea of this proof is to study the behavior of a T-sequence $(T^i \mathbf{a})_{i\in\mathbb{N}}$ of $\mathbb{Z}_m^n$ (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 understand better.

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

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

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

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

If $p = 2$, note that this argument only holds if the T-sequences do not vanish. This explains the additional condition $n' \neq 1$ 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 $P(p^2, n) = p^{v-1}P(p^2, pn')$.

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

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

which implies that $S_0(T^{p^2}\mathbf{a}) \equiv T^p S_0(\mathbf{a}) \pmod{p^2}$. Because $p$ is an odd non-Wieferich prime, $p$ divides $P(p^2, n')$ by Proposition 5.3. 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 $\mathbf{a} \in \mathbb{Z}_p^n$, the subtuple $S_1(\mathbf{a})$ is in $\mathbb{Z}_{p^2}^{pn'}$. We also have

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

where the second and third equalities follow from Lemmas 5.5 and 5.7, respectively. Thus, $S_1(T^{p^v}\mathbf{a}) \equiv T^p S_1(\mathbf{a}) \pmod{p^2}$. Therefore, we obtain

$$P(p^2, n) = p^v p^{-1} P(p^2, pn') = p^{v-1} P(p^2, pn') = p^v P(p^2, n'),$$

as desired, where the last equality follows from the first part.

(3). Suppose $p > 2$ is a non-Wieferich prime. Suppose $v > 1$. We first show that $P(p^3, p^2n') = p^2P(p^3, n')$, and then that $P(p^3, n) = p^{v-2}P(p^3, p^2n')$.

First, we use $S_0$. For $\mathbf{a} \in \mathbb{Z}_{p^3}^{p^2n'}$, the subtuple $S_0(\mathbf{a})$ is in $\mathbb{Z}_{p^3}^{n'}$. By Lemmas 5.5 and 5.8, we have

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

Hence, $S_0(T^{p^4}\mathbf{a}) \equiv T^{p^2}S_0(\mathbf{a}) \pmod{p^3}$. By Proposition 5.3 (it is why we consider $p > 2$ non-Wieferich), $p^2$ divides $P(p^3, n')$. Thus, we obtain $P(p^3, p^2n') = p^4p^{-2}P(p^3, n') = p^2P(p^3, n')$.

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

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

Hence, $S_2(T^{p^v}\mathbf{a}) \equiv T^{p^2}S_2(\mathbf{a}) \pmod{p^3}$. Together with the first part, because $p^2$ divides $P(p^3, p^2n')$ (by Proposition 5.3), we get $P(p^3, n) = p^vp^{-2}P(p^3, p^2n') = p^vP(p^3, n')$ as desired.

To conclude the proof, we consider the case $v = 1$. We have to show that $P(p^3, pn') = pP(p^3, n')$. We use $S_0$. For $\mathbf{a} \in \mathbb{Z}_{p^3}^{pn'}$, the subtuple $S_0(\mathbf{a})$ is in $\mathbb{Z}_{p^3}^{n'}$. As above, using Lemmas 5.5 and 5.8, we have $[T^{p^3}\mathbf{a}]_i \equiv \sum_{j=0}^{p^2} \binom{p^2}{j}\mathbf{a}_{i+jp} \pmod{p^3}$. Hence, $S_0(T^{p^3}\mathbf{a}) \equiv T^{p^2}S_0(\mathbf{a}) \pmod{p^3}$. 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 concludes the proof. □

**Theorem 5.10.** *If $p > 2$ 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 $k, n \in \mathbb{N}$. Write $n = p^vn'$, where $v = v_p(n)$. We show that (1) $P(p^2, n) = pP(p, n)$ and (2) $P(p^3, n) = p^2P(p, n)$.

(1). Points (1) and (2) of Proposition 5.9 yield $P(p, n) = p^vP(p, n')$ and $P(p^2, n) = p^vP(p^2, n')$, respectively. Because $p > 2$ is non-Wieferich and coprime to $n'$, 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).

We complete the proof by Theorem 5.1. □

We are now able to prove the main result of this paper.

