EXISTENCE OF CYCLES IN DUCCI'S FOUR-NUMBER GAME WITH MODULAR MULTIPLICATION

Tasha Fellman
Department of Mathematics, University of Illinois Urbana-Champaign, Champaign, Illinois,
fellman2@illinois.edu

Dominic Klyve
Department of Mathematics, Central Washington University, Ellensburg, Washington
dominic.klyve@cwu.edu

Received: 2/1/23, Revised: 7/7/23, Accepted: 10/27/23, Published: 11/20/23

Abstract

In this paper, we will investigate a variation of Ducci's Four-Number Game using modular multiplication. That is, we will study the cycles formed by repeating the following endomorphism in $\mathbb{Z}_n^4$, $\begin{bmatrix} a & b & c & d \end{bmatrix} \mapsto \begin{bmatrix} ab & bc & cd & da \end{bmatrix}$. Our main goal is to analyze and classify the cycles that arise in this new variation. Specifically, we will determine for which moduli nontrivial cycles exists, and will produce methods to generate them.

1. Introduction

Ducci's 4-number game [4] is a game in which the mapping

$$\begin{bmatrix} a & b & c & d \end{bmatrix} \mapsto \begin{bmatrix} |a-b| & |b-a| & |c-d| & |d-a| \end{bmatrix}$$

is repeated forever with $a, b, c, d \in \mathbb{N}$. We may say that the game ends when the 4-tuple reaches $\begin{bmatrix} 0 & 0 & 0 & 0 \end{bmatrix}$, as from this point onwards, the behavior of the 4-tuples is quite trivial. It simply remains at $\begin{bmatrix} 0 & 0 & 0 & 0 \end{bmatrix}$. The game is often used as a way to help children learn subtraction [1], but the game also exhibits complex behavior. It has been shown by Freedman [5] that this game will always converge to $\begin{bmatrix} 0 & 0 & 0 & 0 \end{bmatrix}$ in finitely many steps, but Yueh and Cheng [8] have found that by working with $a, b, c, d \in \mathbb{R}$ instead of $\mathbb{N}$, it may take infinite amount of steps to converge to 0 such as starting with $\begin{bmatrix} 1 & \varphi & \varphi^2 & \varphi^3 \end{bmatrix}$ with $\varphi = \frac{1+\sqrt[3]{19-3\sqrt{33}}+\sqrt[3]{19+3\sqrt{33}}}{3}$.

DOI: 10.5281/zenodo.10160456

However, it may not always take an infinite amount of steps; $\begin{bmatrix}1 & \sqrt{2} & e & \pi\end{bmatrix}$ converges to $\begin{bmatrix}0 & 0 & 0 & 0\end{bmatrix}$ in 5 iterations. Thus Ullman [7] has mapped out regions of $\mathbb{R}^4$ based off of where it converges as well as how many steps it takes until the game converges. There are also many papers considering a variation on the game (such as *Length of the 7-number game* [6] and *A characterization for the length of cycles of the n-number Ducci game* [3]) where the game is played with either more or less than four numbers.

In this paper, we will instead consider a different variation on the 4-number game:

$$\begin{bmatrix}a & b & c & d\end{bmatrix} \mapsto \begin{bmatrix}ab & bc & cd & da\end{bmatrix},$$

in which the resulting products are taken modulo n for some integer $n \geq 2$. (In our new variation, we will only be considering the case in which $a, b, c, d \in \mathbb{Z}_n$.) Since the space of tuples we are investigating is finite, it is clear that every 4-tuple must enter a cycle after enough iterations. However, unlike the original game described by Ciamberlini and Marengoni [4], the cycles that arise here are not always so simple. For example, starting from $\begin{bmatrix}1 & 4 & 1 & 2\end{bmatrix}$ modulo 7, we get this game,

$$\begin{bmatrix}1 & 4 & 1 & 2\end{bmatrix} \mapsto \begin{bmatrix}4 & 4 & 2 & 2\end{bmatrix} \mapsto \begin{bmatrix}2 & 1 & 4 & 1\end{bmatrix}.$$

Thus, after repeating the mapping twice, we obtain the same 4-tuple as we started with but with all of the variables shifted one spot over. So if we then repeated the mapping six more times, we get back to exactly where we started and so $\begin{bmatrix}1 & 4 & 1 & 2\end{bmatrix}$ is in a cycle modulo 7. We will see later that the six additional iterations are not needed to determine if it is in a cycle. Yet for some moduli such as 4 and 5, there are no cycles other than the cycles consisting of $\begin{bmatrix}0 & 0 & 0 & 0\end{bmatrix}$ and $\begin{bmatrix}1 & 1 & 1 & 1\end{bmatrix}$. Because these two cycles are present in every moduli, we consider them trivial. Our goal in this paper is to explore the cycles excluding these two and to determine for which moduli nontrivial cycles exist. Specifically, the main goal of this paper is to prove the following theorem.

Theorem 1. *A nontrivial cycle exists modulo n if and only if n is neither a Fermat prime nor a power of 2.*

The only known values of n of this form are 3, 5, 17, 257, 65537 (see Boklan and Conway [2]), and powers of 2. Additionally, if there exists nontrivial cycles modulo n, then we will produce methods to generate at least one of them.

This paper will be organized thusly. In the following section, we will provide definitions and observe that we can split our study of these cycles into two different cases. Next, we shall build tools helpful for creating new cycles out of existing ones. We will then determine when nontrivial cycles exist for each of the two cases, which will cover the next two sections. By that point, we will be able to prove Theorem 1. We will then spend the final two sections proving additional facts about the structure of the cycles in this game, such as finding how quickly 4-tuples

converge to a cycle as well as finding a basis for the cycles. So to begin, we shall first need some definitions.

