Spring 2020

An Exploration of the Use of the Fibonacci Sequence in Unrelated Mathematics Disciplines

Molly E. Boodey
University of New Hampshire, Durham

An Exploration of the Use of the Fibonacci Sequence in Unrelated Mathematics Disciplines

Molly Boodey
Advisor: Edward K. Hinson

Department of Mathematics and Statistics
University of New Hampshire

May 2020

Table of Contents

Abstract

The Fibonacci Sequence is recognizable to many – the pattern 1,1,2,3,5,8… is well known for its elegant simplicity. Although these numbers were studied before the time of Fibonacci, the sequence was first given attention in the book *Liber Abaci,* written by Fibonacci in 1202 [13]. While Fibonacci originally expressed this sequence as the number of rabbits present after *n* generations, today we discuss the sequence using the recursive relationship $F_n = F_{n-2} + F_{n-1}$ where $F_1 = F_2 = 1$. While this sequence appears simple on the surface, it is extremely versatile and widely applicable to the majority of mathematical disciplines. The goal of this paper is to demonstrate just how far-reaching this sequence is – specifically by looking into how it plays a role in areas as diverse as primality testing, Hilbert's problems, probability, convergence testing, and other unexpected areas of mathematics. In doing so, this thesis will illuminate connections between concepts that may at first seem unrelated and allow the reader to appreciate the value of this fundamental sequence.

Section One: What is the Fibonacci Sequence?

The Fibonacci Sequence is well-known amongst mathematicians and appears frequently in mathematics literature. The sequence was first given attention in the book *Liber Abaci* [13], where Fibonacci thought of the sequence in this way: "A certain man had one pair of rabbits together in a certain enclosed place, and one wishes to know how many are created from the pair in one year when it is the nature of them in a single month to bear another pair, and in the second month those born to bear also. … There will be two pairs in one month. One of these, namely the first, bears in the second month and thus there are in the second month 3 pairs…" [11, page 404]. Today, we define the Fibonacci numbers not through a hypothetical rabbit scenario, but rather through a sequence definition, shown below.

$$F_n = F_{n-2} + F_{n-1} \text{ for } n > 2$$
$$F_1 = F_2 = 1$$

The goal of this thesis is not to show every way in which the Fibonacci numbers can be connected to every other mathematical discipline. Rather, the purpose of this thesis is to show a connection between the Fibonacci numbers and as many unexpected areas of math as possible. I believe it will be eye-opening to readers to see just how far-reaching the Fibonacci numbers are in their connection to these many different areas of mathematics. Because of this, some well-known results may be omitted in favor of showing more obscure results in an unexpected place. For example, I will put emphasis on connecting Fibonacci numbers to topics such as Hilbert's problems or trigonometry, rather than to other Lucas sequences or to the golden ratio, for example.

Section Two: Combinatorics Connections

2.1 The Binet Formula

I begin by displaying a fundamental theorem known as the Binet Formula. A classic result from any introductory combinatorics course, this formula allows one to calculate the n_{th} Fibonacci number from n rather than from F_{n-1} and F_{n-2} as given in the sequence definition. For this reason, later sections will rely heavily on this formula.

Theorem 2.1.1: $F_n = \frac{1}{\sqrt{5}}\left(\frac{1+\sqrt{5}}{2}\right)^n - \frac{1}{\sqrt{5}}\left(\frac{1-\sqrt{5}}{2}\right)^n$

Proof

First, we recall the sequence definition. $F_n = F_{n-2} + F_{n-1}$ where $F_1 = F_2 = 1$

Now we will employ the method for solving linear recurrence relations described in [27, pg. 300].

$F_n = F_{n-2} + F_{n-1}$ becomes $f^n = f^{n-2} + f^{n-1}$ which is equivalent to $f^2 = f + 1$

Therefore $f = \frac{1 \pm \sqrt{5}}{2}$ and we can conclude $F_n = a\left(\frac{1+\sqrt{5}}{2}\right)^n + b\left(\frac{1-\sqrt{5}}{2}\right)^n$ where a, b are determined by the initial conditions.

Solving the simultaneous equations given by the initial conditions, $1 = a\left(\frac{1+\sqrt{5}}{2}\right)^1 + b\left(\frac{1-\sqrt{5}}{2}\right)^1$ and $1 = a\left(\frac{1+\sqrt{5}}{2}\right)^2 + b\left(\frac{1-\sqrt{5}}{2}\right)^2$, yields $a = \frac{1}{\sqrt{5}}$ and $b = -\frac{1}{\sqrt{5}}$.

Therefore, $F_n = \frac{1}{\sqrt{5}}\left(\frac{1+\sqrt{5}}{2}\right)^n - \frac{1}{\sqrt{5}}\left(\frac{1-\sqrt{5}}{2}\right)^n$

■

2.2 Fibonacci and Probability

The calculation of probability typically involves reducing a scenario into "cases". Thus the Fibonacci sequence easily lends itself to the calculation of probabilities since the value of F_n depends on the value of the previous "cases" F_{n-1} and F_{n-2}. Because of this, the connections between the Fibonacci numbers and probability are likely the least surprising of any connection detailed elsewhere in this thesis. In fact, most courses in combinatorics cover these connections, perhaps with more generic sequences where the initial conditions are not our conventional $F_1 = F_2 = 1$. The book *Applied Combinatorics* [27], for example, goes into this topic in some detail. Because of this I will provide a single example which illustrates the potential applications of this sequence to the computation of various probabilities.

Example 2.2.1: Suppose we have a fair coin where flipping a H gives the value +1 and flipping a tail resets your total to 0. In this case, the probability of obtaining a value of $n = 2$ after k flips (without a premature success) is $\frac{F_{k-1}}{2^k}$ (example from [26]).

Proof

Let $p(k)$ denote the probability of obtaining $n = 2$ after k flips.

First, note that $p(2) = p(HH) = \frac{1}{4}$ and $p(3) = p(THH) = \frac{1}{8}$

Therefore $p(k+3) = p(\text{k trials without double heads}) * p(THH)$

$$= \frac{\text{Number of ways to get no double heads in k trials}}{2^k} * p(THH)$$

Now we shall introduce some notation. Let a_k = number of arrangements of length k where there are no two consecutive heads and let $a_{k,i}$ = number of arrangements of length k where there are no two consecutive heads *and* the last tail is in the i^{th} position.

Using this notation, we note that $a_k = a_{k,k} + a_{k,k-1}$ since the last tail must be in either the k or $(k-1)$ position.

Now we note that $a_{k,k} = a_{k-1}$ since $a_{k,k}$ ends in a tail and therefore cannot end in a double heads.

We also note that $a_{k,k-1} = a_{k-2}$. This follows since $a_{k,k-1}$ must end in TH and therefore the three final positions contain no double heads.

From this we have that $a_k = a_{k-1} + a_{k-2}$.

We note that $a_1 = 2$ since a flip of either H or T is acceptable.

We note that $a_2 = 3$ since flips of HT, TH, and TT are acceptable.

Clearly, $a_k = F_{k+2}$

Using this information, we can compute our formula.

$$p(k+3) = \frac{\text{Number of ways to get no double heads in k trials}}{2^k} * p(THH) = \frac{a_k}{2^k} * \frac{1}{8} = \frac{a_k}{2^{k+3}} = \frac{F_{k+2}}{2^{k+3}}$$

Therefore, $p(k) = \frac{F_{k-1}}{2^k}$.

■

It is also worth noting that if we were to increase n, the desired "end score", we would require Tribonacci numbers (numbers defined by the relation $a_k = a_{k-1} + a_{k-2} + a_{k-3}$), Tetranacci numbers (defined by $a_k = a_{k-1} + a_{k-2} + a_{k-3} + a_{k-4}$), and beyond ($a_k = a_{k-1} + a_{k-2} + \cdots + a_{k-n}$). For example, with $n = 3$ we use Tribonacci numbers to obtain $p(k) = \frac{T_{k-1}}{2^k}$. In general, $p_n(k) = \frac{X_{k-1}}{2^k}$ where X is the Fibonacci sequence of order n.

Section Three: Number Theory Connections

This section is by far the most abundant. The set of Fibonacci numbers is a subset of the natural numbers, and by extension the integers, and therefore we can display connections between various number theoretic functions, well-known arrangements of integers, primes, and more. This section will culminate by detailing how the Fibonacci numbers were key in unlocking the

solution to Hilbert's Tenth Problem, a classic number theory question regarding the solvability of Diophantine equations.