**Theorem 5.11.** *Let $m, n \in \mathbb{N}$ with $m = p_1^{k_1} \cdots p_t^{k_t}$, the prime factorization of $m$. If $p_1, \dots, p_t$ are odd and non-Wieferich, then*

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

*Proof.* The proof follows from Theorems 3.2 and 5.10. □

At this point, a question one may ask is whether we can generalize this result for $p = 2$ and Wieferich primes. The proofs above are considerably dependant on Proposition 5.3, which itself is dependent 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 [2], 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 behave as we would expect. Whether it is possible 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 $\mathbb{Z}_m^n$ that belong to $\mathcal{C}_m^n$. By Theorem 2.3, we already know that $\mathcal{C}_m^n = \{\mathbf{0}\}$, if $m$ and $n$ are powers of 2.

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

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

Note that $\det(T) = 0$, when $n$ is even, and $\det(T) = 2$, when $n$ is odd. We then have the following proposition.

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

*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 $\mathbb{Z}_m^n$, 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 $\mathbf{a} \in \mathbb{Z}_m^n$ by

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

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

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

$$\begin{cases} x_0 + x_1 \equiv a_0, \\ x_1 + x_2 \equiv a_1, \\ \quad \vdots \\ x_{n-1} + x_0 \equiv a_{n-1}, \end{cases} \quad \text{which is equivalent to} \quad \begin{cases} x_1 \equiv a_0 - x_0, \\ x_2 \equiv a_1 - a_0 + x_0, \\ x_3 \equiv a_2 - a_1 + a_0 - x_0, \\ \quad \vdots \\ x_{n-1} \equiv a_{n-2} - a_{n-3} + \cdots + a_0 - x_0, \\ x_0 \equiv a_{n-1} - a_{n-2} + \cdots + a_1 - a_0 + x_0. \end{cases} \tag{6.1}$$

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

Therefore, the map $T$, restricted to the set $\{\mathbf{a} \in \mathbb{Z}_m^n : \sigma(\mathbf{a}) = 0\}$, is a one-to-one correspondence, and we can make the same conclusion as Proposition 6.1.

The last equation of (6.1) shows that the condition is necessary. □

[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.

The following result, concerning $\mathbb{Z}_2^n$, is shown in [10] and in [12] for the Ducci map, which is the same as our map in this case.

**Proposition 6.3.** *In $\mathbb{Z}_2^n$, we have $\operatorname{im}(T) = \{\boldsymbol{a} \in \mathbb{Z}_2^n : |\boldsymbol{a}| = 0\}$ and every $\boldsymbol{a} \in \operatorname{im}(T)$ has exactly two preimages. For odd $n$, a tuple $\boldsymbol{a} \in \mathbb{Z}_2^n$ 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 both in $\operatorname{im}(T)$ or both in $\mathbb{Z}_2^n \backslash \operatorname{im}(T)$. Thus, we have to find a way to characterize tuples of $\operatorname{im}(T)$ that have preimages in $\operatorname{im}(T)$.

This has already been done by Ludington-Young in [10, 11], where the following definition and Theorem 6.4 come from. Here, we only consider tuples of $\mathbb{Z}_2^n$. A tuple $\mathbf{a}$ is *even* if $|\mathbf{a}| = 0$. Suppose $n = 2^r n'$, where $n'$ is odd. We say a tuple $\mathbf{a} \in \mathbb{Z}_2^n$ is *$r$-even* if

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

for $j = 0, \ldots, 2^r - 1$. 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 $n = 2^r n'$ with $n'$ odd. A tuple in $\mathbb{Z}_2^n$ 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.

**Definition 6.5.** *Let $n = p^r n'$ with $r = v_p(n)$. We say a tuple $\boldsymbol{a}$ of $\mathbb{Z}_p^n$ is* even *if $\sigma(\boldsymbol{a}) = 0$. We note*

$$\sigma_j(\boldsymbol{a}) = \sum_{i=0}^{n'-1} (-1)^i a_{p^r i+j} \mod p$$

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

**Theorem 6.6.** *Let $p > 2$ be a prime and $n = p^r n'$ even with $r = v_p(n)$. A tuple of $\mathbb{Z}_p^n$ belongs to a cycle if and only if it is $r$-even.*

*Proof.* The congruences below are all modulo $p$.

