THE FIBONACCI SEQUENCES MOD M

SUNAY MIDUTHURI AND JOSHUA ZUCKER

ABSTRACT. This paper is about the modular fibonacci sequence, or the fibonacci sequence with varied starting numbers and a fixed modulus. An example is the sequence starting with $1, 2$ and mod 4:

$$1, 2, 3, 1, 0, 1, 1, 2, 3, \ldots$$

As we can see, this repeats after the first 6 values. In this paper, we show first that every sequence repeats at some period, and then bound the period. Then, we discuss the problem of finding the period given the modulus and starting numbers, and obtain a result to find it given the periods of the modulus's prime power factors. Then, we investigate a conjecture for prime power moduli. Then, we look to find a modulus and starting numbers given a period. Finally, we present questions for further research.

1. INTRODUCTION

The primary focus of this paper is on the modular fibonacci sequence. Consider the altered fibonacci sequence that starts with two positive integers a and b: $a, b, a+b, a+2b, 2a+3b, 3a+5b$, and so on. We define $f_{a,b}(k)$ to be the kth term in the sequence, where $a = f_1$ and $b = f_2$. For instance, $f_{a,b}(3) = a + b$.

We will discuss the modular fibonacci sequence, as follows.

Definition 1.1. *The **modular fibonacci** sequence is defined by three values: a modulus m, a first term a, and a second term b. We define*

$$f^m_{a,b}(k) = f_{a,b}(k) \pmod{m}.$$

Since this is essentially a fibonacci sequence, we have

$$f^m_{a,b}(k) \equiv f^m_{a,b}(k-1) + f^m_{a,b}(k-2) \pmod{m}.$$

A natural question that arises is what happens to this sequence, given a starting pair of numbers and a modulus. As it turns out, this sequence is always periodic.

Definition 1.2. *The **period** of two starting numbers a, b and a modulus m is defined to be the smallest number $p = \pi(m, a, b)$ such that*

$$f^m_{a,b}(p+1) = f^m_{a,b}(1) = a, \text{ and}$$
$$f^m_{a,b}(p+2) = f^m_{a,b}(2) = b.$$

There's quite a bit to unpack here, so let's see what exactly that means. If

$$f^m_{a,b}(p+1) = f^m_{a,b}(1) = a$$

and

$$f^m_{a,b}(p+2) = f^m_{a,b}(2) = b,$$

we must have that

$$\begin{aligned} & f_{a,b}^m(p+3) \\ & \equiv f_{a,b}^m(p+1) + f_{a,b}^m(p+2) \pmod{m} \\ & \equiv a+b \pmod{m} \\ & \equiv f_{a,b}^m(3) \pmod{m}. \end{aligned}$$

Through strong induction, the following theorem can be shown.

Theorem 1.3. *If $p = \pi(m,a,b)$ is the period of the sequence starting with a, b and with modulus m, then*

$$f_{a,b}^m(p+k) = f_{a,b}^m(k)$$

for all $k \geq 1$.

Now, here's a question. Does every sequence have a period; that is, must every sequence repeat at some point?

2. Does every sequence have a period?

Theorem 2.1. *Given any sequence $\{f_{a,b}^m\}$, it must repeat at some point, with period p. Furthermore, $p \leq m^2$.*

Proof. Consider possible pairs of consecutive terms in the sequence. Each needs to be a valid residue mod m, so there are m options for each. As a result, there are only m^2 possible pairs of consecutive terms. Then, after m^2 terms, we must have seen the consecutive pair of terms we started with, a and b. The entire sequence must repeat after that, so the period is at most m^2. □

3. Part One

This chapter will attempt to answer the question: Given modulus m and starting numbers a, b, what is the period of the resulting sequence? We have one big theorem of the section; the period given a modulus m can be determined from the periods of its prime factors.

First, however, we need to make an observation:

Lemma 3.1. *Given a sequence $\{f_{a,b}^m\}$ with period p, for all x satisfying*

$$f_{a,b}^m(x+1) = a, \text{ and}$$
$$f_{a,b}^m(x+2) = b,$$

$x = kp$ for some positive integer k.