3.1 The Legendre Symbol

A large portion of any number theory class is dedicated to the idea of congruence. In particular, two numbers a and b are said to be congruent (written $a \equiv b(\mathrm{mod}\, n)$) iff $n|(a-b)$. As an example, $13 \equiv 5(\mathrm{mod}\ 4)$ because $13-5=8$ and $4|8$. One can extend the idea of congruence by considering when certain congruency statements are solvable. For example, say we have $x^2 \equiv a(\mathrm{mod}\, b)$, where a and b are known. One way to solve this would involve testing $x = 0,1,2,3,4,5,6,7 \ldots b-1$ to see if any of these values provides a solution. If a solution was found, we would say a is a quadratic residue of b. If no solution was found, we would instead say a is a quadratic nonresidue of b. However, this is clearly not efficient, especially with a larger modulus. Instead, this is best solved through employing the use of the Legendre Symbol. Used to determine whether a number is a quadratic residue or not, it is defined in the following way [7],

$$\left(\frac{a}{p}\right) = \begin{cases} 1, & \text{a is a quadratic residue of p} \\ -1, & \text{a is a quadratic nonresidue of p} \end{cases}$$

where p is an odd prime and $\gcd(a,p)=1$. Interestingly, one is able to connect this symbol to the Fibonacci Sequence.

Theorem 3.1.1: If p is prime and the Legendre symbol is defined as above, then $F_p \equiv \left(\frac{p}{5}\right)(\mathrm{mod}\ p)$ and $F_{p-\left(\frac{p}{5}\right)} \equiv 0(\mathrm{mod}\ p)$ where $p \neq 5$ is an odd prime.

Proof (from [1])

First we will show $F_p \equiv \left(\frac{p}{5}\right)(\mathrm{mod}\ p)$

By Lemma 6.3.2 we know $2F_{p+r} \equiv \left(\frac{p}{5}\right)L_r + F_r \ (\mathrm{mod}\ p)$

Choose $r=0$ and obtain $2F_p \equiv 2\left(\frac{p}{5}\right) \ (\mathrm{mod}\ p)$

Since p is odd we conclude $F_p \equiv \left(\frac{p}{5}\right) \ (\mathrm{mod}\ p)$

Now we will show $F_{p-\left(\frac{p}{5}\right)} \equiv 0 \ (\mathrm{mod}\ p)$

We will again use Lemma 6.3.2 with $r=1$ and $r=-1$

Therefore $2F_{p+1} \equiv \left(\frac{p}{5}\right)+1 \ (\mathrm{mod}\ p)$ and $2F_{p-1} \equiv -\left(\frac{p}{5}\right)+1 \ (\mathrm{mod}\ p)$

If $\left(\frac{p}{5}\right) = -1$ then $F_{p+1} \equiv 0 \pmod{p}$ and if $\left(\frac{p}{5}\right) = 1$ then $F_{p-1} \equiv 0 \pmod{p}$

From this, we may conclude that $F_{p-\left(\frac{p}{5}\right)} \equiv 0 (\mathrm{mod}\ p)$

■

3.2 Fibonacci Numbers and the Mobius Function

The Mobius Function is a well-known number-theoretic function (a function whose domain is the set of positive integers) defined in the following way [7, pgs. 103, 112]

$$\mu(n) = \begin{cases} 1 & n = 1 \\ 0 & p^2 | n \text{ for some prime p} > 1 \\ (-1)^r & n = p_1 p_2 \dots p_r \text{ for distinct } p_i > 1 \end{cases}$$

See the table in the appendix for selected values.

Using this definition, we are able to derive a formula for the Fibonacci numbers using the Mobius Function and the corresponding Mobius Inversion Formula.

Theorem 3.2.1 For any natural number n it follows that $F_n = \prod_{d|n} F^*(d)$ where $F^*(d) = \prod_{k|d} {F_k}^{\mu(\frac{d}{k})}$

Proof (from [10])

This follows directly from the Mobius Inversion Formula (Lemma 6.3.3).

We know from our proof of the Binet Formula that the Fibonacci sequence can be written as a number theoretic function. Let us suppose that there is a second number theoretic function F^* such that

$$F_n = \prod_{m|n} F^*(m)$$

By Lemma 6.3.3, it follows that

$$F^*(m) = \prod_{k|m} {F_k}^{\mu(\frac{m}{k})}$$

Therefore, we have found a multiplicative function such that F_n can be decomposed into factors F^* where these factors are known as the primitive parts of F_n. We shall examine them further when examining the primality of F_n. Additionally, we have successfully found a way to connect the Fibonacci sequence to the Mobius function μ.

■

The first several values of $F^*(m)$ are given in the table on the following page.

Table 3.2.1 $F^*(m)$ Evaluated at Various Values of m			
m	$F^*(m)$ is product of	=	$F^*(m)$
1	${F_1}^{\mu(1)}$	1^1	1
2	${F_1}^{\mu(2)} \cdot {F_2}^{\mu(1)}$	$1^{-1}(1^1)$	1
3	${F_1}^{\mu(3)} \cdot {F_3}^{\mu(1)}$	$1^{-1}(2^1)$	2
4	${F_1}^{\mu(4)} \cdot {F_2}^{\mu(2)} \cdot {F_4}^{\mu(1)}$	$1^0(1^{-1})(3^1)$	3
5	${F_1}^{\mu(5)} \cdot {F_5}^{\mu(1)}$	$1^{-1}(5^1)$	5
6	${F_1}^{\mu(6)} \cdot {F_2}^{\mu(3)} \cdot {F_3}^{\mu(2)} \cdot {F_6}^{\mu(1)}$	$1^1(1^{-1})(2^{-1})(8^1)$	4
7	${F_1}^{\mu(7)} \cdot {F_7}^{\mu(1)}$	$1^{-1}(13^1)$	13
8	${F_1}^{\mu(8)} \cdot {F_2}^{\mu(4)} \cdot {F_4}^{\mu(2)} \cdot {F_8}^{\mu(1)}$	$1^1(1^0)(3^{-1})(21^1)$	7
9	${F_1}^{\mu(9)} \cdot {F_3}^{\mu(3)} \cdot {F_9}^{\mu(1)}$	$1^0(2^{-1})(34^1)$	17
10	${F_1}^{\mu(10)} \cdot {F_2}^{\mu(5)} \cdot {F_5}^{\mu(2)} \cdot {F_{10}}^{\mu(1)}$	$1^1(1^{-1})(5^{-1})(55^1)$	11
11	${F_1}^{\mu(11)} \cdot {F_{11}}^{\mu(1)}$	$1^{-1}(89^1)$	89

3.3 Fibonacci and Pascal's Triangle

There are two ways that we can compute the Fibonacci sequence using Pascal's triangle. One way of computing F_n involves looking solely at the nth row of the triangle and picking out the coefficients. Another way involves looking at the "rising diagonals" of the triangle and computing F_n through a sum of *non*-Fibonacci numbers.

$$\begin{array}{ccccccc} & & & \binom{0}{0} & & & \\ & & \binom{1}{0} & & \binom{1}{1} & & \\ & \binom{2}{0} & & \binom{2}{1} & & \binom{2}{2} & \\ \binom{3}{0} & & \binom{3}{1} & & \binom{3}{2} & & \binom{3}{3} \\ & & & \vdots & & & \end{array}$$

Figure 3.3.1: Pascal's Triangle Viewed as Arrangement of Binomial Coefficients

Method One Pascal's triangle is an arrangement of binomial coefficients (see figure above). As we read across the row n of the triangle, we get the coefficients $\binom{n}{0}, \binom{n}{1}, \binom{n}{2} \ldots \binom{n}{n}$. To compute F_n we plug these values into the expression $\frac{\binom{n}{1}+\binom{n}{3}5+\binom{n}{5}5^2+\cdots+\binom{n}{k}5^{(k-1)/2}+\cdots}{\binom{n}{0}+\binom{n}{2}+\binom{n}{4}+\cdots}$

Proof (from [17])

We begin with the Binet Formula $F_n = \frac{1}{2^n\sqrt{5}}\left(\left(1+\sqrt{5}\right)^n - \left(1-\sqrt{5}\right)^n\right)$