First, note that $T\mathbf{a}$ is $r$-even if $\mathbf{a}$ is $r$-even. Indeed, if $\mathbf{a}$ is $r$-even, then $\sigma_j(T\mathbf{a}) \equiv \sigma_j(\mathbf{a}) + \sigma_{j+1}(\mathbf{a}) \equiv 0$ for each $j$. By Lemma 2.4, we have that $T^{p^r}\mathbf{e} \equiv \mathbf{e} + H^{p^r}\mathbf{e}$ is $r$-even. Thus, every tuple of a cycle must be $r$-even by linearity of $r$-evenness. Hence, the condition is necessary.

We now show the condition is sufficient. Let $\mathbf{a} \in \mathbb{Z}_p^n$ be $r$-even. By (6.1) (it is here that we use the condition that $n$ is even) and because $r$-evenness implies evenness, the tuple $\mathbf{a}$ has $p$ preimages. Let $\mathbf{b}^{(0)}$ be one of these preimages. Hence, all preimages are given by $\mathbf{b}^{(l)} = \mathbf{b}^{(0)} + (l, -l, \ldots, l, -l)$ for $l = 0, \ldots, p-1$. To simplify notation, we write $\sigma_j$ for $\sigma_j\left(\mathbf{b}^{(0)}\right)$.

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

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

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

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

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

Because $n'$ is invertible modulo $p$, the equation $\sigma_0\left(\mathbf{b}^{(l)}\right) \equiv \sigma_0 + n'l \equiv 0 \pmod{p}$ has exactly one solution $l \equiv -\sigma_0/n' \pmod{p}$. 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 $\mathbb{Z}_p^n$ is bijective and the proof is complete. □

## 7. Open Questions

We can see the iterations of the map $T$ on the set $\mathcal{C}_m^n$ (which is bijective when restricted to $\mathcal{C}_m^n$) as the action of the group $\left\{T^k : k \in \mathbb{Z}\right\}$ 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 can the results of this paper be generalized to any linear map of $\mathbb{Z}_m^n$? Do there exist explicit formulas to find $P(p, n)$ for every prime $p$ and positive integer $n$?

## 8. Acknowledgements

The author thanks the anonymous referees for their useful and detailed comments.

## References


[1] C. Avart, *A characterization of converging Ducci sequences over $Z_2$*, The Fibonacci Quarterly, **49.2** (2011), 155–157.

[2] F. Breuer, *Ducci sequences and cyclotomic fields*, Journal of Difference Equations and Applications, **16.7** (2010), 847–862.

[3] F. Breuer, *Ducci sequences in higher dimensions*, INTEGERS: Electronic Journal of Combinatorial Number Theory, **7.24** (2007).

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

[5] A. Ehrlich, *Periods in Ducci's n-number game of differences*, The Fibonacci Quarterly, **28.4** (1990), 302–305.

[6] D. Grinberg and V. Reiner, *Hopf algebras in combinatorics*, `https://arxiv.org/abs/1409.8356v5/`.

[7] D. Grinberg, *The Lucas and Babbage congruences*, `http://www.cip.ifi.lmu.de/~grinberg/`.

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

[9] A. M. Legendre, *Théorie des nombres*, Firmin Didot Frères, Paris, 1830.

[10] A. Ludington Furno, *Cycles of differences of integers*, Journal of Number Theory, **13.2** (1981), 255–261.

[11] A. Ludington-Young, *Even Ducci-sequences*, The Fibonacci Quarterly, **37.2** (1999), 145–153.

[12] M. Misiurewicz, J. G. Stevens, and D. M. Thomas, *Iterations of linear maps over finite fields*, Linear Algebra and its Application, **413.1** (2006), 218–234.

[13] OEIS Foundation Inc. (2011), The On-Line Encyclopedia of Integer Sequences, `https://oeis.org/A001220`, 2017.

[14] F. B. Wong, *Ducci processes*, The Fibonacci Quarterly, **20.2** (1982), 97–105.


MSC2010: 05A10, 11B50, 11B75

Rue Vaudrée 23, 4031 Angleur, Belgium
*Email address*: `bruno.dular@epfl.ch`