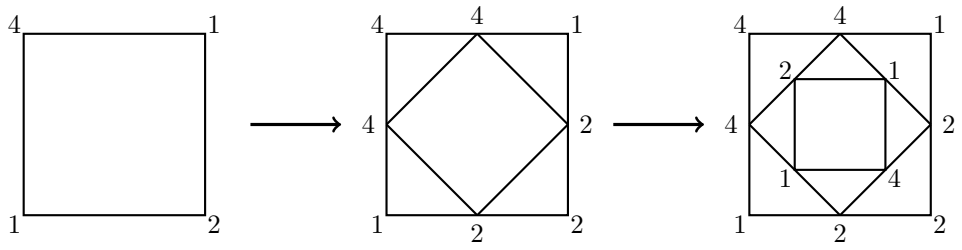

Figure 1: This is a more geometric view of the mapping. We place the four numbers on the corners of a square. On the midpoint of the each of the squares edges, we write the product of the adjacent edges modulo n (in this example, $n = 7$). We may then draw a new square connecting these midpoints and repeat this process in the new square. Note that the inner most square is a flipped version of the outermost square and so it is in a cycle.

2. Definitions

Due to the symmetries of the mapping, we consider two 4-tuples to be *equivalent* if one can be mapped to the other by shifting and reversing the 4-tuples. That is, $\begin{bmatrix} a & b & c & d \end{bmatrix}$, $\begin{bmatrix} a & d & c & b \end{bmatrix}$, $\begin{bmatrix} b & a & d & c \end{bmatrix}$, $\begin{bmatrix} b & c & d & a \end{bmatrix}$, $\begin{bmatrix} c & b & a & d \end{bmatrix}$, $\begin{bmatrix} c & d & a & b \end{bmatrix}$, $\begin{bmatrix} d & a & b & c \end{bmatrix}$, and $\begin{bmatrix} d & c & b & a \end{bmatrix}$ shall be considered equivalent. The reason that they may be considered the same is due to a more geometric formulation of the problem given in Figure 1. It is clear that rotating and reflecting the square in the figure preserves the structure of this games' mapping which then provides the equivalence classes. And so, these 4-tuples may be treated as having the symmetries of a square. These equivalence classes are not strictly necessary but they allow us to greatly shorten the notation. When referring to a 4-tuple, we will treat them as their equivalence class, unless otherwise specified.

A 4-tuple, T, is said to be in a *cycle* when there is some $L \in \mathbb{N}$ such that after iterating the game $L + 1$ many times starting at T, the game returns to a tuple equivalent to T up to symmetry. We say that the cycle itself is the set of 4-tuples arrived at when iterating T in the order that they appear when iterating. We also define the *length* of the cycle to be the smallest positive L for which this property holds. It is also important to note that not every 4-tuple will be in a cycle (this can be demonstrated in Figure 2). However, those 4-tuples are not of our primary concern until Section 6.

The cycles of length 1 consisting of either $\begin{bmatrix} 0 & 0 & 0 & 0 \end{bmatrix}$ or $\begin{bmatrix} 1 & 1 & 1 & 1 \end{bmatrix}$ will be

called *trivial cycles*. They are considered trivial as every modulus will have these simple cycles. A cycle other than these two is a *nontrivial cycle*.

Finally, The set of integers modulo n that are relatively prime to n will be denoted $\mathbb{Z}_n^\times$. Additionally, the smallest positive k such that $\beta^k \equiv 1 \pmod{m}$ will be denoted $o_m(\beta)$. We shall denote the smallest positive integer k such that $a^k \equiv 1 \pmod{n}$ for all a coprime to n as $\lambda(n)$. That is, $\lambda(n) = \operatorname{lcm}\{o_n(\beta) \mid \beta \in \mathbb{Z}_n^\times\}$.

It turns out that cycles can be partitioned into four categories based on whether their elements are relatively prime to n and whether all elements of a 4-tuple are the same. To that end, we shall need two more definitions, which inspired the two following lemmas.

Lemma 2. *If* $\begin{bmatrix} a & b & c & d \end{bmatrix}$ *is in a cycle modulo* n*, then either* $a, b, c, d \in \mathbb{Z}_n^\times$ *or* $a, b, c, d \in \mathbb{Z}_n \setminus \mathbb{Z}_n^\times$.

Proof. Suppose that at least one of a, b, c, and d is in $\mathbb{Z}_n \setminus \mathbb{Z}_n^\times$. Then the game proceeds as follows:

$$\begin{bmatrix} a & b & c & d \end{bmatrix} \mapsto \begin{bmatrix} ab & bc & cd & ad \end{bmatrix} \mapsto \begin{bmatrix} ab^2c & bc^2d & acd^2 & a^2bd \end{bmatrix} \mapsto \begin{bmatrix} ab^3c^3d & abc^3d^3 & a^3bcd^2 & a^3b^3cd \end{bmatrix}.$$

By the fourth step, all elements of the 4-tuple are multiples of something in $\mathbb{Z}_n \setminus \mathbb{Z}_n^\times$, so they must all be in $\mathbb{Z}_n \setminus \mathbb{Z}_n^\times$. Similarly, all elements of future 4-tuples will also be in $\mathbb{Z}_n \setminus \mathbb{Z}_n^\times$. However, these are in a cycle, so $\begin{bmatrix} a & b & c & d \end{bmatrix}$ is also a future step and $a, b, c, d \in \mathbb{Z}_n \setminus \mathbb{Z}_n^\times$. We have therefore shown that either all elements of the 4-tuple in a cycle are in $\mathbb{Z}_n \setminus \mathbb{Z}_n^\times$ or none of them are. □

We can then split cycles into two categories: *coprime cycles*, whose elements are all in $\mathbb{Z}_n^\times$, and *cocomposite cycles*, whose elements are all in $\mathbb{Z}_n \setminus \mathbb{Z}_n^\times$.

Additionally, suppose that we have a 4-tuple in a cycle in which all elements of the 4-tuple are equivalent modulo n. After iterating the game, it is clear that for each 4-tuple in the cycle, the elements of the 4-tuple must be equivalent to each other mod n. We then have a proof of the following lemma.

Lemma 3. *Let* $a, b, c, d, e \in \mathbb{Z}_n$*. If* $\begin{bmatrix} a & b & c & d \end{bmatrix}$ *and* $\begin{bmatrix} e & e & e & e \end{bmatrix}$ *are in the same cycle modulo* n*, then* $a \equiv b \equiv c \equiv d \pmod{n}$.