We can then apply the binomial theorem [7, pgs. 8-10]

$$F_n = \frac{1}{2^n\sqrt{5}}\left(\sum_{k=0}^{n}\binom{n}{k}\left(\sqrt{5}\right)^k - \sum_{k=0}^{n}\binom{n}{k}\left(-\sqrt{5}\right)^k\right)$$

$$= \frac{1}{2^n\sqrt{5}}\left(\left[1+\binom{n}{1}\left(\sqrt{5}\right)^1+\cdots+\left(\sqrt{5}\right)^n\right]-\left[1+\binom{n}{1}\left(-\sqrt{5}\right)^1+\cdots+\left(-\sqrt{5}\right)^n\right]\right)$$

$$= \frac{1}{2^n\sqrt{5}}\left(2\binom{n}{1}\sqrt{5}+2\binom{n}{3}\left(\sqrt{5}\right)^3+2\binom{n}{5}\left(\sqrt{5}\right)^5+\cdots\right)$$

$$= \frac{1}{2^{n-1}\sqrt{5}}\left(\binom{n}{1}\sqrt{5}+\binom{n}{3}\left(\sqrt{5}\right)^3+\binom{n}{5}\left(\sqrt{5}\right)^5+\cdots\right)$$

$$= \frac{1}{2^{n-1}}\left(\binom{n}{1}+\binom{n}{3}\left(\sqrt{5}\right)^2+\binom{n}{5}\left(\sqrt{5}\right)^4+\cdots\right)$$

$$= \frac{1}{2^{n-1}}\left(\binom{n}{1}+\binom{n}{3}5+\binom{n}{5}5^2+\cdots\right)$$

By Lemma 6.3.5 we have that $2^{n-1} = \binom{n}{0}+\binom{n}{2}+\binom{n}{4}+\cdots$

And therefore $F_n = \frac{\binom{n}{1}+\binom{n}{3}5+\binom{n}{5}5^2+\cdots}{\binom{n}{0}+\binom{n}{2}+\binom{n}{4}+\cdots}$

■

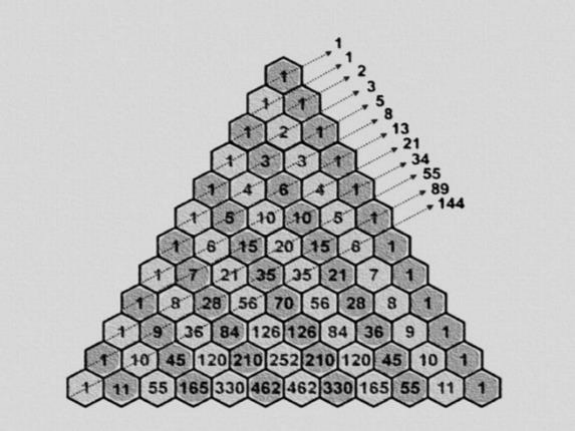

Figure 3.3.2: Rising Diagonals of Pascal's Triangle (from [24])

Method Two: The image above shows the rising diagonals of Pascal's triangle. As in method one, we know Pascal's triangle is based on binomial coefficients and therefore we can express the terms along these "rising" diagonals using $\binom{n}{k}$ where n is the row number and k is the column number (how far into the row you "go"). To sum along a rising diagonal, we begin with $\binom{n-1}{0}$ and then add $\binom{n-2}{1}$ and $\binom{n-3}{2}$ until you reach $\binom{n-1-\left\lfloor\frac{n-1}{2}\right\rfloor}{\left\lfloor\frac{n-1}{2}\right\rfloor}$. It seems that the result of this sum is F_n.

Therefore, we can hypothesize that $F_n = \sum_{k=0}^{k=\left\lfloor \frac{n-1}{2} \right\rfloor} \binom{n-1-k}{k}$ where the sum represents the "rising diagonals" of Pascal's Triangle.

Proof (by strong induction, from [21])

Clearly, the statement holds for $n = 1$.

Now we assume the statement holds for $1, 2, \ldots, n-1$ for some natural number $n \geq 1$.

Examine $\sum_{k=0}^{k=\left\lfloor \frac{n}{2} \right\rfloor} \binom{n-k}{k}$

Assume n is odd.

$$\sum_{k=0}^{k=\left\lfloor \frac{n}{2} \right\rfloor} \binom{n-k}{k} = \sum_{k=0}^{\left\lfloor \frac{n}{2} \right\rfloor} \binom{n-k-1}{k-1} + \sum_{k=0}^{\left\lfloor \frac{n}{2} \right\rfloor} \binom{n-k-1}{k} \text{ by Lemma 6.3.4}$$

$$= \sum_{k=0}^{\frac{n-1}{2}} \binom{n-k-1}{k-1} + \sum_{k=0}^{\left\lfloor \frac{n-1}{2} \right\rfloor} \binom{n-k-1}{k}$$

$$= \sum_{k=1}^{\frac{n-1}{2}} \binom{n-k-1}{k-1} + \binom{n-1}{-1} + \sum_{k=0}^{\left\lfloor \frac{n-1}{2} \right\rfloor} \binom{n-k-1}{k}$$

$$= \sum_{k=1}^{\frac{n-1}{2}} \binom{n-k-1}{k-1} + 0 + \sum_{k=0}^{\left\lfloor \frac{n-1}{2} \right\rfloor} \binom{n-k-1}{k}$$

$$= \sum_{j=0}^{\frac{n-1}{2}-1} \binom{n-j-2}{j} + \sum_{k=0}^{\left\lfloor \frac{n-1}{2} \right\rfloor} \binom{n-k-1}{k}$$

$$= \sum_{j=0}^{\frac{n-3}{2}} \binom{n-j-2}{j} + \sum_{k=0}^{\left\lfloor \frac{n-1}{2} \right\rfloor} \binom{n-k-1}{k}$$

$$= \sum_{j=0}^{\left\lceil \frac{n-2}{2} \right\rceil} \binom{n-j-2}{j} + \sum_{k=0}^{\left\lfloor \frac{n-1}{2} \right\rfloor} \binom{n-k-1}{k}$$

$$= F_{n-1} + F_n$$

$$= F_{n+1}$$

When n is even the proof is similar.

■

3.4 Fibonacci and the Euclidean Algorithm

The Euclidean Algorithm is a process that can be used to obtain the greatest common divisor of two integers a, b (Lemma 6.3.6). When considering the Euclidean Algorithm in the context of Fibonacci numbers, we come across the following theorem:

Theorem 3.4.1 (Lame's Theorem): The number of divisions needed to compute gcd(a,b) by the Euclidean Algorithm is no more than five times the number of decimal digits in b where $a \geq b \geq 2$

Proof (from [21])

Let a and b be given.

Apply the Euclidean Algorithm where we assume the algorithm terminates in n divisions.

$a = bq_1 + r_1$ where $0 \leq r_1 < b$

$b = r_1q_2 + r_2$ where $0 \leq r_2 < r_1$

$r_1 = r_2q_3 + r_3$ where $0 \leq r_3 < r_2$

$\vdots$

$r_{n-3} = r_{n-2}q_{n-2} + r_{n-1}$ where $0 \leq r_{n-1} < r_{n-2}$

$r_{n-2} = r_{n-1}q_{n-1}$

Note that $q_{n-1} > 1$ (aka $q_{n-1} \geq 2$) or we would have $r_{n-2} = r_{n-1}$

We will now work backwards.

We know $r_{n-1} \geq 1 = F_1$

Therefore $r_{n-2} \geq 2r_{n-1} \geq 2 = F_2$

Continuing, we see $r_{n-3} = r_{n-2}q_{n-2} + r_{n-1} > r_{n-2} + r_{n-1} > F_2 + F_1 = F_3$

Continuing yields $r_{n-k-1} > F_{k+1}$

And therefore, when $k = n - 1$ and $k = n$ (beginning of the algorithm), we have $b > F_n$ and $a > F_{n+1}$

We know b (the lesser number) is such that $b > F_n$ and therefore, from the note at the end of Lemma 6.3.8, $b > \frac{n}{5}$.

Therefore $5b > n$

Since we stated that this Euclidean Algorithm terminates in n steps, we can end the proof.

■

Theorem 3.4.2 (An Alternate Lame's Theorem): Let a, b be integers such that $a > b > 0$ where the Euclidean Algorithm to calculate $\gcd(a, b)$ requires n divisions. The smallest such pair a, b that satisfies these conditions is $a = F_{n+2}$ and $b = F_{n+1}$. Note that we define the "smallest pair" by choosing the pair with the least positive a value. If multiple pairs meet this criterion, we choose the pair among these with the least positive b value.

Proof (by strong induction on n, from [2])

First, we will show that $a \geq F_{n+2}$ and $b \geq F_{n+1}$

Assume $n = 1$.

For the Euclidean Algorithm to conclude after one division we must have $a = bq_1$. To minimize a where $a > b > 0$ it follows that $a = 2$ and $b = 1$ and we have $a \geq F_{1+2} = 2$ and $b \geq F_{1+1} = 1$ and the theorem holds.

