FIBONACCI RANDOM GENERATOR AND FOURIER ANALYSIS

ETHAN BOGLE, OWEN BRASS, AND OWEN SHEN

ABSTRACT. The existing literature on the convergence efficiency of the Fibonacci random generator $X_{n+1} = X_n + X_{n-1} + \epsilon$ shows that the number of steps required for this system to reach equilibrium is at most $5(\log m)^2$. We first show, using Fourier Analysis, that a sufficient number of steps is actually $1.18(\log m)^2$. We also identify the limiting factor in the Fourier Analysis approach, and present a possible way to improve the result to something better than $c(\log m)^2$. This ultimately revolves around the poorly studied distribution of Fibonacci-type sequences mod m. We study some aspects of the Fibonacci distribution when m is a power of 3 and find that, even with a deeper understanding of its behavior, the Fourier Analysis approach seems to be an insufficient tool for attaining a bound which is of smaller order than $(\log m)^2$. We furthermore present several computationally-supported conjectures, particularly when m is a Lucas Number, in the hopes of spurring further research in this area. Then, we consider few special choices of the state space and argue for some better bounds on those particular cases. Finally, we formulate some general results and conjectures, with additional algebraic techniques, to discuss future approaches to understand this Fibonacci random generator.

CONTENTS

1. Introduction

The central goal of this paper is to discuss the convergence rate of a stochastic system known as the Fibonacci random generator, $X_{n+1} = X_n + X_{n-1} + \epsilon_{n+1}$, to its limiting distribution. In particular, we want to find the upper bound of the asymptotic convergence efficiency of this Fibonacci random generator to a uniform random variable. The paper will be organized with the following structure: in Section 2: Countable Markov Chain, we review certain key properties and notations of probability theory; in Sections 3 and 4: Fourier Analysis and Convergence Rate, we discuss how to apply Fourier transform to our existing problem; in Section 5: The CDG Process, we demonstrate how to apply the result from Sections 3 and 4 to a process known as the CDG process, $X_n = 2X_{n-1} + \epsilon_n$, which is the precursor of the Fibonacci random generator we are interested in analyzing; in Section 6: Fibonacci Random Generator, we will present the existing results and its proof strategies of said generator; in Section 7: Improvement Over Existing Fourier Bound, we will introduce our first result on how to improve the existing bound for the Fibonacci system from $5(\log m)^2$ to $1.18(\log m)^2$; in Section 8: Special Case with Modulus 3^k, we consider the state spaces whose size is a power of three and discuss how we may gain a deeper understanding of the Fibonacci distribution on such spaces, but ultimately find that such this understanding is insufficient to give a bound which is of a smaller order than $(\log m)^2$; finally, in Section 9: The Fibonacci Distribution Problem, we contextualize our problem into the larger algebraic literature of Fibonacci Distribution and discuss its implications. Section 9 is developed in a more general framework so that its understanding does not require the rest of the paper.

2. Countable Markov Chain

Let us review few propositions of countable Markov Chains and go through our choice of notations for this paper. The countable Markov Chain is a stochastic process on a countable state space that satisfies the Markov Property illustrated below:

$$\mathbf{P}\left\{X_{t+1} = y \mid X_i = x_i, i < t\right\} = \mathbf{P}\left\{X_{t+1} = y \mid X_t = x\right\} = P(x, y).$$

Here, we use the standard notation of the transition kernel $P(i, j)$ of a finite state space Markov Chain on the state space $(i, j, k, \cdots)$ which we shall call $\mathcal{X}$. In this paper, we focus on the state space of $\mathbb{Z}_m$, the integers mod m. The transition kernel is not only encoding the transition probability but is also a matrix, so it makes sense to write $P^t(i, j)$ for some integer t. We can check that

$$\mathbf{P}_x\left\{X_t = y\right\} = P^t(x, y).$$

That is, the probability of moving in t steps from x to y is given by the (x, y) -th entry of P^t. We call these entries the t -step transition probabilities.

Two often used conditions on countable markov chain are the irreducibility and the aperiodicity. Irreducibility means for any pair of $(x, y) \in \mathcal{X} \times \mathcal{X}$, there exists an integer t such that $P^t(x, y)$ is nonzero. Intuitively, it means every state of the chain is accessible from any point, provided with sufficient time. To define aperiodicity, let us first consider the return period as $\mathcal{T}(x) := \{t \geq 1 : P^t(x, x) > 0\}$. Hence, the period of the whole chain is the greatest common divisor of $\mathcal{T}(x)$ for all $x \in \mathcal{X}$. Aperiodicity in this context means the period is one. Aperiodicity is important in the context of mixing. Let us consider the simple example of a simple random walk of $X_i = \sum_{j=1}^{i} \xi_j$ on a group of even order, say 10, where $\xi(1) = \xi(-1) = 0.5$. Then, this chain will not converge well to, say a uniform, because we may check that the states accessible from even steps are disjoint from the states accessible from odd steps.

Another important concept of Markov Chain is its stationary distribution, for which we use the natural notation π for the stationary (equilibrium) distribution. The matrix definition is that π is the vector that satisfies $\pi = \pi P$. The equivalent definition is that

$$\pi(y) = \sum_{x \in \mathcal{X}} \pi(x) P(x, y) \quad \text{for all } y \in \mathcal{X}.$$

Hence, once the chain hits the stationary distribution, the chain will stay at the stationary distribution. The natural question to ask is whether such a stationary distribution exists and whether the existence is unique. Then, let us briefly summarize few propositions about those three concepts, irreducibility, aperiodicity, and stationary distribution and address our concerns here.

Proposition 2.1. *If P is aperiodic and irreducible, then there is an integer r_0 such that $P^r(x, y) > 0$ for all $x, y \in \mathcal{X}$ and $r \geq r_0$.*

Proposition 2.2. *Let P be the transition matrix of an irreducible Markov chain. There exists a unique probability distribution π satisfying $\pi = \pi P$.*

The concept of stationary distribution is central to the discussion of this paper.

3. Fourier Analysis and Convolution

In this section, we will cover all of the background materials of Fourier Analysis needed to understand the strategies in the subsequent sections. Let us first review some basics about Fourier transforms on finite groups.

Definition 3.1. The Fourier transform of $f : \mathbb{Z}_m \to \mathbb{C}$ in the frequency $k \in \mathbb{Z}_m$ is given by

$$\widehat{f}(k) = \sum_{t=0}^{m-1} f(t) e^{-2\pi i k t / m}.$$

The Fourier transform represents the original function in a frequency domain, where the analysis of the function may be easier. An often used simplification is that, for $\theta \neq 0$, we have

$$\sum_{t=0}^{m-1} e^{it\theta} = \frac{1 - e^{im\theta}}{1 - e^{i\theta}}. \tag{3.1}$$

We can compute the Fourier transform of a uniform distribution π on $\mathbb{Z}_m$ as

$$\widehat{\pi}(0) = \sum_{t=0}^{m-1} \frac{1}{m} e^{-2\pi i 0t/p} = \sum_{t=0}^{m-1} \frac{1}{m} = 1$$

and

$$\widehat{\pi}(k) = \sum_{t=0}^{m-1} \frac{1}{m} e^{-2\pi ikt/m} = \frac{1}{m} \frac{1-e^{im\theta}}{1-e^{i\theta}} = \frac{1}{m} \frac{1-e^{-2\pi ki}}{1-e^{-2\pi ik/m}} = 0.$$

Intuitively, the closer a random variable is to the uniform, the more the Fourier transform tends to have a peak in zero state and a small value in non-zero state. For the singular distribution δ_s at $s \in \mathbb{Z}_m$, we have

$$\widehat{\delta_s}(k) = e^{-2\pi iks/m}.$$

Hence, to sum up the intuitive interpretation of Fourier transform, if the random variable has a peak only at zero, then its Fourier transform behaves more like uniform. If it has peaks everywhere, its transform behaves more like singular. The power of discrete Fourier transform is that it is universally applicable:

Proposition 3.2. *Any function $f : \mathbb{Z}_m \to \mathbb{C}$ has the following Fourier expansion:*

$$f(t) = \frac{1}{m} \sum_{k=0}^{m-1} \widehat{f}(k) e^{2\pi ikt/m}, \quad t \in \mathbb{Z}_m.$$

The reverse operation to the Fourier transform is the Inverse Fourier Transform denoted by $g : \mathbb{Z}_m \to \mathbb{C}$ and defined by

$$\check{g}(t) := \frac{1}{m} \sum_{k=0}^{p-1} g(k) e^{2\pi ikt/m}, \quad t \in \mathbb{Z}_m.$$

So we should expect the following proposition:

Proposition 3.3. *If $f : \mathbb{Z}_p \to \mathbb{C}$, then*

$$\widehat{\check{g}}(t) = \check{\widehat{g}}(t) = g(t).$$

One very nice property of the Fourier transform is that it preserves the norm:

Proposition 3.4. *(Plancherel's Theorem) If $f, g : \mathbb{Z}_p \to \mathbb{C}$, then*

$$\langle f, g \rangle = \frac{1}{p} \langle \widehat{f}, \widehat{g} \rangle.$$

In particular, the L^2 norm can be expressed as

$$\|f\|_2 = \frac{1}{\sqrt{p}} \|\widehat{f}\|_2.$$

The Fourier transform is often used in conjunction with the *convolution*, which is defined by:

Definition 3.5. The convolution operator $*$ of two functions f and g is given by

$$(f * g)(t) := \int_{-\infty}^{\infty} f(\tau) g(t-\tau) d\tau.$$

One can quickly check that the convolution is commutative. Since we are only interested in the discrete case, we can naturally replace the definition by summation instead. The reason for using the convolution along with the Fourier transform is the following:

Proposition 3.6. *(Convolution Theorem) If $f, g : \mathbb{Z}_p \to \mathbb{C}$, then*

$$\widehat{f * g} = \widehat{f}\widehat{g}.$$

Thus far we have reviewed some important properties of the Fourier transform and the convolution. In the next section we will see how to apply some of the ideas in the context of convergence rate.

4. Fourier Transform and Convergence Rate

In this section, we will show how to apply the results established above in the context of stochastic variables. In particular, we will identify an upper bound theorem (4.1) which will be the foundation of the sections which follow.

Theorem 4.1. *Let $\mu : \mathbb{Z}_m \to [0,1]$ be a probability distribution and π is the uniform. Then for all $n \in \mathbb{N}$ we have*

$$\frac{1}{2}\sqrt{\frac{1}{m}\sum_{k\in\mathbb{Z}_m\setminus\{0\}} |\widehat{\mu}(k)|^{2n}} \leq \|\mu^{*n} - \pi\|_{TV} \leq \frac{1}{2}\sqrt{\sum_{k\in\mathbb{Z}_m\setminus\{0\}} |\widehat{\mu}(k)|^{2n}}.$$

The reason for writing μ^{*n} is that after n steps the chain's distribution is just the convolution of μ n times. Let us prove the theorem.