This property is quite useful so we shall add another definition for these types of cycles. We say that a cycle is *constant* if all of its tuples have equal components. For example, $\begin{bmatrix} 2 & 2 & 2 & 2 \end{bmatrix} \mapsto \begin{bmatrix} 4 & 4 & 4 & 4 \end{bmatrix} \mapsto \begin{bmatrix} 2 & 2 & 2 & 2 \end{bmatrix}$ is a constant cycle mod 7.

3. Combining Cycles

Given any 4-tuple in a cycle, we shall see in Theorem 6 that we can generate new cycles from a given cycle. First however, we will need to work with creating a cycle

from two given cycles instead of one.

We can define a multiplication of 4-tuples as follows. Let $\begin{bmatrix} a & b & c & d \end{bmatrix}$ and $\begin{bmatrix} e & f & g & h \end{bmatrix}$ be 4-tuples in $\mathbb{Z}_n^4$. Then we can write

$$\begin{bmatrix} a & b & c & d \end{bmatrix} \times \begin{bmatrix} e & f & g & h \end{bmatrix} = \begin{bmatrix} ae & bf & cg & dh \end{bmatrix},$$

which must be in a cycle if $\begin{bmatrix} a & b & c & d \end{bmatrix}$ and $\begin{bmatrix} e & f & g & h \end{bmatrix}$ are in cycles due to the following lemma. One may check that this product provides a commutative monoid structure on the set of 4-tuples in $\mathbb{Z}_n^4$ that are in cycles as a submonoid of $\mathbb{Z}_n^4$ via a consequence of Lemma 4. Note that for this multiplication, we are discussing the 4-tuples themselves and not the equivalence class that the 4-tuples belong to. We will see later that this multiplication does not respect the symmetries of the 4-tuples so we must be very careful when using this product and specify the order of the elements in the 4-tuples.

Lemma 4. *Let A and B be two 4-tuples that are in cycles modulo n of lengths L_A and L_B. Then $A \times B$ is also in a cycle modulo n whose length is a divisor of* $\operatorname{lcm}(L_A, L_B)$.

Proof. Let A and B be two 4-tuples in $\mathbb{Z}_n^4$. Let A_i, B_i, and X_i be the 4-tuples obtained by iterating the game i steps starting with A, B, and $A \times B$, respectively where $i \in \mathbb{N}$. We will show that $X_i = A_i \times B_i$ for all $i \in \mathbb{N}$ via induction.

For the base case of $i = 0$, we know by definition that $X_0 = A \times B = A_0 \times B_0$. Now suppose that $X_i = A_i \times B_i$. We may arbitrarily denote A_i and B_i as $\begin{bmatrix} a_1 & a_2 & a_3 & a_4 \end{bmatrix}$ and $\begin{bmatrix} b_1 & b_2 & b_3 & b_4 \end{bmatrix}$. Then by the inductive hypothesis,

$$X_i = \begin{bmatrix} a_1b_1 & a_2b_2 & a_3b_3 & a_4b_4 \end{bmatrix}.$$

Now we may iterate X_i's game to obtain

$$\begin{aligned} X_i \mapsto X_{i+1} &= \begin{bmatrix} a_1b_1a_2b_2 & a_2b_2a_3b_3 & a_3b_3a_4b_4 & a_4b_4a_1b_1 \end{bmatrix} \\ &= \begin{bmatrix} a_1a_2b_1b_2 & a_2a_3b_2b_3 & a_3a_4b_3b_4 & a_4a_1b_4b_1 \end{bmatrix} = A_{i+1} \times B_{i+1}. \end{aligned}$$

We have then proven by induction that $X_i = A_i \times B_i$ for all $i \in \mathbb{N}$. In particular, if A and B are in cycles of lengths L_A and L_B, respectively then

$$X_{\operatorname{lcm}(L_A,L_B)} = A_{\operatorname{lcm}(L_A,L_B)} \times B_{\operatorname{lcm}(L_A,L_B)} = A \times B = X_0.$$

And so $A \times B$ must be in a cycle whose length divides $\operatorname{lcm}(L_A, L_B)$ and we have our desired result. □

This method of creating cycles is efficient (as we will see in Theorem 13) albeit inconsistent, due to the different equivalencies of the 4-tuples. For example, the 4-tuple $\begin{bmatrix} 1 & 1 & 2 & 2 \end{bmatrix}$ is in a cycle of length 2 when we let the modulus be 7. However, if we multiply it by two 4-tuples that are in cycles and are equivalent to each

other, we may observe that the resulting products may be in different cycles from each other.

$$\begin{bmatrix}1 & 1 & 2 & 2\end{bmatrix} \times \begin{bmatrix}1 & 1 & 2 & 2\end{bmatrix} = \begin{bmatrix}1 & 1 & 4 & 4\end{bmatrix}$$
$$\begin{bmatrix}1 & 1 & 2 & 2\end{bmatrix} \times \begin{bmatrix}2 & 2 & 1 & 1\end{bmatrix} = \begin{bmatrix}2 & 2 & 2 & 2\end{bmatrix}$$

For this reason, we must be careful to specify the order of the elements of the 4-tuple when multiplying them together.

Luckily our next method of generating cycles does not have this issue and we may return to referring to the equivalence classes of 4-tuples rather than their representatives. It is similarly helpful to introduce notation for the following proof as well. Let $a, b, c, d \in \mathbb{Z}_n^\times$. Then we write

$$\begin{bmatrix}a & b & c & d\end{bmatrix}^{-1} = \begin{bmatrix}a^{-1} & b^{-1} & c^{-1} & d^{-1}\end{bmatrix},$$

where the x^{-1} is the multiplicative inverse of x mod n for any $x \in \mathbb{Z}_n^\times$.