Now we assume the statement holds for $1, 2, \ldots, n-1$ for some natural number $n \geq 1$.

Using a generic a and b, we perform the first two divisions.

$a = bq_1 + r_1$ where $0 \leq r_1 < b$

$b = r_1 q_2 + r_2$ where $0 \leq r_2 < r_1$

This second line computes $\gcd(b, r_1)$ and will terminate in $n-1$ steps. Therefore, we know by the inductive hypothesis that $b \geq F_{n+1}$ and $r_1 \geq F_n$.

Since $a \geq bq_1 + r_1 \geq b + r_1 \geq F_{n+1} + F_n = F_{n+2}$, we have shown that it does hold that $a \geq F_{n+2}$ and $b \geq F_{n+1}$.

Finally, we will show that if $a = F_{n+2}$ and $b = F_{n+1}$ the process does terminate in n divisions.

Note that $F_k = F_{k-1} + F_{k-2} < F_{k-1} + F_{k-1} = 2F_{k-1}$

Therefore, if $F_k = q_1(F_{k-1}) + r_1$ then $q_1 = 1$ and $r_1 = F_{k-2}$.

Thus, $\gcd(F_{n+2}, F_{n+1}) = \gcd(F_{n+1}, F_n) = \gcd(F_n, F_{n-1}) = \cdots = \gcd(2,1) = 1$, a total of n divisions.

■

Note that this proof also demonstrates that all adjacent Fibonacci numbers are relatively prime.

3.5 Fibonacci and Primes

Unfortunately, according to [7], "not only is there no known device for predicting which F_n are prime, but it is not certain whether the number of prime Fibonacci numbers is infinite". However, there are a great number of theorems about the Fibonacci sequence and prime numbers that exist

and are valuable in our understanding of prime numbers. I will begin this section with a few intriguing results about primes and Fibonacci numbers in general and then proceed to examining the idea of primality testing using Fibonacci numbers.

The first topic we will discuss involves looking at the Fibonacci sequence modulo some number. This is intriguing for both prime and composite moduli; however, prime moduli are far easier to handle and therefore we will examine them in more depth. In either case, taking the modulus of every number in the Fibonacci sequence yields a periodic sequence of numbers. For example, mod(3) the Fibonacci sequence begins 1,1,2,0,2,2,1,0 and then repeats. Therefore, the period of $F_n \pmod 3$ has length 8. We denote this by $k(3) = 8$. By Lemma 6.3.9, we can see that this sequence is indeed always periodic. We will now examine its value for both prime and composite moduli.

Theorem 3.5.1: Let p be prime. If $p = 2$ then $k = 3$ and if $p = 5$ then $k = 20$. For all other primes, if $p \equiv \pm 1 \pmod{10}$ then $k(p)|p-1$ and if $p \equiv \pm 3 \pmod{10}$ then $k(p)|2p+2$.

Proof (from [28])

The cases where $p = 2$ and $p = 5$ can be seen by inspection.

Now, let us examine the case where $p \equiv \pm 3 \pmod{10}$

By [7, pgs. 88, 171, 191] we know that 5 is a quadratic nonresidue (mod p) and therefore $5^{\frac{p-1}{2}} \equiv -1 \pmod p$

By the section on Pascal's Triangle, $F_n = 2^{1-n}[\binom{n}{1} + 5\binom{n}{3} + 5^2\binom{n}{5} + \cdots]$

Therefore $2^{n-1}F_n = \binom{n}{1} + 5\binom{n}{3} + 5^2\binom{n}{5} + \cdots$

Let $n = p$ and obtain $2^{p-1}F_p = [\binom{p}{1} + 5\binom{p}{3} + \cdots + 5^{\frac{p-1}{2}}\binom{p}{p} + \cdots]$ where the remaining terms are 0

$\therefore 2^{p-1}F_p \equiv [\binom{p}{1} + 5\binom{p}{3} + \cdots + 5^{\frac{p-1}{2}}\binom{p}{p}] \pmod p$

By [7, pg. 180] we have that $2^{\frac{p-1}{2}} \equiv \pm 1 \pmod p$ and it follows that $2^{p-1} \equiv 1 \pmod p$

Therefore $F_p \equiv [\binom{p}{1} + 5\binom{p}{3} + \cdots + 5^{\frac{p-1}{2}}\binom{p}{p}] \pmod p$

Since $p|\binom{p}{k}$ where $k < p$ we know that $F_p \equiv 5^{\frac{p-1}{2}}\binom{p}{p} \pmod p$ and thus $F_p \equiv -1 \pmod p$

Now let $n = p + 1$ in $F_n = 2^{1-n}[\binom{n}{1} + 5\binom{n}{3} + 5^2\binom{n}{5} + \cdots]$

It follows that $F_{p+1} = 2^{-p}[\binom{p+1}{1} + 5\binom{p+1}{3} + \cdots + 5^{\frac{p-1}{2}}\binom{p+1}{p} + \cdots]$ where the remaining terms are 0

Therefore, $F_{p+1} \equiv 2^{-p}[\binom{p+1}{1} + 5\binom{p+1}{3} + \cdots + 5^{\frac{p-1}{2}}\binom{p+1}{p} + \cdots](\text{mod } p)$

Let us examine the middle terms $5\binom{p+1}{3} \ldots 5^{\frac{p-3}{2}}\binom{p+1}{p-2}$

Specifically, we want to examine $\binom{p+1}{k}$ where $1 < k < p$ (or $1 < p + 1 - k$)

Here, $\binom{p+1}{k} = \frac{(p+1)!}{(p+1-k)!k!}$

Since $p + 1 - k > 1$ we may write this as $\frac{(p+1)(p)\ldots(p+2-k)(p+1-k)!}{(p+1-k)!k!}$

$$= \frac{(p+1)(p)\ldots(p+2-k)}{k!},$$

$$\equiv 0(\text{mod } p)$$

Therefore, we have that $F_{p+1} \equiv 2^{-p}[\binom{p+1}{1} + 5^{\frac{p-1}{2}}\binom{p+1}{p}](\text{mod } p)$

Since we know that $5^{\frac{p-1}{2}} \equiv -1$ and it always holds that $\binom{p+1}{1} = \binom{p+1}{p}$ we have

$F_{p+1} \equiv 2^{-p}[\binom{p+1}{1} - \binom{p+1}{1}](\text{mod } p)$

$$\equiv 2^{-p}(0)(\text{mod } p)$$

$$\equiv 0(\text{mod } p)$$

Thus $F_p \equiv -1(\text{mod } p)$ and $F_{p+1} \equiv 0(\text{mod } p)$ and we have the following:

$$F_{p+2} \equiv -1 \equiv -F_1(\text{mod } p)$$

$$F_{p+3} \equiv 0 + (-1) \equiv -1 \equiv -F_2(\text{mod } p)$$

$$F_{p+4} \equiv -F_1 - F_2 \equiv -F_3(\text{mod } p)$$

$$\vdots$$

$$F_{p+k} \equiv -F_{k-1}(\text{mod } p)$$

Let $k = p + 3$ and we see that $F_{2p+3} \equiv -F_{p+2}(\text{mod } p) \equiv 1 \equiv F_1(\text{mod } p)$

Let $k = p + 4$ and we see that $F_{2p+4} \equiv -F_{p+3}(\text{mod } p) \equiv 1 \equiv F_2(\text{mod } p)$

Therefore, we may conclude $k(p)$ repeats at most every $(2p + 3) - 1 = 2p + 2$ and therefore $k(p)|(2p + 2)$

When $p \equiv \pm 1(\text{mod } 10)$ a similar argument shows that $k(p)|p - 1$

■

We can now use this theorem to help us determine the period length of the Fibonacci sequence with non-prime modulus. See the theorem below.

Theorem 3.5.2: If $m = \prod {p_i}^{a_i}$ then $k(m) = lcm\{k_i\}$ where $k_i = k({p_i}^{a_i})$

Proof

See [28, pg. 526]

For example, if we want $k(10)$ we can see that $k(2) = 3$ and $k(5) = 20$ and conclude that $k(10) = 60$. The table below gives the first 20 $k(n)$ values. Note that while the table makes it seem as though $k(p) = 2p + 2$ or $p - 1$ for $p > 5$, this does not always hold. For example, this would imply $\mathrm{k}(29) = 28$ when in reality $k(29) = 14$.