Proof. To prove the upper bound, we may first write the total variation in terms of the summation:

$$4\|\mu^{*n} - \pi\|_{TV}^2 = \left(\sum_{t=0}^{m-1} |\mu^{*n}(t) - \pi(t)|\right)^2$$

Since $\pi(t) = 1/m$ for all $t \in \mathbb{Z}_p$, we have

$$\left(\sum_{t=0}^{m-1} |\mu^{*n}(t) - \pi(t)|\right)^2 = m^2\left(\sum_{t=0}^{m-1} \pi(t)\,|\mu^{*n}(t) - \pi(t)|\right)^2.$$

Now, we can use the inner product by defining

$$f(t) := \pi(t), \quad \text{and} \quad g(t) := |\mu^{*n}(t) - \pi(t)|\,, \quad t \in \mathbb{Z}_p,$$

Then, we use Cauchy-Schwartz Inequality to obtain

$$\left(\sum_{t=0}^{m-1} \pi(t)\,|\mu^{*n}(t) - \pi(t)|\right)^2 = |\langle f, g\rangle|^2 \leqslant \|f\|_2^2\|g\|_2^2. \tag{4.1}$$

Now, we can compute the ℓ^2 norms as

$$\|f\|_2^2 = \sum_{t\in\mathbb{Z}_m} \pi(t)^2 = \sum_{t\in\mathbb{Z}_m} m^{-2} = m^{-1},$$

and by definition of g :

$$\|g\|_2^2 = \sum_{t\in\mathbb{Z}_m} |\mu^{*n}(t) - \pi(t)|^2 .$$

Hence we have proved

$$4\,\|\mu^{*n} - \pi\|_{TV}^2 \leqslant m \sum_{t\in\mathbb{Z}_m} |\mu^{*n}(t) - \pi(t)|^2 = m\,\|\mu^{*n} - \pi\|_2^2 .$$

Now, here is the place we want to demonstrate the power of fourier transform and its ability to preserve the norm: by Plancherel's Theorem, we have that

$$m\,\|\mu^{*n} - \pi\|_2^2 = \left\|\mu^{\widehat{*}} - \pi\right\|_2^2 = \left\|\widehat{\mu^{*n}} - \widehat{\pi}\right\|_2^2 = \sum_{k=0}^{m-1} \left|\widehat{\mu^{*n}}(k) - \widehat{\pi}(k)\right|^2 .$$

Since we know the Fourier transform of the uniform is

$$\widehat{\pi}(k) = \begin{cases} 1, & k = 0 \\ 0, & k \neq 0 \end{cases}$$

On the other hand, as μ^{*n} is a probability distribution, the Fourier transform

$$\widehat{\mu^{*n}}(0) = \sum_{t\in\mathbb{Z}_p} \mu^{*n}(t) = 1.$$

Hence the difference

$$\widehat{\mu^{*n}}(k) - \widehat{\pi}(k) = \begin{cases} 0, & k = 0 \\ \widehat{\mu^{*n}}(k), & k \neq 0 \end{cases}$$

Moreover, by the Convolution Theorem we have

$$\widehat{\mu^{*n}}(k) = \widehat{\mu}(k)^n.$$

Thus

$$\sum_{k=0}^{m-1} \left|\widehat{\mu^{*n}}(k) - \widehat{\pi}(k)\right|^2 = \sum_{k\in\mathbb{Z}_m\setminus\{0\}} |\widehat{\mu}(k)|^{2n}.$$

Hence, the upper bound follows. To prove the lower bound, we only need to modify equation (4.1) and the rest should be the same. In particular, it suffices to show

$$4\,\|\mu^{*n} - \pi\|_{TV}^2 \geq \sum_{t\in\mathbb{Z}_m} |\mu^{*n}(t) - \pi(t)|^2 = \|\mu^{*n} - \pi\|_2^2 ,$$

which is equivalent to show

$$\left(\sum_{t=0}^{m-1} |\mu^{*n}(t) - \pi(t)|\right)^2 \geq \sum_{t\in\mathbb{Z}_m} |\mu^{*n}(t) - \pi(t)|^2 .$$

A direct observation would confirm above inequality. Hence, we can conclude that

$$\frac{1}{2}\sqrt{\frac{1}{m}\sum_{k\in\mathbb{Z}_m\setminus\{0\}} |\widehat{\mu}(k)|^{2n}} \leq \|\mu^{*n} - \pi\|_{TV} \leq \frac{1}{2}\sqrt{\sum_{k\in\mathbb{Z}_m\setminus\{0\}} |\widehat{\mu}(k)|^{2n}}.$$

□

Let us now consider a concrete example of how to apply these bounds. Here, we illustrate a simple random walk on a group as $X_{n+1} \equiv X_n + \varepsilon_n (\text{mod } m)$ where $\varepsilon_n = 0, 1$, or -1, each with probability $\frac{1}{3}$, and $X_0 = 0$. Let us call the distribution of each step as $\epsilon_i \sim \mu(\cdot)$. We want to show that $e^{-\alpha n/m^2} \leq \|P_n - \pi\|_{TV} \leq e^{-\beta n/m^2}$ where π is the uniform distribution and $X_n \sim P_n$.

First, we may compute the Fourier transform as follows:

$$\hat{\mu}(j) = \sum_k q^{kj} \mu(j) = \frac{1}{3} + \frac{2}{3} \cos \frac{2\pi j}{m}.$$

Then, by Theorem 4.1, we can write it as

$$\|P_n - \pi\|_{TV}^2 = \|\mu^{*n} - \pi\|_{TV}^2 \leq \frac{1}{4} \sum_{j \neq 0} \hat{\mu}^{2n}(j) = \frac{1}{4} \sum_{j \neq 0} \left(\frac{1}{3} + \frac{2}{3} \cos \frac{2\pi j}{m} \right)^{2n}.$$

Then, the upper bound can be achieved by using

$$\frac{1}{3} + \frac{2}{3} \cos x \leq e^{-2x^2/9} \qquad \text{for } 0 \leq x \leq \pi/2.$$

For the lower bound, we can use Proposition 4.1 with the choice as

$$f(j) = \cos \frac{2\pi j}{m}.$$

We can verify that $\pi(f) = 0$. In addition, we can write

$$\begin{aligned} P(f) &= \sum_j P_n(j) f(j) \\ &= \sum_j P_n(j) \cos \frac{2\pi j}{m} \\ &= \operatorname{Re} \sum_j P_n(j) e^{\frac{2\pi j}{m}} \\ &= \operatorname{Re} \hat{P}_n(1) = \left(\frac{1}{3} + \frac{2}{3} \cos \frac{2\pi}{m} \right)^n. \end{aligned}$$

To conclude, we use exponential approximation of cosine again to have

$$\|P_n - \pi\| \geq \frac{1}{2} \left(\frac{1}{3} + \frac{2}{3} \cos \frac{2\pi}{m} \right)^n \geq e^{-\alpha N/m^2},$$

where α is some constant. To summarize, we have showed $e^{-\alpha n/m^2} \leq \|P_n - \pi\|_{TV} \leq e^{-\beta n/m^2}$ for a simple random walk on a finite group.

In the following section, we will consider a more complex example of applying this Fourier analysis strategy.

5. The CDG Process

In this section, we will focus on bounding the convergence rate of the system $2X_n = X_{n-1} + \epsilon_n$ to the uniform as defined by the total variation distance with the idea of Fourier transform. This system, known as the CDG process, is the precursor of our Fibonacci random generator, and we are interested in knowing, in the following sections, if the strategies applying to this CDG process can be similarly applied to our Fibonacci random generator. Before that, let us consider the important theorem as an application of the Fourier transform approach. The theorem we are going to prove in this section is the following:

Theorem 5.1. *Suppose X_n satisfies*

$$X_{n+1} \equiv 2X_n + \varepsilon_n (\text{mod } m), \quad X_0 = 0, \ c > 1/\log 9,$$

where $\epsilon_n = 1, 0, -1$ with equal probability of $1/3$. Then for $N \geq c \log m \log\log m$, we have $\|P_N - U\| \to 0$ as $p \to \infty$. In particular, the convergence rate is

$$\|P_N - U\|^2 \leq \frac{1}{2}\left(e^{9^{-d}} - 1\right).$$

In this context, we call that $c \log m \log\log m$ would be "sufficient". This will be the terminology used for the rest of the paper.

Proof. Let us first write the X_n in a more compact form:

$$X_N \equiv \sum_{a=0}^{N-1} 2^{N-1-a} \varepsilon_a (\text{mod} m).$$

Then, recall the addition of random variables is the convolution. We may denote

$$\mu^{(a)}(0) = \mu^{(a)}\left(-2^a\right) = \mu^{(a)}\left(2^a\right) = \frac{1}{3}, \quad 0 \leq a \leq N-1,$$

so that

$$X_N = \mu^{(1)}(\cdot) * \mu^{(2)}(\cdot) \cdots \mu^{(N)}(\cdot).$$

This convenient expression allows up to apply the convolution theorem that simplifies the Fourier transform:

$$\hat{P}_N = \prod_{a=0}^{N-1} \hat{\mu}^{(a)}.$$

Then, according to our upper bound theorem identified in the previous section, we should next bound our total variation distance by the Fourier transform:

$$\begin{aligned}\|P_N - U\|^2 &\leq \frac{1}{4}\sum_{k\neq 0} |\hat{P}(k)|^2 \\ &= \frac{1}{4}\sum_{k\neq 0}\prod_{a=0}^{N-1}\left(\frac{1}{3} + \frac{2}{3}\cos\frac{2\pi 2^a k}{m}\right)^2.\end{aligned}$$

Hence, all that is left is to bound the last term. There are different ways to do the approximation, and here we will use the idea of binary expansion introduced by Chung, Diaconis, and Graham [CDG] for this type of random process. Let us define two functions,

$$g(x) := \left(\frac{1}{3} + \frac{2}{3}\cos 2\pi x\right)^2$$

and the function $h : [0,1] \to \mathbf{R}$ by

$$h(x) = \begin{cases} \frac{1}{9}, & \text{if } x \in \left[\frac{1}{4}, \frac{3}{4}\right), \\ 1, & \text{otherwise.} \end{cases}$$

Function $g(x)$ is exactly the term we are trying the bound for the total variation distance. Our goal is to bound $g(x)$ by $h(x)$. Indeed, $g(x) \leq h(x)$ for $0 \leq x \leq 1$. Then, with $\{x\}$ denoting the fractional part of x, we have

$$\|P_N - U\|^2 \leq \frac{1}{4} \sum_{k \neq 0} \prod_{a=0}^{N-1} h\left(\left\{\frac{2^a k}{m}\right\}\right). \tag{5.1}$$

If we write $x \in [0,1)$ in its binary expansion

$$x = \alpha_1 \alpha_2 \alpha_3, \ldots, \quad \alpha_i = 0 \text{ or } 1 \quad (\text{where } \alpha_i = 0 \text{infinitely often})$$

then

$$h(x) = \frac{1}{9} \quad \text{if and only if } \alpha_1 \neq \alpha_2.$$

For we can check that under binary expansion $10, 01$ mean x is between $[1/2, 1/2 + 1/8]$ and $[1/4, 1/4 + 1/8]$ respectively. The reason for this binary expansion is that we have an exponential term with base 2 in equation (5.1). Thus, if $A_x(N)$ denotes the number of "alternations" in the first N binary digits of x, i.e.,

$$A_x(N) := \left|\{1 \leq i < N : \alpha_i \neq \alpha_{i+1}\}\right|,$$

then

$$\prod_{a=0}^{N-1} h\left(\left\{\frac{2^a k}{m}\right\}\right) = 9^{-A_{k/m}(N+1)}.$$

Let us define the integer t to satisfy

$$2^{t-1} < m < 2^t.$$

We shall choose N to be of the form rt for a large integer $r = r(t)$ to be specified later. Then we want to partition the binary digits. Let us consider the first $N = rt$ digits of the binary expansion of

$$k/p = \alpha_1 \alpha_2 \cdots \alpha_t \alpha_{t+1} \cdots \alpha_{2t} \cdots \alpha_{rt} \cdots .$$

Then, we partition this string into r disjoint blocks $B_{ki}, 1 \leq i \leq r$, each of length t, by defining

$$B_{ki} = \alpha_{(i-1)t+1} \alpha_{(i-1)t+2} \cdots \alpha_{it}$$

Let $A(B_{ki})$ denote the number of alternations in the block B_{ki}. Thus,

$$\prod_{a=0}^{N-1} h\left(\left\{\frac{2^a k}{m}\right\}\right) \leq \prod_{i=1}^{r} 9^{-A(B_{ki})}. \tag{5.2}$$

The inequality sign holds because we ignore the possible alternations between each partitioned string and we only use the first N digits of the sequence. Now, let us observe that for any k ranging over $\mathbb{Z}_m \backslash \{0\}$, the blocks B_{k1} should all be distinct. Moreover, for any $k \in \mathbb{Z}_m \backslash \{0\}$, B_{k1} must have at least one alternation.