Lemma 5. *Let A be a 4-tuple in a coprime cycle modulo n. Then A^{-1} is in a (possibly different) coprime cycle modulo n of the same length.*

Proof. This lemma will follow a very similar structure to that of Lemma 4. Suppose that A is a 4-tuple in $(\mathbb{Z}_n^\times)^4$. Let A_i and X_i be the 4-tuples obtained by iterating the game i steps starting with A and A^{-1}, where $i \in \mathbb{N}$. We will show that $X_i = A_i^{-1}$ via induction.

For the base case of $i = 0$, we know by definition that $X_0 = A_i^{-1}$. Now suppose that $X_i = A_i \times B_i$. We may denote A_i as $\begin{bmatrix}a_1 & a_2 & a_3 & a_4\end{bmatrix}$. Then by the inductive hypothesis,

$$X_i = \begin{bmatrix}a_1^{-1} & a_2^{-1} & a_3^{-1} & a_4^{-1}\end{bmatrix}.$$

Now we may iterate X_i's game to obtain

$$X_i \mapsto X_{i+1} = \begin{bmatrix}a_1^{-1}a_2^{-1} & a_2^{-1}a_3^{-1} & a_3^{-1}a_4^{-1} & a_4^{-1}a_1^{-1}\end{bmatrix} = A_{i+1}^{-1}.$$

We have then proven by induction that $X_i = A_i^{-1}$ for all $i \in \mathbb{N}$. In particular, if A is in a coprime cycle of length L, then

$$X_L = A_L^{-1} = A^{-1} = X_0.$$

And so A^{-1} must be in a cycle with the same length as A's cycle and we have therefore proven the lemma. □

From Lemmas 4 and 5, we can then obtain the following general properties of 4-tuples in cycles.

Theorem 6. *Let $n \geq 2$ and let $a, b, c, d \in \mathbb{Z}_n$. Suppose that $\begin{bmatrix}a & b & c & d\end{bmatrix}$ is in some cycle modulo n. Then the following hold:*

1. $\begin{bmatrix} abcd & abcd & abcd & abcd \end{bmatrix}$ *is also in a (possibly different) cycle;*
2. $ac \equiv bd \pmod{n}$*;*
3. $\begin{bmatrix} ac & ac & ac & ac \end{bmatrix}$ *is in the same cycle as* $\begin{bmatrix} abcd & abcd & abcd & abcd \end{bmatrix}$*;*
4. $\begin{bmatrix} 1 & ac^{-1} & 1 & a^{-1}c \end{bmatrix}$ *is also some entry in a cycle, if* $a, b, c, d \in \mathbb{Z}_n^\times$.

Proof. Let $\begin{bmatrix} a & b & c & d \end{bmatrix}$ be in a cycle. If we multiply it by a 4-tuple that is equivalent to it, $\begin{bmatrix} c & d & a & b \end{bmatrix}$, we see that this forms a new cycle that includes the 4-tuple $\begin{bmatrix} ac & bd & ac & bd \end{bmatrix}$. The next step in $\begin{bmatrix} ac & bd & ac & bd \end{bmatrix}$'s cycle is then

$$\begin{bmatrix} abcd & abcd & abcd & abcd \end{bmatrix},$$

as desired. Since this is a constant cycle that contains $\begin{bmatrix} ac & bd & ac & bd \end{bmatrix}$, we know from Lemma 3 that

$$ac \equiv bd \pmod{n}.$$

Similarly, Lemma 5 shows us that we can multiply $\begin{bmatrix} a & b & c & d \end{bmatrix}$ by $\begin{bmatrix} c & b & a & d \end{bmatrix}^{-1}$ to get a cycle that includes $\begin{bmatrix} 1 & ac^{-1} & 1 & a^{-1}c \end{bmatrix}$. □

4. Cocomposite Cycles

In this section we will determine when nontrivial cocomposite cycles exist. First, we will find the cases of when at least one such cycle exists.

Theorem 7. *If n is not a power of a prime, then there is a nontrivial cocomposite cycle modulo n.*

Proof. Let d be a nontrivial proper divisor of n, such that $\gcd(d, \frac{n}{d}) = 1$. Consider the sequence $\delta_i = d^{2^i} \pmod{n}$ where $i \in \mathbb{N}$. We want to show that this sequence is eventually periodic and avoids 0 and 1 modulo n. We will first show that there are no 0's or 1's in the sequence.

Suppose that $d^{2^i} \equiv 1 \pmod{n}$, that is $d^{2^i} = mn + 1$, for some $m \in \mathbb{Z}$. Taking this modulo d, we then have that $0 \equiv 1 \pmod{d}$ and since $d \neq 1$, we have a contradiction. Now suppose that $d^{2^i} \equiv 0 \pmod{n}$, that is $n | d^{2^i}$. Since $\frac{n}{d} | n$, we then have that $\frac{n}{d} | d^{2^i}$, which contradicts $\gcd\left(d, \frac{n}{d}\right) = 1$.

Thus neither 0 or 1 are in $\{\delta_i \mid i \in \mathbb{N}\}$. Since everything in $\{\delta_i \mid i \in \mathbb{N}\}$ is a multiple of d and not 0, there are $\frac{n}{d} - 1$ possibilities for δ_i's values. Thus, by the Pigeonhole Principle, there must be some $s < \frac{n}{d}$ such that $\delta_{\frac{n}{d}} = \delta_s$. Thus, we can generate the following game.

$$\begin{bmatrix} d^{2^s} & d^{2^s} & d^{2^s} & d^{2^s} \end{bmatrix} \mapsto \begin{bmatrix} d^{2^{s+1}} & d^{2^{s+1}} & d^{2^{s+1}} & d^{2^{s+1}} \end{bmatrix} \mapsto \cdots \mapsto \begin{bmatrix} d^{2^s} & d^{2^s} & d^{2^s} & d^{2^s} \end{bmatrix}.$$

We therefore have a cycle whose length is at most $\frac{n}{d} - 1$. □

We will now prove the converse of Theorem 7. Let T be a 4-tuple in a cocomposite cycle modulo p^k. It is then clear that each element of T must be multiples of p. Let S be the 4-tuple that is $\lceil \log_2 k \rceil$ steps later in T's cycle. It is then clear that all elements of S must be a multiple of p^k, and thus $S \equiv \begin{bmatrix} 0 & 0 & 0 & 0 \end{bmatrix} \pmod{n}$. Since we know that the length of any cycle containing $\begin{bmatrix} 0 & 0 & 0 & 0 \end{bmatrix}$ is 1, it must be the case that T is also $\begin{bmatrix} 0 & 0 & 0 & 0 \end{bmatrix}$ and so the cycle we started with was trivial. We have then proven the following corollary.