Table 3.5.1 First 20 $k(n)$ Values and $2p + 2, p - 1$ Values Where Applicable

n	$k(n)$	$2p+2$	$p-1$	n	$k(n)$	$2p+2$	$p-1$
1	1			11	10		10
2	3			12	24		
3	8	8		13	28	28	
4	6			14	48		
5	20			15	40		
6	24			16	24		
7	16	16		17	36	36	
8	12			18	24		
9	24			19	18		18
10	60			20	60		

Before continuing, we should note the following:

Theorem 3.5.3: If F_n is prime then $n = 4$ or n is prime.

Proof (by contrapositive):

Note that if $F_x = F_y$ then $x = y$ or $x, y \in \{1,2\}$

Assume $n > 4$ is composite

Since n is composite, $n = ab$ for some numbers $a, b > 1$

Therefore, $n \neq a$ and $n \neq b$

By Lemma 6.3.12, $F_a | F_n$ and $F_b | F_n$

If $a = 2$ then $b > 2$

Otherwise, $a > 2$ so at least one of a, b is greater than 2

Without loss of generality, we may assume $a > 2$

Since $a, n > 2$ we know that $F_a \neq F_n$

Also note that since $a > 2$ it follows that $F_a \neq 1$

Since $F_a | F_n$ where $F_a \neq F_n$ and $F_a \neq 1$ we conclude F_n is not prime.

■

Note that the converse is not true. 19 is prime, however, $F_{19} = 4181$, is not.
Our next result examines the idea of prime divisors of generic Fibonacci numbers.

Theorem 3.5.4 (Carmichael's Theorem): $\forall n \geq 13, \exists$ prime p such that $p | F_n$ and $p \nmid F_k$ for $k < m$

Proof

Omitted, see [3]

■

This theorem implies that every Fibonacci number above F_{13} has a "new" prime factor that no Fibonacci number has had before. For example, the only prime factors before F_{13} are 2,3,5,7,11,13,17 and 89. We then begin to see a "new" prime factor as the index of the Fibonacci number increases — F_{13} is divisible by 233, F_{14} is divisible by 29, F_{15} is divisible by 61, F_{16} is divisible by 47, etc. We call these "new" primes characteristic primes.

In a paper by Jarden [18] he defines F'_n as the largest factor of F_n that is relatively prime to every earlier Fibonacci number. He goes on to state that $F'_p = F_p$ for prime p. In other words, he claims that the factors of F_p are all characteristic for prime p. I will show this fact in the theorem below using Lemma 6.3.14, obtained from [23].

Theorem 3.5.5: For odd prime p, F_p is the product of prime factors which are all characteristic or is prime itself.

Proof (by contradiction):

If F_p is prime then it is clear that the value of F_p is characteristic because no earlier Fibonacci number would have this prime as a factor.

Therefore, we can assume that F_p has factors other than 1 and itself. Let us assume that at least one of these prime factors is not characteristic, meaning it has appeared in the factorization of an earlier Fibonacci number. Call this earlier Fibonacci number F_k.

Therefore, $\gcd(F_p, F_k) \neq 1$

By Lemma 6.3.14 we know $\gcd(F_p, F_k) = F_{gcd\ (p,k)}$

Since p is prime and $k < p$ we know that $\gcd(p, k) = 1$

Therefore $\gcd(F_p, F_k) = F_{gcd\ (p,k)} = F_1 = 1$, a contradiction.

■

The table below demonstrates the above three theorems. We can see that F_{19} demonstrates the above theorem since both of its factors are characteristic. We can also see that F_n is prime only where n is prime. Finally, we can see that every Fibonacci number with index $n \geq 13$ has a characteristic prime factor.

Table 3.5.2 First 20 Factored Fibonacci Numbers with Highlighted Odd Prime Indices and Bolded Characteristic Prime Factors

n	F_n	n	F_n
1	1	11	**89**
2	1	12	$3^2 \cdot 2^4$
3	**2**	13	**233**
4	**3**	14	$13 \cdot$ **29**
5	**5**	15	$2 \cdot 5 \cdot$ **61**
6	2^3	16	$3 \cdot 7 \cdot$ **47**
7	**13**	17	**1597**
8	$3 \cdot$ **7**	18	$2^3 \cdot 17 \cdot$ **19**
9	$2 \cdot$ **17**	19	**37 · 113**
10	$5 \cdot$ **11**	20	$3 \cdot 5 \cdot 11 \cdot$ **41**

The Fibonacci numbers are also useful in primality testing. By this, I mean that tools exist for determining the primality of F_n. The remainder of this section will be devoted to this topic.

A paper from Brillhart [4] describes several theorems for testing the primality of N by examining $N \pm 1$. Because of this, there is great benefit in finding more efficient ways to factor $N \pm 1$, or in this case, $F_n \pm 1$. Luckily, in the case of Fibonacci numbers, this can be accomplished through various identities for $F_n \pm 1$. Some of these are detailed in [5] and [6]. The following two theorems

exhibit this. Theorem 3.5.6 is a primality test from [4] and Theorem 3.5.7 is a method of factorizing $F_n - 1$ so that the primality test may be applied.

Theorem 3.5.6: Let $N - 1 = mp$ where p is an odd prime such that $2p + 1 > \sqrt{N}$. If there exists a such that $a^{\frac{N-1}{2}} \equiv -1 (\text{mod } N)$ but $a^{\frac{m}{2}} \not\equiv -1 (\text{mod } N)$ then N is prime.

Proof

Omitted, see [4]

■

Theorem 3.5.7: $F_{4k+1} - 1 = F_k L_k L_{2k+1}$ where L_n denotes the nth Lucas number, defined in the Appendix.

Proof

Omitted, see [5] and [6]

■

To see how all of this comes together and how we are able to assess the primality of F_n using the information above, I will provide an example.

Example: Prove $F_{13} = 233$ is prime using Theorems 3.5.6 and 3.5.7.

Proof

Using the Theorem 3.5.7 we know $F_{13} - 1 = F_3 L_3 L_7 = 2(4)(29)$, We then apply Theorem 3.5.6. Here, $m = 8$ and $p = 29$. Of course, $2(29) + 1 > \sqrt{233}$. Now we note that if $a = 3$ then $3^{\frac{233-1}{2}} \equiv 3^{116} \equiv -1 (\text{mod } 233)$ but $3^{\frac{8}{2}} \equiv 81 \not\equiv -1 (\text{mod } 233)$ and therefore we have found a value of a such that $a^{\frac{N-1}{2}} \equiv -1 (mod\ N)$ but $a^{\frac{m}{2}} \not\equiv -1 (\text{mod } N)$ and thus we can conclude that F_{13} is prime.

■

As of 1999, it had been shown that F_n is prime for n = 3, 4, 5, 7, 11, 13, 17, 23, 29, 43, 47, 83, 131, 137, 359, 431, 433, 449, 509, 569, 571, 2971, 4723, 5387, 9311 and likely prime for $n =$ 9677, 14431, 25561, 30757, 35999, 37511. No other F_n is prime for $n \leq 50000$ [10].

It is also worth noting that we can use similar strategies to assess the primality of ${F^*}_n$, the primitive factors of F_n described in Section 3.2. First, we pull two other useful theorems from [4] and [5].

Theorem 3.5.8: Let $N-1=\prod {p_i}^{k_i}$. If for each p_i there exists an a_i such that ${a_i}^{N-1} \equiv 1 (\text{mod } N)$, $1 < a_i < N-1$, and ${a_i}^{\frac{N-1}{p_i}} \not\equiv 1 (\text{mod } N)$ then N is prime.

Proof

Omitted, see [4]

■

Theorem 3.5.9: ${F^*}_{5k} - 1 = 5F_{k-1}{F^2}_k F_{k+1}$ where $k \geq 7$ and prime.

Proof

Omitted, see [5]

■

Example 3.5.10 Say we wanted to prove ${F^*}_{35} = 141961$ is prime.

Proof

Using Theorem 3.5.9, we know ${F^*}_{35} - 1 = 5F_6{F^2}_7 F_8 = 5(2^3)(13^2)(3)(7)$. Let $p_1 = 2, p_2 = 3, p_3 = 5, p_4 = 7,$ and $p_5 = 13$. We then determine that values of a_i that satisfy Theorem 3.5.8 are $a_1 = 11$ and $a_2 = a_3 = a_4 = a_5 = 2$ and conclude that ${F^*}_{35}$ is prime.