Therefore, all B_{k1} have at least one alternation. Since $(2^t, m) = 1$ coprime for any $t \in \mathbb{N}_0$, the set of blocks $\{B_{ki} : 1 \leq k \leq m-1\}$ is the same as $\{B_{2^i k1} : 1 \leq k \leq m-1\}$. By a similar argument, the set $\{B_{2^i k1} : 1 \leq k \leq m-1\}$ must be distinct, and each element must contain at least one alternation. Moreover, since there are only $m-1$ possible combinations of B_{j1} for any j that is not a multiple of m, then $\{B_{ki} : 1 \leq k \leq m-1\}$ is a permutation of $\{B_{k1} : 1 \leq k \leq m-1\}$. In other words, the two sets contain the exact same elements. Now by (5.1) and (5.2), we can write

$$\|P_N - U\|^2 \leq \frac{1}{4} \sum_{k \neq 0} \prod_{i=1}^{r} 9^{-A(B_{ki})}$$

Let us observe the algebraic inequality that if $a \leq a', b \leq b'$, and $0 < \gamma < 1$ then we have

$$\gamma^{a+b'} + \gamma^{a'+b} \leq \gamma^{a+b} + \gamma^{a'+b'}.$$

In our context, each a_i corresponds to $A(B_{k_i})$ and γ corresponds to $1/9$. Then, since $\{B_{ki} : 1 \leq k \leq m-1\}$ are all indentical in i, we want to rearrange them so that every copy of $A(B_{k_1})$ is grouped together. In other words, we have, by successively interchanging pairs of exponents $A\left(B_{ki}\right), A\left(B_{k'i}\right)$

$$\sum_{k \neq 0} \prod_{i=1}^{r} 9^{-A(B_{ki})} \leq \sum_{k \neq 0} 9^{-rA(B_{k1})}. \tag{5.3}$$

Then, we want use the fact that for each element in $\{B_{ki} : 1 \leq k \leq m-1\}$, such element has at least one alternation. In particular, the right-hand side of (5.3) is upper-bounded by summing over all blocks B of length t having at least one alternation:

$$\{9^{-rA(B_{k1})}, 1 \leq k \leq m-1\} \subset \{9^{-rA(B)}, |B| = t, A(B) > 0\}$$

so that

$$\sum_{k \neq 0} 9^{-rA(B_{k1})} \leq \sum_{\substack{\text{length } B = t \\ A(B) > 0}} 9^{-rA(B)}. \tag{5.4}$$

As a result, the right hand term of (5.4) can be approached by the combinatorics method. Let $M(j)$ denotes the number of blocks of length t with exactly j alternations. Then

$$M(j) \leq 2 \begin{pmatrix} t-1 \\ j \end{pmatrix} \leq 2 \begin{pmatrix} t \\ j \end{pmatrix}.$$

Here, we can apply the combinatorics fact that

$$\sum_{j=1}^{t} \begin{pmatrix} t \\ j \end{pmatrix} x^j = (1+x)^t - 1 \leq \left(e^{tx} - 1\right)$$

and we can summarize everything so far by letting $x = 9^{-r}$:

$$\begin{aligned}
\|P_N - U\|^2 &\leq \frac{1}{4}\sum_{k\neq 0} 9^{-rA(B_{k1})} \\
&\leq \frac{1}{4} \sum_{\substack{\text{length } B = t \\ A(B)>0}} 9^{-rA(B)} \\
&\leq \frac{1}{4}\sum_{j=1}^{t} M(j) 9^{-rj} \\
&\leq \frac{1}{2}\sum_{j=1}^{t} \left(\begin{array}{c} t \\ j \end{array} \right) 9^{-rj} \\
&= \frac{1}{2}\left\{ \left(1+9^{-r}\right)^t - 1 \right\} \\
&\leq \frac{1}{2}\left(e^{t9^{-r}} - 1\right).
\end{aligned}$$

Since the choice of r is at out disposal here, we can make

$$r \geq \frac{\log t}{\log 9} + d$$

so that

$$\|P_N - U\|^2 \leq \frac{1}{2}\left(e^{9^{-d}} - 1\right).$$

The last inequality would establish the convergence result as well as the upper bound on convergence rate.

□

In the next section, we will transition to the discussion of Fibonacci random generator of the form $X_{n+1} = X_n + X_{n-1} + \epsilon_{n+1}$. The generator was originally studied by Diaconis and Chatterjee in [2], who proved that the sufficient number of steps for this generator is $5(\log m)^2$ by a five-step argument. The next section will briefly summarize this five-step strategy from [2], and discuss how to improve this strategy to yield a better result.

6. The Fibonacci Generator

Let us first briefly go through the five-step arguments provided by Chatterjee and Diaconis [CD] that concluded an upper bound of $5(\log m)^2$.

(i) The Fibonacci random number generator takes the following form: define a process $X_0, X_1, \dots$ on $\mathbb{Z}_m$ by $X_0 = 0$, $X_1 = 1$ and

$$X_{k+1} = X_k + X_{k-1} + \epsilon_{k+1} \pmod{m}$$

where ϵ_i are independent, taking values 0,1 and -1 with equal probabilities. Let $P_n(j) := \mathbb{P}(X_n = j)$ and $U(j) := 1/m$ for $j \in \mathbb{Z}_m$. The reason that this stochastic process is a Fibonacci random number generator is that if we represent the sequence in the explicit form, the chain can be written as

$$X_n = F_n + F_{n-1}\epsilon_2 + F_{n-2}\epsilon_3 + \cdots F_1\epsilon_n \pmod m$$

with F_k the usual Fibonacci numbers $0, 1, 1, 2, 3, 5, \ldots$ (so $F_5 = 5$).

(ii) Then, we want to Fourier transform this generator

$$\widehat{P}_n(a) = \mathbb{E}\left(e^{2\pi i a X_k/m}\right) = e^{2\pi i a F_n/m} \prod_{b=1}^{n-1} \left(\frac{1}{3} + \frac{2}{3}\cos\left(2\pi a F_b/m\right)\right).$$

And bound the distance by such Fourier transform, according to the upper bound result identified by Theorem 4.1:

$$4\left\|P_n - U\right\|_{TV}^2 \leq \sum_{a=1}^{m-1} \prod_{b=1}^{n-1} \left(\frac{1}{3} + \frac{2}{3}\cos\left(2\pi a F_b/m\right)\right)^2. \tag{6.1}$$

(iii) The third step would be to identify the interval of the form $A = [1/3, 2/3]$. Hence, if $x \in A$, then $\cos(2\pi x) \in [-1, -1/2]$; so if $F_b/n \in A$, then

$$\frac{1}{3} + \frac{2}{3}\cos\left(2\pi a F_b/n\right) \in [-1/3, 0].$$

In other words, in the cases where $F_i \in A$, we can bound the trigonometry function of (6.1) by 9^{-1}; in the other case, we can bound the function by 1. Therefore, we are interested in knowing how many times we can apply this bound of 9^{-1}.

(iv) The next step would be to find the frequency of the occurrences in such an interval. The proposition for this frequency proved by Diaconis and Chatterjee is the following:

Proposition 6.1. *Take any m such that at least one x_i is not divisible by m. Let b_n be the remainder of x_n modulo m. Then, for any j, there is some $j \leq n \leq j + 8 + 3\log_{3/2} m$ such that $b_n \in [m/3, 2m/3]$.*

(v) With this frequency, one will have that, if we let $m' = 8 + 3\log_{3/2} m$, then we get that at least $[(n-1)/m']$ among $aF_1, \ldots, aF_{k-1}$ are in $[m/3, 2m/3]$ modulo m. Combining this with the upper bound lemma, Diaconis and Chatterjee have established that

$$4\left\|P_n - U\right\|_{TV}^2 \leq n 9^{-(n-1)/m'}.$$

After simplification and some numerical calculations, those five steps lead to the following theorem:

Theorem 6.2. *For any $m \geq 22$ and $n = 5\left[(\log m)^2 + c\log m\right]$, $\left\|P_n - U\right\|_{TV} \leq 1.6e^{-c/2}$.*

Therefore, the number of steps required is $(5+\epsilon)(\log m)^2$, where $\epsilon > 0$.

There are not many ways one can improve this bound. Over the five steps, step one and step two are essentially to establish the setting of the strategy. Step five is to combine previous steps using upper bound lemma. The only places one can potentially improve the bound by using this strategy is to improve step three and step four. In particular, one wants to find an optimal choice of interval A and an optimal upper bound on the functions (6.1) formed by the Fourier transform. In the next section, we will show how exactly can we improve this result by focusing on step three and step four.

7. Improvements over existing Fourier Bound

In this section, we will employ a similar argument to Diaconis and Chatterjee's proof [CD] in above section, and conclude with a better bound of $1.18(\log m)2$ steps. In particular, we will consider to bound the trigonometry function by multiple intervals. Let us go through few notations here. The set A is of the form $[m/2 - dm/2, m/2 + dm/2]$ where $d \geq 1/3$. Then, let us denote left-of-A as $A_l := [0, m/2 - dm/2)$, and right-of-A as $A_r := (m/2 - dm/2, 1]$. It is convenient to write

$$\beta = \sup_{x \in A} \left(\frac{1}{3} + \frac{2}{3} \cos(\frac{2\pi x}{m}) \right)^2 .$$

In this section, we use the classical bound on Fibonacci that $F_n \geq (3/2)^n, n \geq 11$. The basic idea of this demonstration is that since Diaconis and Chatterjee identified the worst number of steps taken from any point to reach some interval A, we can potentially improve the bound a little if we consider more intervals and run a similar argument more carefully. The main result of this section is that the strategy we follow is able to show $1.18(\log n)^2$ steps would be sufficient, where the existing bound is of $5(\log n)^2$.

Proposition 7.1. *Let us use b_j denote the F_j mod m. With intervals A_r and A_l so defined above, if two consecutive b_i and b_{i+1} are in the same interval, that is $b_i, b_{i+1} \in A_r$ or $b_i, b_{i+1} \in A_l$, at least some for some $i + 1 \leq j \leq i + 11 + \log_{3/2}(m/2 - dm/2)$ we have $b_j \in A$.*

Proof. Let us observe that by symmetry, a point $x \in A$ if and only if $x^{-1} \in A$. Therefore, it suffices to consider only A_l. Let us recall that since the size of A, or dm, is at least $m/3$, so a Fibonacci sequence of any starting points cannot jump over the inverval A. Therefore, the index of the next point b_j will be bounded according to the classical bound on Fibonacci we identified above. In other words, at least some for some $i + 1 \leq j \leq i + 11 + \log_{3/2}(m/2 - dm/2)$.

□

Proposition 7.2. *Whenever $b_i \in A_r$ and $b_{i+1} \in A_l$, at least for some*

$$i + 1 \leq j \leq i + 12 + \log_{3/2}(m/2 - dm/2)$$

we have either $b_j, b_{j+1} \in A_r$ *or* $b_j, b_{j+1} \in A_l$. *Similarly, whenever* $b_j \in A_r$ *and* $b_{i+1} \in A_l$, *at least some for some*

$$i + 1 \leq j \leq i + 12 + \log_{3/2}(m/2 - dm/2)$$

we have $b_j, b_{j+1} \in A_r$ *or* $b_j, b_{j+1} \in A_l$.