Corollary 1. *There is a nontrivial cocomposite cycle modulo n if and only if n is not a power of a prime.*

Interestingly, the fact that these are cycles of specifically 4-tuples is not needed in this proof. A very similar argument can show that there exists a nontrivial cocomposite cycle of t-tuples modulo n if and only if n is a power of a prime, where t is some positive integer.

5. Coprime Cycles

As was the case for cocomposite cycles, coprime cycles exist for almost all n. Indeed we can give a method to explicitly generate cycles using the following theorem.

Theorem 8. *If $\lambda(n)$ is not a power of 2, then there is some nontrivial coprime cycle modulo n.*

Proof. Let d be an odd nontrivial divisor of $\lambda(n)$ and let $k = \frac{\lambda(n)}{d}$. Also define σ to be the smallest positive integer such that $2^\sigma \equiv \pm 1 \pmod{d}$. Note that it follows that σ either equals $o_d(2)$ or $\frac{1}{2}o_d(2)$. Since $d \neq 1$, we know that $\lambda(n) \nmid k$. By the definition of $\lambda(n)$, there must then be some α coprime to n such that $\alpha^k \not\equiv 1 \pmod{n}$. This ensures that our starting configuration is not equivalent to $\begin{bmatrix} 1 & 1 & 1 & 1 \end{bmatrix}$. If we begin with an initial 4-tuple of the form $\begin{bmatrix} 1 & \alpha^k & 1 & \alpha^{-k} \end{bmatrix}$, the game proceeds as the following sequence of 4-tuples.

$$\begin{bmatrix} 1 & \alpha^k & 1 & \alpha^{-k} \end{bmatrix} \mapsto \begin{bmatrix} \alpha^k & \alpha^k & \alpha^{-k} & \alpha^{-k} \end{bmatrix} \mapsto \begin{bmatrix} \alpha^{2k} & 1 & \alpha^{-2k} & 1 \end{bmatrix},$$

which is equal to the initial 4-tuple but with each entry squared, up to equivalency. So after 2σ steps, we get

$$\begin{bmatrix} 1 & \alpha^{2^\sigma k} & 1 & \alpha^{-2^\sigma k} \end{bmatrix}.$$

Then by the definition of k, we can rewrite this as

$$\begin{bmatrix} 1 & \alpha^{\frac{2^\sigma}{d}\lambda(n)} & 1 & \alpha^{-\frac{2^\sigma}{d}\lambda(n)} \end{bmatrix}.$$

By definition of σ, $2^\sigma = jd \pm 1$ for some integer j, so we rewrite it again as

$$\begin{bmatrix} 1 & \alpha^{\frac{jd\pm 1}{d}\lambda(n)} & 1 & \alpha^{\frac{-jd\mp 1}{d}\lambda(n)} \end{bmatrix} = \begin{bmatrix} 1 & \alpha^{j\lambda(n)\pm\frac{\lambda(n)}{d}} & 1 & \alpha^{-j\lambda(n)\mp\frac{\lambda(n)}{d}} \end{bmatrix}.$$

By definition of $\lambda(n)$, we then know that, modulo n, this is equivalent to

$$\left[1 \quad \alpha^{\pm\frac{\lambda(n)}{d}} \quad 1 \quad \alpha^{\mp\frac{\lambda(n)}{d}}\right].$$

Plugging k back in, we then have a 4-tuple equivalent to the initial 4-tuple (up to symmetry),

$$\left[1 \quad \alpha^{\pm k} \quad 1 \quad \alpha^{\mp k}\right].$$

Since we iterated 2σ steps, we have a cycle of length 2σ. So we have therefore shown that there exists a nontrivial coprime cycle modulo n whose length is either $o_d(2)$ or $2o_d(2)$. □

In our next theorem, we will show that this is the strictest condition on n to guarantee a nontrivial coprime cycle possible.

Theorem 9. *If $\lambda(n)$ is a power of 2, then there are no nontrivial coprime cycles modulo n.*

Proof. Let $\lambda(n) = 2^L$ for some $L \in \mathbb{N}$. Suppose $\left[a \quad b \quad c \quad d\right]$ is in a coprime cycle modulo n. Then, we know from Theorem 6.3 that there is a (possibly different) constant cycle containing $\left[\delta \quad \delta \quad \delta \quad \delta\right]$, where $\delta \equiv ac \equiv bd \pmod{n}$. The game for $\left[\delta \quad \delta \quad \delta \quad \delta\right]$ proceeds as the following sequence.

$$\left[\delta \quad \delta \quad \delta \quad \delta\right] \mapsto \left[\delta^2 \quad \delta^2 \quad \delta^2 \quad \delta^2\right] \mapsto \left[\delta^4 \quad \delta^4 \quad \delta^4 \quad \delta^4\right] \mapsto \cdots$$

Thus, if the length of the new cycle is γ, we know that $\delta^{2^\gamma} \equiv \delta \pmod{n}$. Since δ is coprime to n, we can multiply both sides by δ^{-1} to obtain

$$\delta^{2^\gamma - 1} \equiv 1 \pmod{n}.$$

Briefly suppose for the sake of contradiction that $\delta \not\equiv 1 \pmod{n}$. Then by Lemma 10 (below), $\gcd(2^\gamma - 1, \lambda(n)) > 1$. Since $\lambda(n)$ is a power of 2, it has no odd factors whereas $2^\gamma - 1$ must have only odd factors. We therefore have a contradiction. It must therefore be the case that

$$\delta \equiv ac \equiv bd \equiv 1 \pmod{n}.$$

That is, $c \equiv a^{-1}$ and $d \equiv b^{-1}$. The game for $\left[a \quad b \quad c \quad d\right]$ then continues in the following sequence.