■

As of 1999, it had been demonstrated that ${F_n}^*$ is prime for odd numbers n = 9, 15, 21, 33, 35, 39, 45, 51, 63, 65, 75, 93, 105, 111, 119, 121, 123, 135, 145, 185, 195, 201, 207, 209, 225, 231, 235, 245, 285, 287, 299, 301, 321, 335, 363, 399, 423, 453, 473, 693, 707, 771, 1047, 1113, 1215, 1365, 1371, 1387, 1533, 1537, 1539, 2185, 2285, 2289, 2361, 2511, 2587, 2733, 2877, 3211, 3339, 3757, 3857, 3867, 3927, 4025, 4881, 5579, 5691, 6285, 6705, 7035, 7225, 7917, 8275, 9813, 10025, 10377, 11545, 11915, 12717, 14203 and likely prime for 24 other values of $n \leq 20{,}000$. This list excludes those n for which F_n is prime and is complete given these stipulations. [10]

3.6 Fibonacci Numbers and Polynomials

Interestingly, it is possible to find a polynomial whose positive outputs are identically the Fibonacci numbers. I display this polynomial (and its corresponding proof) below. We then apply many of the lemmas used to find this polynomial to Hilbert's Tenth Problem in Section 3.7.

Theorem 3.6.1: The set of Fibonacci numbers is identical with the set of positive values of $2y^4x + y^3x^2 - 2y^2x^3 - y^5 - yx^4 + 2y$ for $x, y \in \mathbb{N}$.

Proof (from [19])

If y is Fibonacci, then $\exists x \in Z^+$ such that $(y^2 - xy - x^2)^2 = 1$ by Lemma 6.3.18.

Therefore, $y(2 - (y^2 - xy - x^2)^2) = y$

Hence, the set of Fibonacci numbers is a subset of the values of this polynomial.

Now we will show that only Fibonacci numbers are positive outputs of $y(2 - (y^2 - xy - x^2)^2)$.

Assume $w = y(2 - (y^2 - xy - x^2)^2)$ where $w > 0$

Since $w, y > 0$ it follows that $0 < (y^2 - xy - x^2)^2 < 2$ (by Lemma 6.3.19)

This implies $(y^2 - xy - x^2)^2 = 1$ and y is Fibonacci by Lemma 6.3.18.

Using the definition of w, see that $w = y$ and therefore w is Fibonacci.

■

An illustration of this fact is given in the table below.

Table 3.6.1 Values of $2y^4x + y^3x^2 - 2y^2x^3 - y^5 - yx^4 + 2y$ With Highlighted Positive Values

$y\backslash x$	1	2	3	4	5	6	7	8	9
1	1	-23	-119	-359	-839	-1679	-3023	-5039	-7919
2	2	-28	-238	-796	-1918	-3868	-6958	-11548	-18046
3	-69	3	-237	-1077	-2877	-6069	-11157	-18717	-29397
4	-476	-56	-92	-1016	-3356	-7736	-14876	-25592	-40796
5	-1795	-595	5	-595	-3115	-8395	-17395	-31195	-50995
6	-5034	-2388	-474	-84	-2154	-7764	-18138	-34644	-58794
7	-11753	-6713	-2513	-161	-833	-5873	-16793	-35273	-63161
8	-24184	-15472	-7672	-2032	8	-3184	-13432	-32752	-63352
9	-45351	-31311	-18207	-7551	-1071	-711	-8631	-27207	-59031
10	-79190	-57740	-37190	-19340	-6230	-140	-3590	-19340	-50390
11	-130669	-99253	-68629	-40909	-18469	-3949	-253	-10549	-38269
12	-205908	-161448	-117588	-76776	-41748	-15528	-1428	-3048	-24276
13	-312299	-251147	-190307	-132587	-81107	-39299	-10907	13	-10907
14	-458626	-376516	-294322	-215236	-142786	-80836	-33586	-5572	-1666

3.7 A Discussion of Hilbert's Tenth Problem

To begin, it is important to obtain rigorous definitions for Diophantine equations, functions and sets, the subjects of Hilbert's Tenth Problem. According to [7, pg. 33], "it is customary to apply the term Diophantine equation to any equation in one or more unknowns that is to be solved in the integers". The paper found in [8] defines it more exactly, writing "A Diophantine equation is an equation of the form $P(x_1, \dots, x_n) = 0$ where P is a polynomial with integer coefficients and a solution in integers is required". The paper found in [9] then defines a Diophantine set as a set $S = \{(x_1, \dots, x_n) | \exists (y_1, \dots, y_m)$ where $P(x_1, \dots, x_n, y_1, \dots, y_m) = 0$ and $y_i \in \mathbb{Z}^+\}$, essentially a collection of n-tuples which are solutions of some Diophantine equation P. Furthermore, a Diophantine function is a function f where the set $\{(x_1, \dots, x_n, y) | \, y = f(x_1, \dots, x_n)\}$ is a Diophantine set [9]. To clarify these terms, I provide a few examples. A sample Diophantine equation is $172x + 20y - 1000 = 0$ [7, pg. 35]. The set of composite numbers is an example of a Diophantine set where $S = \{x | \exists (y, z)$ such that $x - (y + 1)(z + 1) = 0$ and $y, z \in \mathbb{Z}^+\}$ [9]. An example of a Diophantine function is F_{2n}, as we will show below [22].

In 1900, when David Hilbert presented a list of 23 questions relating to the domain of number theory, his tenth problem focused on the solvability of these Diophantine equations [22]. He stated his question in the following way: "Given a Diophantine equation with any number of unknown quantities and with rational integral numerical coefficients: To devise a process according to which it can be determined by a finite number of operations whether the equation is solvable in rational integers" [22]. In other words, he wanted to know whether there existed a single algorithm that could determine the solvability of a *generic* Diophantine equation. In 1971, this problem was finally answered in the negative: there is no general algorithm that will work for every possible Diophantine equation [22]. However, the beginning stages of the solution actually appeared in a 1961 paper by Davis, Putnam and Robinson which showed that Hilbert's algorithm could not exist if there existed a Diophantine function with exponential growth [8, 19]. The 1971 breakthrough occurred when mathematicians were able to show that F_{2n} meets these criteria [22]. This is shown below in Theorem 3.7.1.

Theorem 3.7.1: F_{2u} is a Diophantine function and has exponential growth. Using the results stated above, this implies Hilbert's Tenth Problem is unsolvable.

Proof (from [22])

Unless stated otherwise, assume all variables $a \ldots z$ are positive.

First, we will show that F_{2u} has exponential growth (this means that $\forall u\ F_{2u} \leq u^u$ and for any k we can find u such that $u^k < F_{2u}$).

Using Lemmas 6.3.20 and 6.3.21 we see that $2^{u-1} \leq F_{2u} < 3^u$ and therefore $\forall u\ F_{2u} \leq u^u$

Now let k be arbitrary. $u^k < 2^{u-1}$ holds for some u and therefore u can be found such that $u^k < F_{2u}$

Conclude F_{2u} has exponential growth.

Now we will show that F_{2u} is a Diophantine function.

To do this, we will first show that there exist numbers such that iff

$$u < l$$
$$v < l$$
$$l^2 - lz - z^2 = 1$$
$$g^2 - gh - h^2 = 1$$
$$l^2 | g$$
$$l | m - 2$$
$$2h + g | m - 3$$
$$x^2 - mxy + y^2 = 1$$
$$l | x - u$$
$$\text{and } 2h + g | x - v$$

then $v = F_{2u}$

($\Rightarrow$)

Since $l^2 - lz - z^2 = 1$ and $g^2 - gh - h^2 = 1$, by Lemma 6.3.16 we have l is Fibonacci ($l = F_s$), $h = F_{2k}$ and $g = F_{2k+1}$

Therefore $2h + g = 2F_{2k} + F_{2k+1} = F_{2k} + F_{2k+2}$

Since $l^2 | g$, $l = F_s$ and $g = F_{2k+1}$ we have ${F_s}^2 | F_{2k+1}$ and by Lemma 6.3.22 $F_s = l | 2k + 1$

Since $u < l$ we have that $l \geq 2$

$l \geq 2$ and $l | m - 2$ imply $m \geq 2$

Let $Y_{i,0} = 0, Y_{i,1} = 1$ and $Y_{i,j+1} = iY_{i,j} - Y_{i,j-1}$

$m \geq 2$ and $x^2 - mxy + y^2 = 1$ and Lemma 6.3.23 imply that $x = Y_{m,n}$

$2h + g | m - 3$, and $2h + g = F_{2k} + F_{2k+2}$ imply $F_{2k} + F_{2k+2} | m - 3$

$m \geq 2$, $F_{2k} + F_{2k+2} | m - 3, x = Y_{m,n}$ and Lemma 6.3.24 imply that $x \equiv F_{2n} (\text{mod } F_{2k} + F_{2k+2})$