Proof. Intuitively, this proposition determines the number of steps taken to have two consecutive elements falling in the same interval, either in A_r or A_l. By symmetry, it suffices to consider only one case, namely that $b_i \in A_r$ and $b_{i+1} \in A_l$. In particular, it suffices to express the problem in some Fibonacci distance problem and use the classical bound on Fibonacci we identified above.

Let us denote ϵ_1 as $n - 1 - b_i$ and ϵ_2 as b_{i+1}. Intuitively, epsilons denote the distance to the boundary. In particular, one distance to the left boundary and one distance to the right boundary. In general, ϵ_k as $n - 1 - b_{i+k-1}$ and ϵ_{k+1} as b_{i+k-1}, where k is odd. The goal is to find for some consecutive points in the future, one distance becomes negative and the other distance remains positive. In that case, we would have two consecutive points on the same interval, either in A_r or A_l.

Indeed, let us first observe that ϵ_3 can be expressed as $\epsilon_1 - \epsilon_2$ so that $\epsilon_1 = \epsilon_2 + \epsilon_3$. By inductive reasoning, we have $\epsilon_m = \epsilon_{m+1} + \epsilon_{m+2}$. Therefore, the distance declays according to Backwards Fibonacci. Since our goal is to find the worst bound such that this Backwards Fibonacci reaches negative, we consider the longest path from 0 to $\max\{\epsilon_1, \epsilon_2\} \leq (m/2 - dm/2)$, which would take $i + 11 + \log_{3/2}(m/2 - dm/2)$ steps. We add one to this expression for we take consecutive points. As a result, we can conclude that if $b_i \in A_r$ and $b_{i+1} \in A_l$, at least some for some $i + 1 \leq j \leq i + 12 + \log_{3/2}(m/2 - dm/2)$ we have $b_j, b_{j+1} \in A_r$ or $b_j, b_{j+1} \in A_l$.

□

Proposition 7.3. *Whenever* $b_i \in A_r$, *at least some for some*

$$i + 1 \leq j \leq i + 23 + 2\log_{3/2}(m/2 - dm/2)$$

we have $b_j \in A$.

Proof. This would follow from previous two propositions, for two steps after i, the worst case would be either $b_i \in A_r$ and $b_{i+1} \in A_l$, or $b_j \in A_r$ and $b_{i+1} \in A_l$. So the result follows.

□

Finally, let us note that the index for the first element in A is surely bounded by $23 + 2\log_{3/2}(m/2 - dm/2)$, and we are ready to conclude the result. After an identical argument according to the strategy in previous section, we have

$$4\left\|P_n - U\right\|_{TV}^2 \leq m\beta^{[(n-1)/m']},$$

where $m' = 23 + 2\log_{3/2}(m/2 - dm/2)$.

In the case where $A = 1/3$, which is the original choice by Diaconis and Chatterjee, we have

$$4\left\|P_n - U\right\|_{TV}^2 \leq m9^{-[(n-1)/m']}.$$

where $m' = 23 + 2\log_{3/2}(m/3)$. From this expression, one can numerically verify that $2.9(\log m)^2$ steps would be sufficient.

A different choice of d would be $1/2$. The nice property about this choice is that whenever a Fibonacci sequence arrivies at A from either A_r or A_l, the sequence would stay in A for at least two consecutive elements. Therefore, we can derive a similar bound by using

$$4\left\|P_n - U\right\|_{TV}^2 \le m\beta^{[2(n-1)/m']},$$

where $m' = 24 + 2\log_{3/2}(m/4)$ and $\beta = \sup_{x\in[1/4,3/4]}(1/3 + 2/3\cos(2\pi x))^2 = 1/9$. We double the coefficient of $(k-1)$ because the occurrence in A of this particular choice of d will at least appear in pairs; we add one to m' because we shift the index when adding two elements instead of one in A. From this expression, one can numerically verify that $1.4(\log m)^2$ steps would be sufficient.

One can also test a different value of d, say $d = 5/6$. Then whenever a Fibonacci sequence arrives at A from either A_r or A_l, the sequence would stay in A for at least three consecutive elements. Therefore, we can derive a similar bound by using

$$4\left\|P_n - U\right\|_{TV}^2 \le m\beta^{[3(n-1)/m']},$$

where $m' = 25+2\log_{3/2}(m/12)$ and $\beta = \sup_{x\in[1/12,11/12]}(1/3+2/3\cos(2\pi x))^2 < 0.83$. Roughly $10.5(\log m)^2$ steps would be sufficient.

Of course, we can test different values for d and find the optimal choice of d. Moreover, one can combine several d_i and form an even tighter bound. For example, one can count the number of occurrences in $[1/4, 3/4]$, then count the number of occurrences in $[1/12, 11/12] - [1/4, 3/4]$. In general, for a given sequence of $d_1 < d_2 < d_3 \cdots$, the bound can be expressed as

$$4\left\|P_n - U\right\|_{TV}^2 \le m\left(\prod_{i=1}^{j} \beta_i^{[\alpha_i(n-1)/m_i]-\alpha_{i-1}(n-1)/m_{i-1}]}\right)$$

where α_i denotes the number of consecutive occurences in A_i guaranteed by the choice of d_i, $\beta_i = \sup_{x\in[1/2-d/2,1/2+d/2]}(1/3 + 2/3\cos(2\pi x))^2$, and $m_i = 22 + \alpha_i + 2\log_{3/2}(m/2 - d_i m/2)$. Here we have to manually define $\alpha_0 = 0$, for there is nothing to subtract from the first interval d_1.

In the example of combing $d_1 = 1/3, d_2 = 1/2$, we get

$$4\left\|P_n - U\right\|_{TV}^2 \le m(\frac{1}{9})^{[2(n-1)/m_1]}(0.83)^{[3(k-1)/m_2]-[(n-1)/m_2]},$$

where $m_1 = 24 + 2\log_{3/2}(m/12)$ and $m_2 = 25 + 2\log_{3/2}(m/12)$. It could be verified numerically that $1.18(\log m)^2$ steps would be sufficient:

Theorem 7.4. *For a Fibonacci random generator, if $n \ge 1.18(\log m)^2$, we have $\left\|P_n - U\right\|_{TV} \to 0$ as $m \to \infty$.*

Of course one may pursue a more complicated argument that combines more d_i and potentially result in an coefficient that is smaller than 1.18. However, we will not pursue further for we believe the actual bound is much smaller than the order of

$(\log m)^2$ and combining more d_i would not help improving such order. To summarize, the strategy proposed here allows us to improve the efficiency from $5(\log m)^2$, as suggested originally in Diaconis and Chaterjee, to $1.18(\log m)^2$, and it is very possible to even push this coefficiency beyond the threshood of $1(\log m)^2$. However, to look for a much better bound, one should probably take an alternative approach or focus on few nicer cases. Those alternative approaches and the consideration of special cases will be the focus on the remainder of this paper.

8. Special Case with Modulus 3^k

In proving their upper bound on the mixing time of the Fibonacci process, Chatterjee and Diaconis [2] made use of the following estimate:

$$\|P_n - U\|^2 \leq \frac{1}{4}\sum_{a\neq 0}\prod_{b=0}^{n-1}\left(\frac{1}{3}+\frac{2}{3}\cos\left(\frac{2\pi F_b a}{m}\right)\right)^2$$
$$\leq \frac{1}{4}m\left(\frac{1}{9}\right)^{(n-1)/(10\log m)}.$$

Note that the $10\log m$ comes from their estimate that it takes at most $10\log m$ steps for any given Fibonacci sequence to enter the middle interval $[m/3, 2m/3]$. Certainly, something on the order of $\log m$ steps is necessary for *some* starting points of the Fibonacci sequence, seeing as Fibonacci growth with $x_0 = 0$, $x_1 = 1$ is approximately exponential after sufficiently many steps, and $m/3$ grows linearly in m. On the other hand, if we can say that, for *sufficiently many* a, the sequence $aF_b \pmod m$ will reliably enter the middle interval in a smaller number of steps, then a better bound might be possible by breaking up the sum into "efficient" a and "inefficient" a. In fact, gathering more detailed information about the Fibonacci distribution on $\mathbb{Z}/m\mathbb{Z}$ seems to be the only method by which the Fourier analysis estimate approach can provide a bound on the mixing time which is better than some quantity on the order of $(\log m)^2$.

Given this perceived potential for improvement, our goal in this section is to estimate, given $x_0, x_1 \in \mathbb{Z}/m\mathbb{Z}$ (not both 0), how many iterations it takes for the Fibonacci sequence defined by $x_{i+1} = x_i + x_{i-1}$ to enter the interval $[m/3, 2m/3]$. Proposition 6.1, due to Chatterjee and Diaconis [2], provides a universal bound on this quantity, but we believe it would be worthwhile to gain a deeper understanding of the distribution. It will be shown in this section that, although a deeper understanding may be attainable, it seems to be insufficient to prove a bound of smaller order than $(\log p)^2$ on the mixing time of the Fibonacci process using the Fourier analysis approach.

We restrict ourselves to moduli of the form $m = 3^k$ throughout this section; nonetheless, with some modification, one should be able to adapt the arguments which follow to general m. We want to re-frame the Fibonacci sequence $\{x_i\}$ on $\mathbb{Z}/m\mathbb{Z}$ as a sequence $\{v_i\}$ on $(\mathbb{Z}/m\mathbb{Z})^2$ by defining:

$$v_0 = (x_0, x_1), \quad v_{i+1} = (v_i^{(2)}, v_i^{(1)} + v_i^{(2)})$$

Thus, our starting conditions will be completely determined by $v_0 \in (\mathbb{Z}/m\mathbb{Z})^2$. Now, observe that, using base-3 expansion, given any $v \in (\mathbb{Z}/m\mathbb{Z})^2$, we may write out v *uniquely* in the form

$$v = a_1 3^{k-1} + a_2 3^{k-2} + \cdots + a_{k-1}3 + a_k$$

where $a_1, \dots, a_k \in \{0,1,2\}^2$. We may identify $\{0,1,2\}^2$ with $(\mathbb{Z}/3\mathbb{Z})^2$ in order to make use of its ring structure; note that we may maintain the uniqueness of the representation by restricting ourselves to writing out elements of $\mathbb{Z}/3\mathbb{Z}$ only using the representatives 0, 1, and 2.

Now, suppose that v is the starting point of our Fibonacci recursion (that is, $v_0 = v$). Consider the Fibonacci recursion on $(\mathbb{Z}/3\mathbb{Z})^2$:

$$... \to (0,1) \to (1,1) \to (1,2) \to^* (2,0) \to (0,2) \to (2,2) \to^* (2,1) \to^* (1,0) \to ...$$

The transitions marked with $\to^*$ indicate steps where the corresponding Fibonacci recursion $\{x_i\}$ on $\mathbb{Z}/3\mathbb{Z}$ reaches the end of $\{0,1,2\}$ and "wraps back around" in $\mathbb{Z}/3\mathbb{Z}$. Each a_j undergoes this cycle as the Fibonacci process is applied iteratively starting at $v_0 = v$; however, observe that they do not do so independently of one another. When a_j (for $j > 1$) reaches a transition marked by $\to^*$, it follows that the term $3^{k-j}a_j$ adds 3^{k-j+1} to the sum in the formula for x_i, and hence it adds 1 to the second component of a_{j-1}, pushing it to a different position in the cycle. We will call the process of a_j adding 1 to the second component of a_{j-1} "incrementing one below." Another way in which a_j could "increment one below" is if a_j acquires a 2 in the second component after step i due to its natural cycle, and a_{j+1} "increments one below" at step i, thus adding 1 to 2 in the second component of a_j, and making it so that the Fibonacci recursion in the jth slot "wraps back around" in $\mathbb{Z}/3\mathbb{Z}$. Note that, in a single step, a_j can at most increment 1 above, and no more (since it can only wrap around at most once in a single step by the nature of the Fibonacci recursion).