$$\left[a \quad b \quad a^{-1} \quad b^{-1}\right] \mapsto \left[ab \quad a^{-1}b \quad a^{-1}b^{-1} \quad ab^{-1}\right] \mapsto \left[b^2 \quad a^{-2} \quad b^{-2} \quad a^2\right].$$

This is equivalent to the initial 4-tuple, but everything is squared. Continuing the game for $2L$ many more steps, we arrive at a 4-tuple equivalent (after shifting and reversing the 4-tuple) to

$$\left[a^{2^L} \quad b^{2^L} \quad a^{-2^L} \quad b^{-2^L}\right] = \left[a^{\lambda(n)} \quad b^{\lambda(n)} \quad a^{-\lambda(n)} \quad b^{-\lambda(n)}\right] = \left[1 \quad 1 \quad 1 \quad 1\right].$$

Thus, from Lemma 3 and the fact that $\begin{bmatrix}1 & 1 & 1 & 1\end{bmatrix}$ is in a cycle of length 1,

$$a \equiv b \equiv c \equiv d \equiv 1 \pmod{n},$$

and so the only coprime cycle modulo n is $\begin{bmatrix}1 & 1 & 1 & 1\end{bmatrix}$. □

Lemma 10. *If $\alpha \in \mathbb{Z}_n^\times \setminus \{1\}$ and $\alpha^k \equiv 1 \pmod{n}$, then $\gcd(k, \lambda(n)) > 1$.*

Proof. Since $\alpha \not\equiv 1$, it is clear that $o_n(\alpha) > 1$. We write $k = mo_n(\alpha) + b$, where m and b are integers and $0 \le b < o_n(\alpha)$. Then

$$1 \equiv \alpha^k = \alpha^{mo_n(\alpha)+b} = \alpha^{mo_n(\alpha)}\alpha^b \equiv \alpha^b \pmod{n}.$$

If $b \neq 0$, this would contradict $o_n(\alpha)$ being the minimal positive integer with its defining property. It must therefore be the case that $o_n(\alpha)|k$. Since $\alpha^{\lambda(n)}$ is also congruent to 1, we can use a similar process to arrive at $o_n(\alpha)|\lambda(n)$. We have therefore shown that $\gcd(k, \lambda(n)) \ge o_n(\alpha) > 1$. □

Taking Theorem 8 and Theorem 9 together, we may prove the following theorem.

Theorem 11. *There is a nontrivial coprime cycle modulo n if and only if $\lambda(n)$ is not a power of 2.*

In fact, this theorem can easily be generalized for a game acting on a given abelian group, as very few parts of the structure of $\mathbb{Z}_n^\times$ were used in the relevant proofs. So we can state (without proof as it would be a retreading of the majority of this paper) the following corollary.

Corollary 2. *Suppose that $G = (S, \cdot)$ is an abelian group with a finite exponent. Then the iterations of the endomorphism in G^4 that maps*

$$\begin{bmatrix}a & b & c & d\end{bmatrix} \mapsto \begin{bmatrix}a \cdot b & b \cdot c & c \cdot d & d \cdot a\end{bmatrix}$$

may enter a cycle other than the length 1 cycle consisting of the 4-tuple of G's identity if and only if the exponent of G is not a power of 2.

Note that Corollary 2 does not only apply to finite abelian groups; it only requires that the exponent of the group must be finite. For example, Corollary 2 tells us that when $G = (\mathbb{Z}_4[[x]], +)$, the game in G^4 does not have any nontrivial cycles. Whereas if G were equal to $\left(\mathbb{Z}_{24}\left[x, y\right]/\left\langle x^6 - 9xy\right\rangle, +\right)$ then G^4 does have nontrivial cycles when the game is played.

We can then see that Theorem 1 drops out as a corollary of Theorem 11 and Corollary 1 since if $\lambda(n)$ is a power of 2, then n is some power of 2 times a product of distinct Fermat primes. But if n itself is a power of a prime, that only leaves n as either a power of 2 or a Fermat prime. And we therefore have a proof of Theorem 1. So now we shall turn to additional facts about the structure of these cycles.

6. Speed of Convergence

Now that we know those n for which all 4-tuples converge to a trivial cycle, the question arises: how fast do they converge?

Theorem 12. *If there are only trivial cycles modulo n, any starting position will take at most $1 + 3\log_2 \lambda(n)$ steps until it reaches a trivial cycle.*

Proof. Suppose our initial 4-tuple is $\begin{bmatrix} a_1 & b_1 & c_1 & d_1 \end{bmatrix}$, not necessarily in a cycle. We will use subscripts to indicate in which step of the game a 4-tuples occurs. We will proceed by cases.

`Case 1.` Suppose at least one of a_1, b_1, c_1, and d_1 are in $\mathbb{Z}_n \setminus \mathbb{Z}_n^\times$. Then we know from the method developed from Lemma 2 that 4 steps later, all elements of the 4-tuple will share a factor with n. Since there are no nontrivial cocomposite cycles, we know from Corollary 1 that $n = p^k$, for some prime p and positive integer k. Then, a_4, b_4, c_4, and d_4 are all multiples of p. Similarly a_5, b_5, c_5, and d_5 will all be multiples of p^2, and $\lceil \log_2 k \rceil$ many steps later, all entries will be a multiple of p^k. That is, in $4 + \left\lceil \log_2 \log_p n \right\rceil \leq 4 + \lceil \log_2 \log_2 n \rceil$ steps, the 4-tuple will converge to $\begin{bmatrix} 0 & 0 & 0 & 0 \end{bmatrix}$.