$(2h + g) = F_{2k} + F_{2k+2} | x - v$ and $x \equiv F_{2n} (\text{mod } F_{2k} + F_{2k+2})$ imply $v \equiv F_{2n} (\text{mod } F_{2k} + F_{2k+2})$

To ease notation, let $n = (2k+1)i + j$ where $0 \leq j < 2k+1$

Using Lemma 6.3.25 and $v \equiv F_{2n} (\text{mod } F_{2k} + F_{2k+2})$ we have $v \equiv F_{2j} (\text{mod } F_{2k} + F_{2k+2})$

$l^2 | g$ shows $l \leq g$

$v < l \leq g$, $h = F_{2k}$ and $g = F_{2k+1}$ show that $v < F_{2k+1}$

Therefore $v < F_{2k+2} + F_{2k}$

Since $v \equiv F_{2j} (\text{mod } F_{2k} + F_{2k+2})$, Lemma 6.3.26 shows $v + F_{2(2k+1-j)} \equiv 0 (\text{mod } F_{2k} + F_{2k+2})$

Therefore, $v + F_{2(2k+1-j)} \geq F_{2k} + F_{2k+2}$

Using $v < F_{2k+1}$ we have $F_{2(2k+1-j)} \geq F_{2k} + F_{2k+2} - v > F_{2k} + F_{2k+2} - F_{2k+1} > F_{2k}$

This implies $2k + 1 - j > k$ and therefore $k + 1 > j$

This implies $F_{2j} < F_{2k+2}$ and therefore $F_{2j} < F_{2k} + F_{2k+2}$

$F_{2j} < F_{2k} + F_{2k+2}$, $v < F_{2k} + F_{2k+2}$ and $v \equiv F_{2j} (\text{mod } F_{2k} + F_{2k+2})$ show that $v = F_{2j}$

By Lemma 6.3.30 we have $j \leq F_{2j} = v$ and since $v < l$ we have that $j \leq v < l$

$x = Y_{m,n}$ and $l | m - 2$ and Lemma 6.3.24 show that $x \equiv n (\text{mod } l)$

Since $l | x - u$ and $x \equiv n (\text{mod } l)$ we have that $u \equiv n (\text{mod } l)$

Above, we stated that $n = (2k+1)i + j$. Since $l | 2k + 1$ and $u \equiv n (\text{mod } l)$ we have that $u \equiv j (\text{mod } l)$

$u < l$, $j < l$ and $u \equiv j (\text{mod } l)$ show that $u = j$

Therefore, since $v = F_{2j}$, we have that $v = F_{2u}$

($\Leftarrow$)

First, let $l = F_{24u+1}$ and $z = F_{24u}$

Using Lemma 6.3.21, note that $Y_{3,12u} = F_{24u}$

We than apply Lemma 6.3.20 and obtain $2^{12u-1} \leq F_{24u}$

Therefore $u < 2^{12u-1} \leq F_{24u+1} = l$

Recall that $l = F_{24u+1}$ and thus $v = F_{2u} < F_{24u+1} = l$

Applying $= F_{24u+1}$ and $z = F_{24u}$ yields $l^2 - lz - z^2 = 1$ by Lemma 6.3.15

Let $g = F_{l(24u+1)}$ and $h = F_{l(24u+1)-1}$

Using Lemma 6.3.11 with $i = 8u, s = 3$ and $j = 1$ we obtain $F_{24u+1} \equiv 3^{8u} (\text{mod } 2)$

Therefore, $l \equiv 1 (\text{mod } 2)$ and $l(24u + 1) - 1 \equiv 0 (\text{mod } 2)$

In Lemma 6.3.15, let $F_{j+1} = g$ and $F_j = h$ to get $g^2 - hg - h^2 = (-1)^{l(24u+1)-1} = 1$

Using Lemma 6.3.27 with $s = 24u + 1$ and $t = l$ gives $l^2 | F_{l(24u+1)} = g$

Using Lemma 6.3.11 with $i = 6u, s = 4$ and $j = 1$ we obtain $F_{24u+1} \equiv 5^{6u} \equiv 1 (\text{mod } 3)$

Therefore, $l \equiv 1 (\text{mod } 3)$ and $l(24u + 1) - 1 \equiv 0 (\text{mod } 3)$

Let us write $l(24u + 1) - 1 = 3t$ for some t

Therefore, using Lemma 6.3.11, $h = F_{l(24u+1)-1} = F_{3t} \equiv F_0 {F_4}^t (\text{mod } 2) \equiv 0 (\text{mod } 2)$ and we conclude h is even

Set $m = 3 + (2h + g)\frac{h}{2}$

Since $l^2 | g$ we know $m \equiv 3 + (2h)\frac{h}{2} (\text{mod } l) \equiv 3 + h^2 (\text{mod } l)$

Since $g^2 - gh - h^2 = 1$ and $l^2 | g$ we have that $-h^2 \equiv 1 (\text{mod } l)$

Therefore, $m \equiv 3 - 1 (\text{mod } l)$ and we have $l | m - 2$

Also $2h + g | m - 3$ from $m - 3 = (2h + g)\frac{h}{2}$

Set $x = Y_{m,u}$ and $y = Y_{m,u+1}$

Using Lemma 6.3.28, it is clear that $x^2 - mxy + y^2 = 1$

Using the fact that $l | m - 2$ and $x = Y_{m,u}$ and $y = Y_{m,u+1}$, as well as Lemma 6.3.24 we get $x \equiv u (\text{mod } l)$ and therefore $l | x - u$

Using $2h + g | m - 3$, $x = Y_{m,u}$ and $y = Y_{m,u+1}$, and $v = F_{2u}$, as well as Lemma 6.3.24 again, we get $x \equiv v (\text{mod } 2h + g)$ and therefore $2h + g | x - v$

Thus, all of the necessary conditions have been demonstrated.

To finally show that $v = F_{2u}$ is a Diophantine function we note that the set of conditions described above is identical with the set of equations

$$u + a = l$$
$$v + b = l$$
$$l^2 - lz - z^2 = 1$$
$$g^2 - gh - h^2 = 1$$
$$l^2 c = g$$
$$ld = m - 2$$
$$(2h + g)e = m - 3$$
$$x^2 - mxy + y^2 = 1$$
$$l(p - q) = x - u$$
$$(2h + g)(r - s) = x - v$$

Now note that if we have multiple expressions $f_1 \ldots f_k = 0$, we can express them with the single equation ${f_1}^2 + {f_2}^2 + \cdots + {f_k}^2 = 0$ and this the above equations are sufficient to conclude F_{2u} is a Diophantine function.

■

Section Four: Fibonacci and Trigonometry

Using the Binet Formula, we can easily connect the Fibonacci Sequence to a trigonometric function simply by expressing $\frac{1+\sqrt{5}}{2}$ and $\frac{1-\sqrt{5}}{2}$ as values of the cosine function. This is detailed in Section 4.1. However, we can also express the Fibonacci numbers by evaluating the argument of a cosine function at values that depend on n. This theorem is detailed in Section 4.2.

4.1 A Fibonacci Cosine Expression

Theorem 4.1.1: $F_n = \frac{2^n}{\sqrt{5}}\left(\cos^{\mathrm{n}}\frac{\pi}{5} - \cos^{\mathrm{n}}\frac{3\pi}{5}\right)$

Proof (from [13, pg. 67])

The Binet Formula establishes that $F_n = \frac{1}{\sqrt{5}}\left(\left(\frac{1+\sqrt{5}}{2}\right)^n - \left(\frac{1-\sqrt{5}}{2}\right)^n\right)$

We know $\frac{1+\sqrt{5}}{2} = 2\cos\frac{\pi}{5}$ and $\frac{1-\sqrt{5}}{2} = 2\cos\frac{3\pi}{5}$

Therefore $F_n = \frac{1}{\sqrt{5}}\left(\left(2\cos\frac{\pi}{5}\right)^n - \left(2\cos\frac{3\pi}{5}\right)^n\right)$

Therefore $F_n = \frac{2^n}{\sqrt{5}}\left(\cos^{\mathrm{n}}\frac{\pi}{5} - \cos^{\mathrm{n}}\frac{3\pi}{5}\right)$

■

4.2 A More Elaborate Trigonometric Expression for F_n

Theorem 4.2.1: $F_n = \prod_{k=1}^{\left\lfloor\frac{n-1}{2}\right\rfloor} 3 + 2\cos\frac{2k\pi}{n}$

Proof (from [12, 15, 29])

This theorem uses Fibonacci polynomials (see the appendix).