Note that this process of "incrementing one below" makes it so that another possible state is added to the above cycle for a_j on $(\mathbb{Z}/3\mathbb{Z})^2$, assuming $j < k$: in the case that a_j reaches $(0,2)$ at the ith step, and a_{j+1} increments one below, we get that a_j takes on the value $(0,0)$. It will stay in this state exactly until a_{j+1} increments one below again, at which point a_j will take on the value $(0,1)$.

Our goal is to determine how many steps it takes for a_1 to acquire a second component equal to 1, as this is equivalent to the corresponding Fibonacci sequence $\{x_i\}$ on $\mathbb{Z}/m\mathbb{Z}$ entering the "middle third" $[m/3, 2m/3]$. Note that, without the process of "incrementing one below," meaning that if all of the a_j's simply independently cycled through the standard Fibonacci sequence on $(\mathbb{Z}/3\mathbb{Z})^2$, it would take at most 5 steps for this to occur. In other words, we need to understand the process of "incrementing one below" in order to grasp what might prevent a_1 from undergoing its natural cycle and reaching a state with second component equal to 1 very quickly. To this end, we define the following notion: A *restricted orbit* is a nonempty ordered collection $u_1, u_2, \dots, u_p \in (\mathbb{Z}/3\mathbb{Z})^2$ such that none of $u_1, u_2, \dots, u_p$ have 1 in the second component, and it is possible for a certain a_j (for j sufficiently smaller than k) to take on the values, in order,

$$u_1 \to u_2 \to \cdots \to u_p \to u_1 \to u_2 \to \cdots \to u_p;$$

that is, it is possible for a_j to cycle through the list $u_1, u_2, \ldots, u_p$ twice in a row. We may, without loss of generality, limit our attention to restricted orbits which do not consist of the same list repeated multiple times.

Intuitively, the only way that a_1 will be prevented from acquiring a 1 in its second component is if it is inside of a restricted orbit (there are only two possible next values for a given a_j whose current value is known, and only finitely many possible values; thus, if it stays away from values with 1 in the second component for sufficiently many steps, then it will necessarily traverse a restricted orbit). The problem then reduces to classifying the possible restricted orbits (of which there are far fewer than might be expected), analyzing how many starting points allow a_1 to get stuck in such an orbit, and estimating how long it takes for a_1 to escape each type of restricted orbit.

Proposition 8.1. *The only restricted orbits (up to repetition and ordering) are:*

(1) *(0, 0)*
(2) *(2, 2)*
(3) *(2, 0), (0, 2)*

Proof. Firstly, we will show that all three of these are indeed restricted orbits. We use the notation $(a_j)_i$ to mean a_j at step i. We may assume that $j < k$. Suppose that $(a_j)_i = (0, 0)$. Moreover, suppose that $(a_{j+1})_i = (0, 0)$. In the next step, there are two options: either a_{j+2} does not increment one below, in which case $(a_{j+1})_{i+1} = (0, 0)$, and $(a_j)_{i+1} = (0, 0)$, or a_{j+2} increments one below, in which case $(a_{j+1})_{i+1} = (0, 1)$, but a_{j+1} still does not increment one below, and hence $(a_j)_{i+1} = (0, 0)$. In any case, we see that it is possible to have $(a_j)_i = (0, 0)$ and $(a_j)_{i+1} = (0, 0)$. By definition, $(0, 0)$ is a restricted orbit.

Now, suppose that $(a_j)_i = (2, 2)$, and suppose that $(a_{j+1})_i = (2, 2)$. In the next step, suppose that a_{j+2} increments one below. In this case, $(a_{j+1})_{i+1} = (2, 1)$ (and in particular hits a transition marked by $\to^*$), so a_{j+1} increments one below. At the same time, the "natural" transition for a_j is to obtain the value $(2, 1)$, but a_{j+1} has incremented one above, so it instead re-obtains the value $(a_j)_{i+1} = (2, 2)$. We see that it is possible to have $(a_j)_i = (a_j)_{i+1} = (2, 2)$. By definition, $(2, 2)$ is a restricted orbit.

Now, suppose that $(a_j)_i = (a_{j+1})_i = (a_{j+2})_i = (2, 0)$. In the next step, suppose that a_{j+3} does not increment one below. Then, we would have that all three of a_j, a_{j+1}, a_{j+2} maintain their "natural" cycles, and hence $(a_j)_{i+1} = (a_{j+1})_{i+1} = (a_{j+2})_{i+1} = (0, 2)$. Now, suppose that in the next step, a_{j+3} does increment one below. The natural cycle for a_{j+2} would be to take on the value $(2, 2)$ next, but when it gets incremented by a_{j+3}, it instead takes on the value $(2, 0)$ *and* increments one below. By the same logic, the same occurs for a_{j+1} and a_{j+2}, so that we return to $(a_j)_{i+2} = (a_{j+1})_{i+2} = (a_{j+2})_{i+2} = (2, 0)$. Finally, if in the next step a_{j+3} does not increment one below, we again obtain (by the same reasoning as in the first step) $(a_j)_{i+3} = (a_{j+1})_{i+3} = (a_{j+2})_{i+3} = (0,2)$. Note that we can repeat this process over and over again so long as a_{j+3} continues alternating between incrementing one below and not incrementing one below (it may be seen that the only way for this to be possible is if a_{j+3} is stuck in the same restricted orbit $(2,0),(0,2)$). Thus, we have that a_j has, in order, taken on the values

$$(2,0) \to (0,2) \to (2,0) \to (0,2) \to (2,0).$$

By definition, $(2,0),(0,2)$ is a restricted orbit (and as is $(0,2),(2,0)$).

Now, we will show that these are all of the restricted orbits. A restricted orbit must be nonempty, and hence must include at least one element of $(\mathbb{Z}/3\mathbb{Z})^2$. Suppose that it includes $(0,0)$. The only possible next values for a_j after $(0,0)$ are $(0,0)$ (in the case that a_{j+1} does not increment one below) and $(0,1)$ (in the case that a_{j+1} does increment one below). But $(0,1)$ cannot be in a restricted orbit, because it has 1 in the second component. Therefore, inductively, any restricted orbit which contains $(0,0)$ must consist only of $(0,0)$'s (as we must be able to go through the orbit twice without reaching an element with a 1 in the second component). Since we are limiting to restricted orbits which do not consist of the same list repeated multiple times, we conclude that the only restricted orbit containing $(0,0)$ is the list consisting only of $(0,0)$.

Suppose that the restricted orbit includes $(2,2)$. The only possible next values for a_j after $(2,2)$ are $(2,1)$ (in the case that a_{j+1} does not increment one below) and $(2,2)$ (in the case that a_{j+1} does increment one below). But $(2,1)$ cannot be in a restricted orbit. Therefore, the only restricted orbit containing $(2,2)$ is the list consisting only of $(2,2)$.

Suppose that the orbit includes $(2,0)$. The only possible next values for a_j after $(2,0)$ are $(0,2)$ (in the case that a_{j+1} does not increment one below) and $(0,0)$ (in the case that a_{j+1} does increment one below). But we already know that $(0,0)$ cannot be in any restricted orbit other than the list $(0,0)$ itself, so we must have that $(0,2)$ is next in the restricted orbit. The only possible next values for a_j after $(0,2)$ are $(2,2)$ (in the case that a_{j+1} does not increment one below) and $(2,0)$ (in the case that a_{j+1} increments one below). As with $(0,0)$, we already know that $(2,2)$ cannot be in any restricted orbit other than the list $(2,2)$ itself, so we must have that $(2,0)$ is next in the orbit. By the same reasoning as before, we must then return to $(0,2)$, and so on. This shows that the only restricted orbit containing either $(2,0)$ or $(0,2)$ is $(2,0),(0,2)$ (or $(0,2),(2,0)$).

It is clear that no restricted orbit can contain either $(1,0)$, $(1,2)$, since, in order take on these values in one step, a_j would have to start at a value with 1 in the second component, and no such element can be a part of a restricted orbit. Of course, by definition, none of $(0,1)$, $(1,1)$, or $(2,1)$ are in a restricted orbit. We conclude that $(0,0)$, $(2,2)$, and $(2,0),(0,2)$ are (up to repetition and ordering) the only possible restricted orbits.

□

Observe that the only way out of restricted orbit (1) (i.e. $(0,0)$) for a_j is to be iterated by a_{j+1} and forced to go to $(0,1)$, so we know that, if $a_1 = (0,0)$ initially, then the number of steps it takes for a_1 to acquire a second component equal to 1 is precisely the number of steps required to escape orbit (1). Similarly, the only way out of orbit (2) (i.e. $(2,2)$) for a_j is for a_{j+1} to *fail* to iterate one below so that a_j proceeds naturally to $(2,1)$. Thus, if $a_1 = (2,2)$ initially, then the number of steps it takes for a_1 to acquire a second component equal to 1 is precisely the number of steps required to escape orbit (2).

Meanwhile, in the case of restricted orbit (3) (i.e. $(2,0),(0,2)$), there are two ways by which a_j could escape the orbit: one option is that a_j has value $(2,0)$, and in the next step a_{j+1} increments one below, so a_j acquires the value $(0,0)$ (and hence falls into orbit (1)); the other option is that a_j has value $(0,2)$, and in the next step a_{j+1} fails to increment one below, so a_j acquires the value $(2,2)$ (and hence falls into orbit (2)).

Some important (though imprecise) observations about each orbit is the following:

(1) In order for a_j to remain stuck in orbit (1), a_{j+1} needs to be consistently failing to increment one below at every step, which only happens for many steps on end if a_{j+1} is itself stuck in orbit (1);
(2) In order for a_j to remain stuck in orbit (2), a_{j+1} needs to be consistently incrementing one below at every step, which only happens for many steps on end if a_{j+1} is itself stuck in orbit (2);
(3) In order for a_j to remain stuck in orbit (3), a_{j+1} needs to be consistently alternating between incrementing one below and failing to increment one below (in the right order), which only happens for many steps on end if a_{j+1} is itself stuck in orbit (3) (at the same position as a_j).

Inductively, these observations imply that a_j remains "stuck" in a restricted orbit if and only if a_{j+r} is stuck in the same orbit for all $r \in \{1,\dots,R\}$ (for some $R \geq 1$), where the number of steps increases with increasing R. We make this intuition precise with the following propositions.

Proposition 8.2. *Suppose that, for $v = v_0$ written out in the form*

$$v = a_1 3^{k-1} + a_2 3^{k-2} + \cdots + a_{k-1}3 + a_k,$$

we have that $a_1 = (0,0)$. Let t be the smallest index such that $a_t \neq (0,0)$. Then it will take at least $2(t-2)+1$ and at most $3(t-2)+4$ steps of the Fibonacci recursion for the sequence $\{x_i\} \subset \mathbb{Z}/3^k\mathbb{Z}$ corresponding to $\{v_i\} \subset (\mathbb{Z}/3^k\mathbb{Z})^2$ to enter the interval $[m/3, 2m/3]$.