In other words, when it repeats, it must repeat at multiples of its period.

Proof. We'll use proof by contradiction. Suppose that $x \not\equiv 0 \pmod{p}$. Then, we can write $x = kp + q$, for some positive integer k and $0 < q < p$. We have that

$$f_{a,b}^m(p+1) = f_{a,b}^m(p+p+1) = \cdots = f_{a,b}^m(kp+1) = a, \text{ and}$$
$$f_{a,b}^m(p+2) = f_{a,b}^m(p+p+2) = \cdots = f_{a,b}^m(kp+2) = b.$$

In other words, the sequence repeats after kp terms. However, since it repeats after $kp+q$ terms, it must repeat after q terms. However, q is less than the period, a contradiction.

Therefore, x must be a multiple of p.

□

Theorem 3.2. *Consider starting numbers a, b and a modulus m. Let*

$$m = p_1^{e_1} p_2^{e_2} \dots p_k^{e_k},$$

where the p_i are all distinct primes. Then,

$$\pi(m, a, b) = \text{lcm}(\pi(p_1^{e_1}, a, b), \pi(p_2^{e_1}, a, b), \dots, \pi(p_k^{e_k}, a, b)).$$

Proof. If $\pi(m, a, b) = p$, then we have two modular equations: $f_{a,b}^m(p+1) \equiv a \pmod m$ and $f_{a,b}^m(p+2) \equiv b \pmod m$. Let $p_i^{e_i} = m_i$ By the Chinese Remainder Theorem [1] , since the $p_i^{e_i}$ are all relatively prime, each of these equations becomes a system of k equations:

$$\begin{aligned}
f_{a,b}^{m_1}(p+1) &\equiv a \pmod{m_1} \\
f_{a,b}^{m_2}(p+1) &\equiv a \pmod{m_2} \\
&\vdots \ \vdots \ \vdots \\
f_{a,b}^{m_k}(p+1) &\equiv a \pmod{m_k}, \text{ and} \\
f_{a,b}^{m_1}(p+2) &\equiv b \pmod{m_1} \\
f_{a,b}^{m_2}(p+2) &\equiv b \pmod{m_2} \\
&\vdots \ \vdots \ \vdots \\
f_{a,b}^{m_k}(p+2) &\equiv b \pmod{m_k}.
\end{aligned}$$

In other words, all the sequences $\{f_{a,b}^{m_i}\}$ repeat after p terms. Therefore, by Lemma 2.1, for all $1 \le i \le k$,

$$\pi(m_i, a, b) | p.$$

Therefore, the period p is the smallest multiple of all these periods, or

$$\pi(m, a, b) = p = \text{lcm}(\pi(m_1, a, b), \pi(m_2, a, b), \dots, \pi(m_k, a, b)).$$

□

4. Prime Powers

Now, this question has been reduced to one in which the modulus is a prime power.

Definition 4.1 (Generalized WSS Prime)**.** *A Generalized Wall-Sun-Sun Prime under starting numbers (a, b)*[2]*, or GWSS prime, is a prime p such that $f_{a,b}(\pi(p, a, b) + 1) - a$ is a multiple of p^2.*

It has been proven that any existing WSS prime (a GWSS under $(1, 1)$) must be larger than 2^{64}. If a GWSS prime exists, then the period mod p^k is equal to the period mod p. On the other hand, suppose p is not a Wall-Sun-Sun.

Conjecture 4.2 ([1])**.** *If p is not a GWSS prime under a, b, then $\pi(p^k, a, b) = p^{k-1}\pi(p, a, b)$, for all $k > 1$.*

[1] The proof for this theorem is omitted; however, a nice proof can be found here: `https://kconrad.math.uconn.edu/blurbs/ugradnumthy/crt.pdf`

[2] Generalization of WSS primes under arbitrary starting numbers a, b. WSS primes under $(1, 1)$ can be found here: `https://en.wikipedia.org/wiki/Wall-Sun-Sun\_prime`

5. Part Two

In this section, we'll try to answer a different question: Given a period, what is a modulus and starting numbers that achieve that period? To answer that question, we'll need a couple lemmas.