`Case 2.` This proof will follow a similar structure to Theorem 9. Suppose a_1, b_1, c_1, and d_1 are all coprime to n. The next step of the game will be:

$$\begin{bmatrix} a_1 & b_1 & c_1 & d_1 \end{bmatrix} \mapsto \begin{bmatrix} a_2 & b_2 & c_2 & d_2 \end{bmatrix} \equiv \begin{bmatrix} a_1b_1 & b_1c_1 & c_1d_1 & a_1d_1 \end{bmatrix}.$$

Consider the product $\delta_i = a_ic_i \equiv b_id_i \pmod{n}$, for $i \geq 2$. We will now show that δ_i will converge to 1. We will proceed by induction. For the base case, $i = 2$, we already know that

$$\delta_i \equiv \delta_2^{2^{i-2}} \pmod{n}.$$

Suppose that $\delta_i \equiv \delta_2^{2^{i-2}} \pmod{n}$ for an arbitrary $i \geq 2$. We want to show that $\delta_{i+1} \equiv \delta_2^{2^{i-1}}$. We then have that

$$\delta_{i+1} = a_{i+1}c_{i+1} = a_ib_ic_id_i = \delta_i^2 = \delta_2^{2^{i-1}}.$$

In particular, if $s = 2+\log_2 \lambda(n)$, which we know must be an integer from Theorem 9, then

$$a_sc_s \equiv b_sd_s \equiv \delta_s \equiv \delta_2^{\lambda(n)} \equiv 1 \pmod{n}.$$

The game then continues as follows:

$$\begin{bmatrix} a_s & b_s & a_s^{-1} & b_s^{-1} \end{bmatrix} \mapsto \begin{bmatrix} a_sb_s & a_s^{-1}b_s & a_s^{-1}b_s^{-1} & a_sb_s^{-1} \end{bmatrix} \mapsto \begin{bmatrix} b_s^2 & a_s^{-2} & b_s^{-2} & a_s^2 \end{bmatrix}.$$

This is equivalent to the sth step, with each element squared. Thus for each $r \in \mathbb{N}$, we can see that

$$\begin{bmatrix} a_{s+2r} & b_{s+2r} & c_{s+2r} & d_{s+2r} \end{bmatrix} \equiv \begin{bmatrix} a_s^{2^r} & b_s^{2^r} & a_s^{-2^r} & b_s^{-2^r} \end{bmatrix} \pmod{n}.$$

In particular, $2\log_2 \lambda(n)$ iterations after s, we will arrive at the 4-tuple,

$$\begin{bmatrix} a^{\lambda(n)} & b^{\lambda(n)} & a^{-\lambda(n)} & b^{-\lambda(n)} \end{bmatrix}.$$

By the definition of $\lambda(n)$, this 4-tuple is equivalent to $\begin{bmatrix} 1 & 1 & 1 & 1 \end{bmatrix}$. Thus, it will take at most $1 + 3\log_2 \lambda(n)$ steps to converge to $\begin{bmatrix} 1 & 1 & 1 & 1 \end{bmatrix}$.

Thus, no matter what is selected for the initial 4-tuple, the game will take at most $\max\left(4+\lceil \log_2 \log_2 n \rceil, 1 + 3\log_2 \lambda(n)\right)$ steps to reach a trivial cycle. Since there are only trivial cycles modulo n, we know from Theorem 1 that n is either a Fermat prime or a power of 2. For each of these cases, it is clear that $1 + 3\log_2 \lambda(n) \geq 4 + \lceil \log_2 \log_2 n \rceil$ except for when $n = 3$. However, the $n = 3$ case is small enough to check by hand and one may verify that it takes at most $4 = 1 + 3\log_2 \lambda(3)$ steps for any 4-tuple to converge to a trivial cycle. The reason for this discrepancy is that the substituting of $\log_p$ for $\log_2$ in Case 1 enlarges the bound more than needed but this is the only term where it matters. Without this substitution, we indeed get that it will take 4 steps for any 4-tuple to reach a trivial cycle modulo 3. As such, we may obtain a bound of simply $1 + 3\log_2 \lambda(n)$ for any n. □

Table 1 shows how many steps it takes for an arbitrary 4-tuple to reach a trivial cycle for the moduli that only have trivial cycles. As we did in Corollary 2, we can generalize these results from Case 2 quite well to abelian groups with finite exponents. If the game is played on a group G^4, then any 4-tuple will take at most $1 + 3\log_2 \lambda(G)$ many steps to converge to the 4-tuple of G's identity if there are no other cycles, where $\lambda(G)$ here represents the exponent of G.

Modulus	Steps
1	0
2	4
3	4
4	5
5	7
17	13
257	25
65537	49
2^k	$3k - 5$

Table 1: The maximum number of steps needed to reach a trivial cycle in each modulus given by Theorem 12. The number k may be any integer greater than or equal to 3.

In Figure 2, we show a tree of all 4-tuples modulo 5 in which each vertex represents a 4-tuple (up to symmetry) and vertices are connected by an edge if playing the game on one of them may reach the other. Notice that it takes each tuple at most 7 steps to reach a trivial 4-tuple, which are indicated by hollow vertices. The

tree on the left corresponds to Case 1 and the tree on the right corresponds to Case 2.

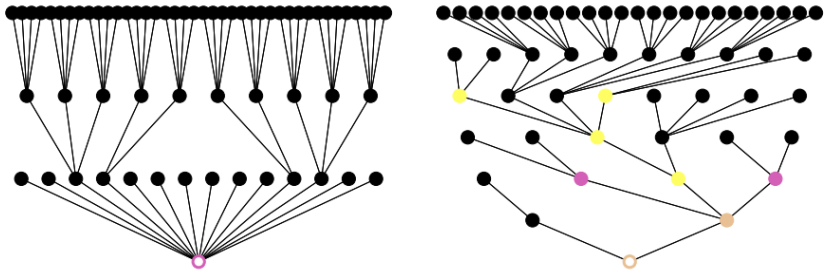

Figure 2: The trees of all 4-tuples (up to symmetry) and their iterations when the game is played modulo 5. The edges each represent playing the game on the upper node, which results in the lower node. Note how all tuples converge to a trivial cycle (indicated by hollow vertices) in up to 7 steps. The purple vertices indicate that the 4-tuple is constant and the yellow vertices represent 4-tuples that are of the form $\begin{bmatrix} x & y & x^{-1} & y^{-1} \end{bmatrix}$ for some $x, y \in \mathbb{Z}_5^\times$. The tuples that fall under both categories are a mix of both colors.