Proof. By the minimality of t, we know that $(a_j)_0 = (0,0)$ for all $j \in \{1,\dots,t-1\}$. Note that no incrementation will occur on any a_j (for $j \in \{1,\dots,t-2\}$) without first occurring on a_{j+1}; thus, our analysis will begin at a_t and work downwards to a_1. Since $(a_t)_0 \neq (0,0)$, one may check that it will take at most 4 steps for a_t to "increment one below" (4 is the largest number of steps possible before hitting a transition in the "natural cycle" on $(\mathbb{Z}/3\mathbb{Z})^2$ marked with a $\to^*$, and being incremented by a_{t+1} could only possibly decrease the number of steps necessary for a_t to "increment one below"). We will denote by $\ell_t \in [1,4]$ the number of steps required for a_t to increment one below. When a_t increments one below, a_{t-1} will acquire a value of $(0,1)$; that is, we have that $(a_{t-1})_{\ell_t} = (0,1)$. Since the transition $(0,0) \to (0,1)$ induces no increment below, we have that $(a_j)_{\ell_t} = (0,0)$ for all $j \in \{1,\ldots,t-2\}$.

Referring again to the "natural Fibonacci cycle" on $(\mathbb{Z}/3\mathbb{Z})^2$, we see that it will take at most 3 additional steps for a_{t-1} to increment one below (exactly 3 if a_t does not increment one below during those steps); on the other hand, it will take at least 2 steps, since the first additional step after step ℓ will send a_{t-1} naturally to $(1,1)$ (which causes no increment below), or, if a_t increments one below, to $(1,2)$ (which again causes no increment below). Thus, no matter what, we must have that $(a_{t-2})_{\ell_t+1} = (0,0)$ (and, of course, likewise for all $j \in \{1,\ldots,t-3\}$). We will denote by $\ell_{t-1} \in [2,3]$ the number of additional steps it takes for a_{t-1} to increment one below.

Thus, we have that $(a_{t-2})_{\ell_t+\ell_{t-1}} = (0,1)$, and $(a_j)_{\ell_t+\ell_{t-1}} = (0,0)$ for all $j \in \{1,\ldots,t-3\}$. By the same logic as above, the number of additional steps ℓ_{t-2} it takes for a_{t-2} to increment one below will lie inside of $[2,3]$.

We repeat this process for $a_{t-3}, a_{t-4}, \ldots, a_3, a_2$, finding at each step that the number of additional steps ℓ_j required to increment one below lies inside of $[2,3]$. Ultimately, we obtain that the first step n where $(a_1)_n \neq (0,0)$ (and hence, necessarily, where $(a_1)_n = (1,0)$) is given by:

$$n = \ell_t + \ell_{t-1} + \cdots + \ell_2.$$

Since $\ell_t \in [1,4]$ and $\ell_j \in [2,3]$ for all $j \in \{2,\ldots,t-1\}$, it follows that

$$n \in [2(t-2)+1, 3(t-2)+4],$$

as claimed. The statement is proven. □

We obtain a similar result for the case where $a_1 = (2,2)$.

Proposition 8.3. *Suppose that, for $v = v_0$ written out in the form*

$$v = a_1 3^{k-1} + a_2 3^{k-2} + \cdots + a_{k-1}3 + a_k,$$

we have that $a_1 = (2,2)$. Let t be the smallest index such that $a_t \neq (2,2)$. Then it will take at least $2(t-2)+1$ and at most $3(t-2)+4$ steps of the Fibonacci recursion for the sequence $\{x_i\} \subset \mathbb{Z}/3^k\mathbb{Z}$ corresponding to $\{v_i\} \subset (\mathbb{Z}/3^k\mathbb{Z})^2$ to enter the interval $[m/3, 2m/3]$.

Proof. The proof is nearly identical to that for Proposition 8.2. □

From Proposition 8.2, we obtain the following corollary.

Corollary 8.4. *For $2 \leq q \leq k = \log_3 m$, a proportion of at least $\left(\frac{1}{9}\right)^q$ of all possible starting points in $(\mathbb{Z}/m\mathbb{Z})^2$ produce a corresponding Fibonacci sequence $\{x_i\} \subset \mathbb{Z}/m\mathbb{Z}$ which fails to enter $[m/3, 2m/3]$ within $2(q-2)+1$ steps.*

Proof. Starting points $v \in (\mathbb{Z}/m\mathbb{Z})^2$ with $a_1 = (0,0)$ account for exactly $\frac{1}{9}$ of all starting points. Furthermore, given that $a_1 = (0,0)$, exactly $\frac{8}{9}$ of all such elements have $a_2 \neq (0,0)$ (so that 2 is the smallest t with $a_t \neq (0,0)$). Similarly, exactly $\frac{8}{9} \cdot \frac{1}{9}$ of all elements with $a_1 = (0,0)$ have $a_2 = (0,0)$ and $a_3 \neq (0,0)$ (so that 3 is the smallest t with $a_t \neq (0,0)$). In general, a proportion of exactly $\frac{8}{9} \cdot \left(\frac{1}{9}\right)^{t-2}$ of all elements with $a_1 = (0,0)$ have $a_j = (0,0)$ for all $j \in \{1, \dots, j-1\}$ and $a_t \neq (0,0)$. We know from Proposition 8.2 that, given that $a_1 = (0,0)$, the only elements which could enter $[m/3, 2m/3]$ within $2(q-2)+1$ steps are those for which the minimal t with $a_t \neq (0,0)$ is at most equal to q. Thus, we have that an upper bound on the proportion of starting points with $a_1 = (0,0)$ which enter $[m/3, 2m/3]$ within $2(q-2)+1$ steps is given by:

$$\frac{8}{9}\left(\sum_{j=0}^{q-2}\left(\frac{1}{9}\right)^j\right)$$
$$= \frac{8}{9}\left(\frac{1-\left(\frac{1}{9}\right)^{q-1}}{1-\frac{1}{9}}\right)$$
$$= 1 - \left(\frac{1}{9}\right)^{q-1}.$$

Therefore, a lower bound on the proportion of starting points with $a_1 = (0,0)$ which fail to enter $[m/3, 2m/3]$ within $2(q-2)+1$ steps is $\left(\frac{1}{9}\right)^{q-1}$. Since $v \in (\mathbb{Z}/m\mathbb{Z})^2$ with $a_1 = (0,0)$ account for $\frac{1}{9}$ of all starting points, it follows that at least a proportion of $\left(\frac{1}{9}\right)^q$ of all possible starting points in $(\mathbb{Z}/m\mathbb{Z})^2$ produce a corresponding Fibonacci sequence $\{x_i\} \subset \mathbb{Z}/m\mathbb{Z}$ which fails to enter $[m/3, 2m/3]$ within $2(q-2)+1$ steps. The statement is proven. □

Note that, using Proposition 8.1, similar results may be obtained for other starting values of a_1 (besides $(0,0)$ and $(2,2)$). However, Corollary 8.4 is sufficient to explain why it seems likely that the Fourier analysis approach will not be able to give a bound on the mixing time of the Fibonacci generator which is of a smaller order than $(\log m)^2$. We recall the estimate given by the Fourier upper bound theorem (Theorem 4.1):

$$\|P_n - U\|^2 \leq \frac{1}{4}\sum_{a\neq 0}\prod_{b=0}^{n-1}\left(\frac{1}{3}+\frac{2}{3}\cos\left(\frac{2\pi F_b a}{m}\right)\right)^2.$$

We make the assumption that the sequences aF_b with $a < \frac{m}{3}$ have starting points which are representative of the set of all starting points in the first third $[0, m/3]$ (this is in fact conservative, since the first starting point for all such sequences is 0, so there is in fact a higher likelihood is having a larger number of $(0,0)$'s for the a_j's). We want to break up the sum between "efficient" a and "inefficient" a

(where "efficient" a correspond to sequences aF_b which enter the middle interval more frequently). Let $g(m)$ be the number of steps (in terms of m) which it takes for "efficient" sequences to enter the middle interval, and let $n(m)$ be the mixing time (in terms of m). We know from Corollary 8.4 that the number of "inefficient" a, say Q, will be bounded below as follows

$$Q \geq \frac{m}{3}\left(\frac{1}{9}\right)^{\frac{g(m)+3}{2}}$$

Note that this lower bound is quite conservative, since we have only accounted for the "inefficient" a inside of the first third. We will assume (generously) that Q is fairly close to this lower bound, so that in particular (for large m), Q is much smaller than m. Moreover, since the Fibonacci sequence grows approximately exponentially after sufficiently many steps, we know that *some* starting points of the Fibonacci sequence will require something on the order of $\log m$ steps to reach the middle interval, so we will assume that 1 in $C_1 \log m$ (for C_1 a constant) is the frequency of entering the middle interval for the "inefficient" sequences. Thus, we may break up the sum as follows:

$$\frac{1}{4}\sum_{a\neq 0}\prod_{b=0}^{n(m)-1}\left(\frac{1}{3}+\frac{2}{3}\cos\left(\frac{2\pi F_b a}{m}\right)\right)^2$$
$$\leq \frac{1}{4}\left((m-Q)\left(\frac{1}{9}\right)^{\frac{n(m)}{g(m)}} + Q\left(\frac{1}{9}\right)^{\frac{n(m)}{C_1 \log m}}\right)$$

In order for this expression to converge to 0 as $m \to \infty$, we must have that $n(m)$ is at least sufficiently large to cancel out $g(m)$ and $(m-Q) \approx m$ from the first term and sufficiently large to cancel out $C_1 \log m$ and Q from the second term. Thus, with $C_2, C_3 > 0$ being some constants, we must have that:

$$n(m) = C_2 g(m)\log(m) = C_3 \log(m)\log(Q)$$
$$\geq C_3 \log(m) \log\left(\frac{m}{3}\left(\frac{1}{9}\right)^{\frac{g(m)+3}{2}}\right).$$

Solving for $g(m)$, we have:

$$\frac{C_2}{C_3} g(m) \geq \log\left(\frac{m}{3}\left(\frac{1}{9}\right)^{\frac{g(m)+3}{2}}\right)$$

$$e^{\frac{C_2}{C_3}g(m)} \geq \frac{m}{3}\left(\frac{1}{9}\right)^{\frac{g(m)+3}{2}}$$

$$3^{g(m)+4} e^{\frac{C_2}{C_3}g(m)} \geq m$$

$$e^{(\log 3 + C_2/C_3)g(m) + 4\log 3} \geq m$$

$$g(m) \geq \left(\frac{1}{\log 3 + C_2/C_3}\right)\log m - \frac{4\log 3}{\log 3 + C_2/C_3}.$$

Plugging this back into the mixing time $n(m)$, we obtain that

$$n(m) \geq \left(\frac{C_2}{\log 3 + C_2/C_3}\right)(\log m)^2 - \left(\frac{4\log 3}{\log 3 + C_2/C_3}\right)\log m$$

which is still on the order of $(\log m)^2$. Thus, we see that, even equipped with more knowledge about the behavior of Fibonacci sequences on $\mathbb{Z}/m\mathbb{Z}$ (and some generous assumptions), the Fourier analysis approach still fails to give an upper bound on the mixing time of the Fibonacci random process of order smaller than $(\log m)^2$. As such, it seems advisable that the Fourier analysis strategy be abandoned in future research with the aim of improving this particular bound.

Nevertheless, the results of this section and the section which follows may be of more general interest to those studying the distribution of Fibonacci sequences on $\mathbb{Z}/m\mathbb{Z}$.

9. The Fibonacci Distribution Problem

Chung, Diaconis, and Graham's [3] study of the system $X_{n+1} = 2X_n + \epsilon_n \pmod{m}$ using Fourier analysis exploited similarities in the base-2 expansions of a/m, as a ranged from 1 to $m-1$. When Chatterjee and Diaconis [2] attempted to use the same technique to study the Fibonacci system $X_{n+2} = X_{n+1} + X_n + \epsilon_n \pmod{m}$, they needed information about the long-term behavior of (deterministic) Fibonacci-type sequences modulo m. This is not well-studied, which forced them to make do with a worst-case scenario result, namely Proposition 6.1. We have somewhat improved upon their result with our results in Section 7.