Lemma 5.1. *Consider the sequence $\{f_{a,b}^m\}$. For all $k \geq 3$, the kth term of the sequence can be written as $f_{a,b}^m(k) \equiv F_{k-2}a + F_{k-1}b \pmod{m}$.*

Proof. We'll use strong induction. The first few base cases are trivial; note that $f_{a,b}^m(3) \equiv a+b$, and $f_{a,b}^m(4) \equiv a + 2b$. Now, assume this statement is true from $k = 3$ up to n. Then, we have

$$f_{a,b}^m(n+1) \equiv f_{a,b}^m(n) + f_{a,b}^m(n-1) \equiv F_{n-2}a + F_{n-1}b + F_{n-3}a + F_{n-2}b = F_{n-1}a + F_n b,$$

as desired.

□

Lemma 5.2. *For all positive integers $k \geq 1$,*

$$\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}^k = \begin{pmatrix} F_{k+1} & F_k \\ F_k & F_{k-1} \end{pmatrix}.$$

Proof. We'll proceed by induction. The base case is obviously true; $F_0 = 0$, $F_1 = 1$, and $F_2 = 1$. Now, assume this is true for $k = n$, so

$$\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}^k = \begin{pmatrix} F_{k+1} & F_k \\ F_k & F_{k-1} \end{pmatrix}.$$

Multiplying both sides by

$$\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix},$$

the result follows immediately. □

Corollary 5.3. *For all positive integers k,*

$$F_{k+1}F_{k-1} - F_k^2 = (-1)^k.$$

Proof. We take determinants on both sides of Lemma 3.2. The desired result follows immediately. □

6. Modulus Given Period

Now, the big theorem of this chapter:

Theorem 6.1. *Given a period k, there exists a sequence mod*

$$m = (-1)^{k+1} + F_{k+1} + F_{k-1} - 1,$$

where F_r denotes the rth Fibonacci number - note, this is the actual Fibonacci sequence - with period $p|k$.

7. Proof

Proof. If the period of $\{f_{a,b}^m\}$ divides k, it repeats, after k terms, so we have that

$$f_{a,b}^m(k+1) = a, \text{and}$$
$$f_{a,b}^m(k+2) = b.$$

By the result of Lemma 3.1, we can transform these equations:

$$F_{k-1}a + F_k b \equiv a \pmod{m}$$
$$F_k a + F_{k+1} b \equiv b \pmod{m}.$$

Through algebra, we find that

$$m = ((-1)^{k+1} + F_{k+1} + F_{k-1} - 1).$$

□

Conjecture 7.1. *The period k equals p for all values of p.*

Through a computer program [3], we have proven this conjecture for all values of $p < 10,000$. However, we are unsure if this pattern holds for all values of p.

8. Starting Numbers Given Period

We find that $a = F_k$, $b = 1 - F_{k-1}$ work. We can test this:

$$(F_{k-1} - 1)a + F_k b = F_k(F_{k-1} - 1 + b) \equiv 0 \pmod{m}, \text{ and}$$
$$F_k a + (F_{k+1} - 1)b = F_k^2 + F_{k+1} - 1 - F_{k+1}F_{k-1} + F_{k-1} = m \equiv 0 \pmod{m},$$

as desired. Note that b is negative in this example, so we add to m to get a positive number, $(-1)^{k+1} + F_{k+1}$, when considering the sequence.

References

[1] The Fibonacci Sequence Modulo M, by Marc Renault [Internet]. Rutgers.edu. 2024 [cited 2024 Feb 29]. Available from: https://sites.math.rutgers.edu/ zeilberg/essays683/renault.htm

[3] `https://github.com/sunaymid/modfib`