7. Factoring Cycles

Finally we shall turn to factoring the cycles. Specifically, we are going to show that every cycle can be expressed as a product of a constant cycle and a generalization of the type of cycle used in Theorem 8. We shall define a *generator* 4*-tuple* as a 4-tuple of the form $\begin{bmatrix} 1 & x & 1 & x^{-1} \end{bmatrix}$ that is in a cycle, where $x \in \mathbb{Z}_n^\times$. A cycle containing generator 4-tuples will be referred to as a *generator cycle*. Note that every second step in a generator cycle will be a generator 4-tuple.

Theorem 13. *Every coprime cycle is a product of a constant cycle and two generator cycles.*

Proof. Let $I = \begin{bmatrix} a & b & c & d \end{bmatrix}$ be in a coprime cycle. We know that it must be the case from Theorem 6 that $\begin{bmatrix} abcd & abcd & abcd & abcd \end{bmatrix}$, $\begin{bmatrix} 1 & a^{-1}c & 1 & ac^{-1} \end{bmatrix}$, and $\begin{bmatrix} bd^{-1} & 1 & b^{-1}d & 1 \end{bmatrix}$ are all in cycles. Let A, B, and C each be the 4-tuples that are two steps earlier in each of these cycles, respectively. Specifically, A, B, and C are the 4-tuples themselves and not their equivalence class from shifting and reversing the tuples since we will need to multiply these. We then define

$$G = A \times B \times C,$$

which we know from Lemma 4 must be in a cycle. Using the methods in that lemma's proof, we see that by iterating the game for G twice, we obtain

$$\begin{bmatrix} abcd & abcd & abcd & abcd \end{bmatrix} \times \begin{bmatrix} 1 & a^{-1}c & 1 & ac^{-1} \end{bmatrix} \times \begin{bmatrix} bd^{-1} & 1 & b^{-1}d & 1 \end{bmatrix} = \begin{bmatrix} ab^2c & bc^2d & acd^2 & a^2bd \end{bmatrix}.$$

However, this is exactly the same as the second step of iterating I's game. Since I and G are both in cycles, it must be the case that they are in the same cycle. Since they each result in the same 4-tuple in two steps of the game, it must be the case that $I = G$, that is

$$\begin{bmatrix} a & b & c & d \end{bmatrix} = A \times B \times C.$$

We know from Lemma 3 that A must be a constant 4-tuple. It is clear from iterating a generator 4-tuple twice that every even step will also be a generator 4-tuple. Thus, B and C are both generator 4-tuples. We have therefore shown that any 4-tuple in a cycle is a product of a constant 4-tuple and generator 4-tuples, each in a cycle. □

The basis given in the previous theorem is particularly nice as constant cycles' and generator cycles' iterations within this game are quite regular, with constant cycles squaring with every iteration and generator cycles squaring with every second iteration. Decomposing 4-tuples in a cycle in this manner allows us to find the i-th step quite easily, even if we do not know what other 4-tuples in its cycle are. In addition, as is routine with our theorems regarding the coprime cycles, Theorem 13 can also be easily generalized into games on abelian groups with finite exponents. We leave this as an exercise for the interested reader. Experimentally, Theorem 13 also seems to hold for cocomposite cycles as well.

Conjecture 1. Every cocomposite cycle is a product of a constant cycle and two generating cycles.

This conjecture has been verified for all moduli up to 161. One possible direction of proving this conjecture is to show that all cocomposite cycles are a product of a cocomposite constant cycle and a coprime cycle, but we have been unsuccessful on this front.

8. Conclusion

Taking Corollary 1 and Theorem 11 together, we therefore establish our main theorem from the start of the paper, that is, that every modulus excluding powers of 2 and the Fermat primes 3, 5, 17, 257, and 65537 (see Boklan and Conway [2]) has some nontrivial cycle. Additionally, if they exist, we give an explicit form of at least one nontrivial coprime cycle (Theorem 8) and a nonexplicit method of creating a

nontrivial cocomposite cycle (Theorem 7). Furthermore, we obtain an upper bound on how many steps it takes for a given 4-tuple to fall into a trivial cycle in the case that no nontrivial cycles exist. We have also shown that all coprime cycles can be factored into much simpler cycles. Finally, we have been able to generalize almost all of these results to abelian groups with finite exponents.

Acknowledgements. We would like to acknowledge Matthew Helmer, Arianna Koch, Brendan Perez, and Denis Selyuzhitski for their encouragement and creating a nice space to work alongside them. In addition, we would like to thank the directors of the CC-REU, Dr. Sooie-Hoe Loke and Dr. Brandy Wiegers for providing instruction and resources for this research. This work was supported by the CC-REU NSF summer REU experience (DMS: 2050692).

References

[1] A. Behn, C. Bribs-Zaleta, and V. Ponomarenko, The convergence of difference boxes, *Amer. Math. Monthly* **112** (2005), 426–439.

[2] K. D. Boklan and J. H. Conway, Expect at most one billionth of a new Fermat prime!, *Math. Intelligencer* **39** (2017), 3–5.

[3] N. J. Calkin, J. G. Stevens, and D. M. Thomas, A characterization for the length of cycles of the n-number Ducci game, *Fibonacci Quart.* **43** (2005), 53–59.

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

[5] B. Freedman, The four number game, preprint, `arXiv:1109.0051`

[6] A. L. Ludington, Length of the 7-number game, *Fibonacci Quart.* **26** (1988), 195–204

[7] D. Ullman, More on the four-numbers game, *Math. Mag.* **65** (1992), 170–174

[8] W. C. Yueh and S. S. Cheng, Quadruples in the four-number game with large termination times, *Internat. J. Math. Ed. Sci. Tech.* **33** (2002), 879–891