In the present section, therefore, we concern ourselves with the purely number-theoretic general question:

Aim. *What is the long-term behavior, modulo m, of any sequence $x_0, x_1, x_2, \ldots$ obeying the Fibonacci relation*

$$x_{n+1} = x_n + x_{n-1}.$$

As this is a purely number-theoretic question, this section is independent of all prior sections.

While a great deal is known about the periodicity of Fibonacci-type sequences modulo m, the Fibonacci Distribution Problem (i.e. the distribution of those elements mod m), does not appear to be well-studied, at least as we have formulated it. We first present a useful and visually descriptive reformulation of the problem by associating to each modulus m a cycle-disjoint graph on m^2 vertices. We will also present a review of known results, which almost exclusively deal with the length of said cycles.

Computational experiments allowed us to formulate a number of reasonable-sounding conjectures, but even the simplest ones proved unexpectedly difficult to prove. These conjectures and associated questions will be listed, and we hope that the proofs or refutations of some or all of them will not be too difficult for future investigators to unearth.

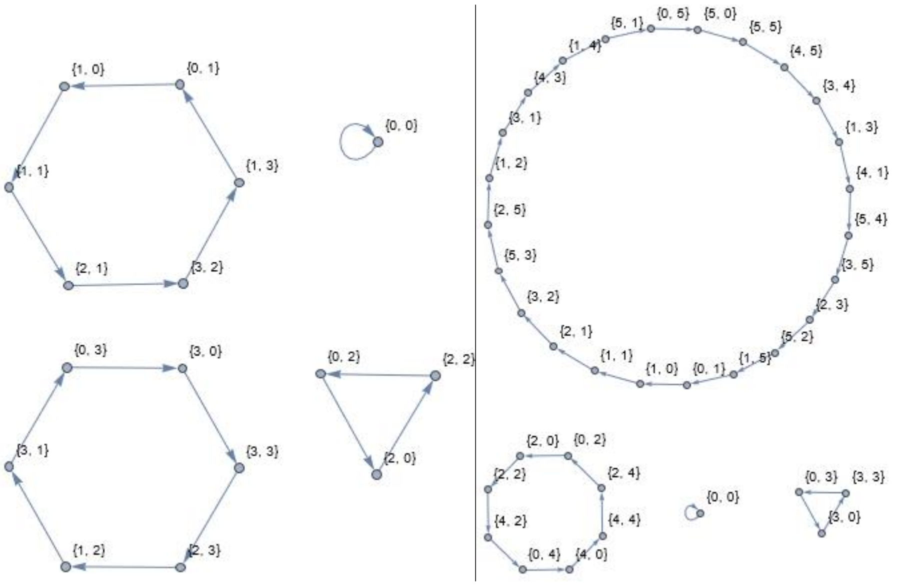
9.1. **Definitions: Cycles in the Fibonacci Directed Graph of Ordered Pairs.**

Observe that knowing the values of x_n and x_{n-1} mod m completely determine the entire future and past of the Fibonacci-type sequence $x_0, x_1, x_2, \ldots$ modulo m. Therefore, if the same sequence of two values x_{n-1}, x_n ever repeats, the entire sequence will be periodic mod m. Since there are only m^2 possible pairs of values x_{n-1}, x_n, a pair of successive values is bound to reappear within m^2 steps, so every Fibonacci-type sequence is periodic modulo m.

This can be formalized as follows: Define the map

$$f : \mathbb{Z}_m \times \mathbb{Z}_m \to \mathbb{Z}_m \times \mathbb{Z}_m, \quad (a, b) \mapsto (a + b, a)$$

Then observe that both the first and second components of $f^n(a, b)$ (where the exponent denotes repeated function composition) satisfy the Fibonacci relation as n increases. Of course, letting the elements of $\mathbb{Z}_m \times \mathbb{Z}_m$ be a vertex set, we can define the graph representation $G(m)$ of the Fibonacci iterator f by defining $G(m)$ to be the directed graph on $\mathbb{Z}_m \times \mathbb{Z}_m$ having directed edges $(a, b) \to f(a, b)$. This gives us a very quick way to visualize the action of the Fibonacci recursion on $\mathbb{Z}_m \times \mathbb{Z}_m$. For example, $G(4)$ and $G(6)$ are:



Several patterns are immediately apparent and easily proven:

Fact. *Each ordered pair (a, b) has exactly one successor, namely $(a + b, a)$, and exactly one predecessor, namely $(b, a - b)$. Therefore, $G(m)$ consists of disjoint directed cycles. Moreover, $(0, 0)$ is the only ordered pair that maps to itself, hence the only one-element cycle.*

This basic groundwork naturally prompts three inquiries:

(1) Given m, what is the set of cycle lengths that make up the graph $G(m)$?
(2) Given a starting ordered pair (a, b), how long is the cycle containing it?
(3) Given a starting ordered pair (a, b) and $\delta \in [0, 1/2]$, how many elements of the cycle containing (a, b) lie in $[\delta m, (1 - \delta)m]$?

The language used to state (3) is not rigorously defined. We remedy this.[1]

Definition 9.1. The Fibonacci Iteration Function f and the Fibonacci Graph $G(m)$ are defined as above. Moreover:

(1) Given an ordered pair $(a, b) \in \mathbb{Z}_m \times \mathbb{Z}_m$, the set of all ordered pairs in the same cycle as (a, b) in $G(m)$ is denoted $C_m(a, b)$, or $C(a, b)$ if m is clear from context.

(2) Naturally, $|C_m(a, b)|$ denotes the length of said cycle. This function is commonly known as the *Pisano Period*, especially if the starting pair is $(1, 0)$. Usually, the Pisano Period is written with the notation $\pi(m) = |C_m(1, 0)|$, or more generally $\pi_{(a,b)}(m) = |C_m(a, b)|$. Most results about cycle length are expressed using this notation, and due to its compactness, we will use it as well.

(3) If a set $C \subseteq \mathbb{Z}_m \times \mathbb{Z}_m$ just happens to represent a cycle of $G(m)$, we freely abuse notation by writing $C \in G(m)$.

(4) We say that an ordered pair $(a, b) \in \mathbb{Z}_m \times \mathbb{Z}_m$ *lies in* the interval $[c, d] \subseteq [0, m]$, where $0 \leq c \leq d \leq m$, if a is equivalent to[2] an element of $[c, d]$, or alternatively if

$$\frac{a}{m} - \left\lfloor \frac{a}{m} \right\rfloor \in \left[\frac{c}{m}, \frac{d}{m} \right].$$

We freely abuse notation and write $(a, b) \in [c, d]$ in this case.

(5) If C is a cycle, we define

$$\chi_\delta(C) = |\{(a, b) \in C : (a, b) \in [\delta m, (1 - \delta)m]\}| \quad \text{and} \quad \chi_\delta(a, b) = \chi_\delta(C(a, b)).$$

That is, χ_δ counts the number of elements of a cycle falling within the associated "middle interval".

(6) If C is a cycle, then we define

$$\kappa_\delta(C) = \frac{|\chi_\delta(C)|}{|C|} \quad \text{and} \quad \kappa_\delta(a, b) = \kappa_\delta(C(a, b)).$$

That is, κ_δ measures the *ratio* of cycle elements in the middle interval $[\delta m, (1 - \delta)m]$ to the total number of cycle elements.

(7) We define $M_\delta(m)$ to be the minimum value of κ_δ over all cycles, or equivalently over all ordered pairs. That is:

$$M_\delta(m) = \min_{C \in G(m)} \kappa_\delta(C) = \min_{(a,b) \in \mathbb{Z}_m \times \mathbb{Z}_m} \kappa_\delta(a, b).$$

[1] As this appears to be a new area of inquiry, this notation is by no means standardized. There may exist better notation. The use of f and G for the iteration function and graph, respectively, should be clear. C stands for "cycle", of course. Although closely related, we defined χ_δ and κ_δ as separate entities because, while χ_δ is a direct count, and probably easier to work with mathematically, κ_δ captures the idea of long-term behavior better. Since both are counts or closely related to counts, and C and c are already in use, we chose the c-sounding Greek letters χ and κ to represent these functions.

[2] We thus treat a as the "observed value" of the ordered pair (a, b), though in theory we could treat b as the observed value instead and all the same results would hold.

With these definitions in hand, it will now be possible to efficiently state known results and conjectures.

9.2. **Known Results.** The majority of known results pertain to the the value of $\pi(m) = |C_m(1,0)|$ for various values of m, or more generally to $\pi_{(a,b)}(m) = |C_m(a,b)|$. The website [4] provides a more complete list of results, but we list some of the most interesting and potentially relevant here:

Theorem 9.2 (Listed in Renault)**.** *Bounds and Particular Values of $\pi(m), m = 2, 3, 4, \dots$:*

(1) *Parity: $\pi(2) = 3$, and $\pi(m)$ is even otherwise.*
(2) *Upper Bound: $\pi(m) \leq 6m$. Equality holds exactly when $m = 2 \cdot 5^k, k = 1, 2, 3, \dots$.*
(3) *Lower Bound: If $L_k \leq m$, then $\pi(m) \geq 2k$. Equality can hold, for example if $m = L_k$ and $k \geq 3$ is odd.*
(4) *Fibonacci Number Moduli: If $k \geq 4$ is even, then $\pi(F_k) = 2k$. If $k \geq 5$ is odd, then $\pi(F_k) = 4k$.*
(5) *Lucas Number Moduli: If $k \geq 3$ is odd, then $\pi(L_k) = 2k$. If $k \geq 4$ is even, then $\pi(L_k) = 4k$.*[3]
(6) *Fixed Points: $\pi(m) = m$ if and only if $m = 24 \cdot 5^k$ for $k = 1, 2, 3, \dots$.*

Theorem 9.3 (Listed in Renault)**.** *Computing $\pi(m)$:*

(1) $\pi(\mathrm{lcm}(m,n)) = \mathrm{lcm}(\pi(m), \pi(n))$. *Consequently, $n \mid m$ implies $\pi(n) \mid \pi(m)$ and if $p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$ is the prime factorization of m, then*

$$\pi(m) = \mathrm{lcm}(\pi(p_1^{e_1}), \pi(p_2^{e_2}), \dots, \pi(p_k^{e_k})).$$

(2) *If p is a prime, then $\pi(p^e) = p^{e-1}\pi(p)$ unless $\pi(p) = \pi(p^2)$, in which case p is called a Wall-Sun-Sun prime. No Wall-Sun-Sun primes are known to exist (i.e. any prime you can physically write down has already been confirmed not to be a Wall-Sun-Sun prime).*
(3) *If p is a prime, then $\pi(2) = 3$, $\pi(5) = 20$, $\pi(p) \mid p - 1$ if $p \equiv \pm 1 \pmod{10}$, and $\pi(p) \mid 2p + 2$ if $p \equiv \pm 3 \pmod{10}$.*

Theorem 9.4 (Listed in Renault)**.** *Assume throughout that $\gcd(a, b, m) = 1$. In the case that $\gcd(a, b, m) > 1$, the system can be reduced to a smaller one by dividing all numbers by $\gcd(a, b, m)$. Moreover, define $D = b^2 - ab - a^2$.*

(1) $\pi_{(a,b)}(m) \mid \pi(m)$.
(2) *If $\gcd(D, m) = 1$, then $\pi_{(a,b)}(m) = \pi(m)$.*
(3) *Theorem 9.3(1) holds with $\pi_{(a,b)}$ in place of π.*
(4) $\pi_{(a,b)}(2^e) = \pi(2^e)$.
(5) *$\pi_{(a,b)}(5^e) = \pi(5^e)$ unless $5 \mid D$, in which case $\pi_{(a,b)}(5^e) = (1/5)\pi(5^e)$.*
(6) *If $p \equiv \pm 3 \pmod{10}$ is prime, then $\pi_{(a,b)}(p^e) = \pi(p^e)$.*

[3] Though stated to be a well-known result on Wikipedia, we have been unable to find a reliable source for this particular result. We proved most of this result independently as just a matter of algebra, however, and have no reason to doubt it.

(7) *Suppose* $p \equiv \pm 1 \pmod{10}$ *is prime. If* $\pi(p^e) \equiv 0 \pmod 4$*, then* $\pi_{(a,b)}(p^e) = \pi(p^e)$*. If* $\pi(p^e) \equiv 2 \pmod 4$*, then either* $\pi_{(a,b)}(p^e) = \pi(p^e)$ *or* $\pi_{(a,b)}(p^e) = (1/2)\pi(p^e)$*, and there are ordered pairs* (a, b) *producing both values.*

Remark 9.5. The results above are quite extensive without being completely exhaustive, almost completely answering question (2) from the beginning of this section. With a little interpretation, these results might go a long ways towards providing a complete characterization of the cycle lengths for various moduli m and thereby answering question (1) from the beginning of this section.

Remark 9.6. It should be noted that the cycle lengths can go as low as around $\log(m)$ steps (for example if m is a Lucas or Fibonacci number) or as high as $6m$ steps. Since the CDG convergence theorems described in the rest of this paper assume only taking somewhere between $O(\log m)$ and $O((\log m)^2)$ steps, merely answering the questions asked in the beginning of this section will not be sufficient to determine the mixing time of the Fibonacci CDG process except when the maximum cycle length is known to be $O(\log m)$ (or maybe slightly worse).

Remark 9.7. There is one paper we could find that dealt more directly with the Fibonacci Distribution Problem (problem (3) formulated above), by Bundschuh and Bundschuh [1]. They gave a rather comprehensive description of the residues of the Fibonacci and Lucas numbers when m is a power of 3, but it it not intuitive and would take some work to translate into an answer for question (3). We therefore omit it here and encourage the reader to check out the original paper.

Having summarized what is known about the answers to questions (1) and (2), we now turn to question (3).

9.3. **Conjectures on the Distribution of Fibonacci Numbers Modulo m.**

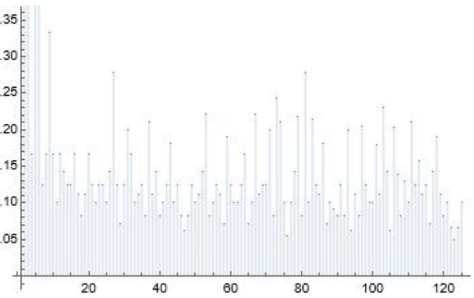
We now present a series of conjectures that seem to be true based on computational evidence. Almost all of these deal specifically with Lucas Number moduli, which seem to be even nicer than Fibonacci Number moduli in many respects.

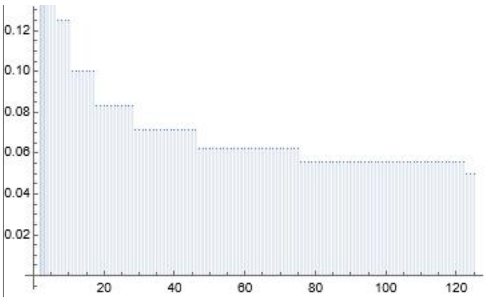
Conjecture 9.8. *For all* $k \geq 3$ *and* $a, b \in \mathbb{Z}_{L_k}$*,* $(a, 0)$ *and* $(b, 0)$ *are not in the same cycle (i.e.* $C_{L_k}(a, 0) \neq C_{L_k}(b, 0)$*) unless* k *is even and* $a \equiv -b \pmod{L_k}$*, in which case they are.*

This seems like a matter of algebra to prove, or could fall out from a more thorough treatment of cycle types and cycle lengths specifically targeted at Lucas Number moduli. A similar uniqueness does not appear to hold for the Fibonacci numbers (or more general numbers). For example $(1, 0)$ is in the same cycle as $(5, 0)$ in $G(8)$. Nevertheless, studying which of the set of pairs $(1, 0), (2, 0), \ldots, (m-1, 0)$ tend to show up in the same cycles would likely be vital to a fuller understanding of the cycle decomposition of $G(m)$. Note, however, that there are usually cycles that do not include any 0s at all, and hence no pairs of the form $(a, 0)$ or $(0, a)$.

Conjecture 9.9. *For all* $k \geq 3$*,* $\kappa_{1/3}(L_k) = \frac{1}{2k}$*. Moreover, if* $L_k < m < L_{k+1}$*, then* $\kappa_{1/3}(L_k) > \frac{1}{2k}$*.*

Here is a graph of $M_{1/3}(m)$ for $2 \leq m \leq 125$ and beside it a graph of the running minimum value of $M_{1/3}$.





It can be checked that the points at which $M_{1/3}$ attains a new low are precisely the Lucas Numbers, and the rest of the conjecture can be checked to correspond to the computational data.

This conjecture does not appear to be directly generalizable to all δ. For example, when $\delta = 1/4$, the values of m at which a new minimum value of $M_{1/4}(m)$ are obtained are $m = 5, 7, 9, 11, 13, 17, 29, 47, 72, 123$, which as of this writing do not line up with any known sequences according to the OEIS. The actual value of $M_{1/4}(m)$ at these points also does not follow a recognizable pattern.

Conjecture 9.10. *For all sufficiently large k, $M_\delta(L_k) = \kappa_\delta(C_{L_k}(1, 0))$. That is, the starting pair $(1, 0)$ gives the lowest fraction of cycle elements in the middle interval. In particular, $M_{1/3}(L_k) = \kappa_{1/3}(C_{L_k}(1, 0))$ for all $k \geq 3$, and $M_{1/4}(L_k) = \kappa_{1/4}(C_{L_k}(1, 0))$ for all $k \geq 4$.*

Although this has been observed to hold in certain small cases, this particular conjecture is mainly inspired by wishful thinking. If this were true, then we would only have to restrict ourselves to the Fibonacci sequence itself to identify the worst-case behavior of κ_δ across all starting pairs whenever m is a Lucas Number. It is also possible this conjecture could be extended to Fibonacci Number moduli.

Conjecture 9.11. *For sufficiently large k, the value of $\chi_\delta(C_{L_k}(1, 0))$ is dependent only on δ and whether k is odd or even. In particular, for $k \geq 3$,*

$$\chi_{1/3}(C_{L_k}(1,0)) = \begin{cases} 1 & k \text{ is odd} \\ 2 & k \text{ is even} \end{cases}$$

and for $k \geq 4$,

$$\chi_{1/4}(C_{L_k}(1,0)) = \begin{cases} 3 & k \text{ is odd} \\ 6 & k \text{ is even} \end{cases}$$

If true, this conjecture quantifies how strongly the Fibonacci sequence tends to "cluster" around the edges (i.e. close to 0) rather than in the middle (i.e. close to $m/2$). The intuition is rather simple: we are trying to find the solutions n of the inequality

$$\delta \leq \frac{F_n}{L_k} - \left\lfloor \frac{F_n}{L_k} \right\rfloor \leq (1 - \delta).$$

For small n, the middle term is close to $\varphi^{n-k}/\sqrt{5}$ (where φ is the golden ratio), and taking logs reveals that there are a fixed number of solutions regardless of k. However, making this formal, even in the $\delta = 1/3$ case, has proved quite difficult. For one, the error

$$\frac{F_n}{L_k} - \frac{\varphi^{n-k}}{\sqrt{5}}$$

grows exponentially with n, so we will probably need to intentionally restrict to small n (which is okay given periodicity) in order to keep the error manageable. Even so, the error still causes problems to the argument. The situation is further complicated by the fact that $\frac{F_k}{L_k} \to \frac{1}{\sqrt{5}}$ as $k \to \infty$, implying that the size of k needed to ensure stability in the value of χ_δ may blow up as δ approaches $\frac{1}{\sqrt{5}}$.

Although the line of inquiry above has taken us quite far from the original topic of this paper, it is quite interesting in its own right. As a means to slightly tie the above inquiries back to the Fibonacci Random Generator question, we present one last conjecture:

Conjecture 9.12. *Consider the* $(m-1) \times (n-1)$ *array of numbers*

$$\begin{pmatrix} F_1 & F_2 & \cdots & F_{n-1} \\ 2F_1 & 2F_2 & \cdots & 2F_{n-1} \\ \vdots & \vdots & \ddots & \vdots \\ (m-1)F_1 & (m-1)F_2 & \cdots & (m-1)F_{n-1} \end{pmatrix}.$$

Then for $m, n \geq 5$, *at least* $2/7$ *of these numbers are in* $[m/3, 2m/3]$ *mod* m *and* $2/5$ *of these numbers are in* $[m/4, 3m/4]$ *mod* m.

As n and m increase, there appears in both cases to be some limiting behavior to a number greater than 2/7ths and 2/5ths, respectively. This is hard to visualize without 3D interactivity, however. If true, then at least an appreciable fraction of the factors in the Fourier Series bounding expression are "small."

References

[1] Ralf Bundschuh and Peter Bundschuh. Distribution of fibonacci and lucas numbers modulo 3^k. Last accessed 26 August 2021.

[2] Sourav Chatterjee and Persi Diaconis. Speeding up markov chains with deterministic jumps, 2020.

[3] F. R. K. Chung, Persi Diaconis, and R. L. Graham. Random walks arising in random number generation. *Ann. Probab.*, 15(3):1148–1165, 1987.

[4] Marc Renault. The fibonacci sequence modulo m. Last accessed 26 August 2021.

Code

Here, we include Mathematica code critical to generating some of the conjectures and diagrams.

The Fibonacci Iteration Function was implemented as follows:

```
f[{i_, j_}, p_]:=Mod[{i + j, i}, p];
```

This is the graphing function used to generate the graphs in the text:

```
graphNoHighlights[p_]:=
  Graph[
    Normal[AssociationMap[f[#,p]&, Flatten[Table[{i,j}, {i,0,p − 1}, {j,0,p − 1}], 1]]],
  VertexLabels → “Name”]
```

It can be made easy to spot patterns in the distribution of the numbers by defining a variant function that adds the option

```
  VertexStyle->{{n_/;Between[n,{p/3,2p/3}]}->Red}
```

to the arguments of **Graph[]**. This particular example will highlight in red any ordered pair (a, b) with $a \in [p/3, 2p/3]$ (the code uses p instead of m for the modulus, with the same meaning). The chosen interval can also be changed by modifying the code.

The following code defines a function for the value of $M_{1/3}(p)$ as defined in Section 9:

```
findMinFraction[p_]:=Module[{cyclelist = FindCycle[graph[p], Infinity, All]},
Min[Table[Count[First/@First/@cycle,n_/;Between[n,{p/3,2p/3}]]/Length[cycle], {cycle, cyclelist}]]]
```

This code is easily altered to accommodate any choice of δ.

The following code, together with Theorem 9.2(5), can be used to test Conjecture 9.11:

```
Table[
  Count[
    NestList[Mod[{First[#] + Last[#], First[#]}, LucasL[k]]&, {0, 1}, 4k]
  , n_/;Between[First[n], {1LucasL[k]/3, 2LucasL[k]/3}]]
, {k, 3, 300}]
```

Department of Mathematics, Stanford University, Stanford, CA, USA
Email address: ebogle@stanford.edu

Department of Mathematics, Stanford University, Stanford, CA, USA
Email address: obrass02@stanford.edu

Department of Mathematics, Stanford University, Stanford, CA, USA
Email address: owenshen@stanford.edu