Note that $U_n(1) = F_n$

The Binet Formula equivalent for Fibonacci polynomials is $U_n = \frac{\left(\frac{x+\sqrt{x^2+4}}{2}\right)^n - \left(\frac{x-\sqrt{x^2+4}}{2}\right)^n}{\sqrt{x^2+4}}$

Let us find the roots of this equation.

First, assume $x = 2i\cos\theta$ where $0 \leq \theta < \pi$

Ift $U_n = \frac{\left(\frac{2i\cos\theta+\sqrt{(2i\cos\theta)^2+4}}{2}\right)^n - \left(\frac{2i\cos\theta-\sqrt{(2i\cos\theta)^2+4}}{2}\right)^n}{\sqrt{(2i\cos\theta)^2+4}}$

$$= \frac{\left(\frac{2i\cos\theta + 2\sin\theta}{2}\right)^n - \left(\frac{2i\cos\theta - 2\sin\theta}{2}\right)^n}{2\sin\theta}$$

$$= \frac{(i\cos\theta + \sin\theta)^n - (i\cos\theta - \sin\theta)^n}{2\sin\theta}$$

$$= \frac{\left(ie^{-i\theta}\right)^n - \left(ie^{i\theta}\right)^n}{2\sin\theta}$$

$$= \frac{i^n[e^{-i\theta n} - e^{i\theta n}]}{2\sin\theta}$$

$$= \frac{i^n(-2i\sin n\theta)}{2\sin\theta}$$

$$= \frac{-i^{n+1}\sin n\theta}{\sin\theta}$$

This is equivalent to 0 when $\theta = \frac{\pi k}{n}$ for $k = 1 \ldots n-1$ and therefore U_n has roots $2i\cos(\frac{\pi k}{n})$ where $k = 1 \ldots n-1$

Since we have the roots of U_n we may write $U_n = a(x - r_1) \ldots (x - r_{n-1})$ where r_k represents a root of U_n

Since U_n is always monic, we know $a = 1$ and therefore $U_n = (x - r_1) \ldots (x - r_{n-1})$

$= \prod_{k=1}^{n-1}(x - r_k) = \prod_{k=1}^{n-1}\left(x - 2i\cos\frac{k\pi}{n}\right) = \prod_{k=1}^{n-1}\left(x + 2i\cos\frac{(n-k)\pi}{n}\right)$

Choose $x = 1$ and we get $F_n = \prod_{k=1}^{n-1}\left(1 + 2i\cos\frac{(n-k)\pi}{n}\right)$

Now assume n is even.

It follows that

$$F_n = \left(\prod_{k=1}^{\frac{n-2}{2}} 1 + 2i\cos\frac{(n-k)\pi}{n}\right)\left(1 + 2i\cos\frac{(n-\frac{n}{2})\pi}{n}\right)\left(\prod_{k=\frac{n+2}{2}}^{n-1} 1 + 2i\cos\frac{(n-k)\pi}{n}\right)$$

(see next page)

$$= \left(\prod_{k=1}^{\frac{n-2}{2}} 1 + 2i\cos\frac{(n-k)\pi}{n}\right)\left(\prod_{k=\frac{n+2}{2}}^{n-1} 1 + 2i\cos\frac{(n-k)\pi}{n}\right)$$

$$= \prod_{k=1}^{\frac{n-2}{2}} \left(1 + 2i\cos\frac{(n-k)\pi}{n}\right)\left(1 + 2i\cos\frac{k\pi}{n}\right)$$

$$= \prod_{k=1}^{\frac{n-2}{2}} \left(1 + 2i\cos\frac{(n-k)\pi}{n} + 2i\cos\frac{k\pi}{n} - 4\cos\frac{(n-k)\pi}{n}\cos\frac{k\pi}{n}\right)$$

$$= \prod_{k=1}^{\frac{n-2}{2}} 1 - 2i\cos\frac{k\pi}{n} + 2i\cos\frac{k\pi}{n} + 4\cos\frac{k\pi}{n}\cos\frac{k\pi}{n}$$

$$= \prod_{k=1}^{\frac{n-2}{2}} 1 + 4\cos^2\frac{k\pi}{n}$$

When n is odd, the process is similar and yields

$$\prod_{k=1}^{\frac{n-1}{2}} 1 + 4\cos^2\frac{k\pi}{n}$$

And therefore, for any positive integer n,

$$F_n = \prod_{k=1}^{\left\lfloor\frac{n-1}{2}\right\rfloor} 1 + 4\cos^2\frac{k\pi}{n}$$

Using the identity $\cos(2x) = 2\cos^2 x - 1$, we may conclude

$$F_n = \prod_{k=1}^{\left\lfloor\frac{n-1}{2}\right\rfloor} 3 + 2\cos\frac{2k\pi}{n}$$

■

In addition, I provide an illustrating example of the proof above. Let us compute F_6 where we begin with the statement $F_n = \prod_{k=1}^{n-1}\left(1 + 2i\cos\frac{(n-k)\pi}{n}\right)$

$$F_6 = \prod_{k=1}^{5} 1 + 2i\cos\frac{(6-k)\pi}{6}$$

$$= (1 + 2i\cos\frac{5\pi}{6})(1 + 2i\cos\frac{4\pi}{6})\,(1 + 2i\cos\frac{3\pi}{6})\,(1 + 2i\cos\frac{2\pi}{6})\,(1 + 2i\cos\frac{\pi}{6})$$

$$= (1 + 2i\cos\frac{5\pi}{6})(1 + 2i\cos\frac{4\pi}{6})\,(1 + 2i\cos\frac{2\pi}{6})\,(1 + 2i\cos\frac{\pi}{6})$$

$$= (1 + 2i\cos\frac{5\pi}{6})(1 + 2i\cos\frac{\pi}{6}) \cdot (1 + 2i\cos\frac{4\pi}{6})\,(1 + 2i\cos\frac{2\pi}{6})$$

$$= \prod_{k=1}^{2} (1 + 2i\cos\frac{(6-k)\pi}{6})(1 + 2i\cos\frac{k\pi}{6})$$

$$= \prod_{k=1}^{2} (1 + 2i\cos\frac{(6-k)\pi}{6} + 2i\cos\frac{k\pi}{6} - 4\cos\frac{(6-k)\pi}{6}\cos\frac{k\pi}{6})$$

$$= \prod_{k=1}^{2} 1 - 2i\cos\frac{k\pi}{6} + 2i\cos\frac{k\pi}{6} + 4\cos\frac{k\pi}{6}\cos\frac{k\pi}{6}$$

$$= \prod_{k=1}^{2} 1 + 4\cos^2\frac{k\pi}{6}$$

$$= \prod_{k=1}^{2} 3 + 2\cos\frac{2k\pi}{6}$$

$$= (3 + 2\cos\frac{2\pi}{6})(3 + 2\cos\frac{4\pi}{6})$$

$$= 8$$

■

Section Five: Fibonacci Convergence Test

5.1 A Fibonacci Convergence Test

Theorem 5.1.1: $\sum_{n=1}^{\infty} g(n)$ converges iff $\sum_{n=1}^{\infty} F_n g(F_n)$ converges.

Proof (from [20])

Without loss of generality, assume $g(n)$ is a non-increasing positive function.

(⇒)
Assume $\sum_{n=1}^{\infty} g(n)$ converges

Let $n > 3$

Then $F_n > 2$

$\therefore F_{n+1} > F_{n-1} + 2$

$\therefore F_{n+1} - 1 > F_{n-1} + 1$

Therefore, the list $(F_{n-1} + 1), \dots, (F_{n+1} - 1)$ is an increasing list of integers

This list has $(F_{n+1} - 1) - (F_{n-1} + 1) + 1 = F_{n+1} - 1 - F_{n-1} = F_n - 1$ terms.

Since this is an increasing list, we know that each of the numbers in the list is less than F_{n+1}

Note that since g is a non-increasing positive function $g(k) \geq g(l)$ where $k < l$

Therefore $g(F_{n-1} + 1), \dots, g(F_{n+1} - 1) \geq g(F_{n+1})$

Since there are $F_n - 1$ terms in the list, we have that

$g(F_{n-1} + 1) + \cdots + g(F_{n+1} - 1) \geq (F_n - 1)g(F_{n+1})$

$\therefore g(F_{n-1} + 1) + \cdots + g(F_{n+1} - 1) + g(F_{n+1}) \geq F_n g(F_{n+1})$

$\therefore g(F_{n-1} + 1) + \cdots + g(F_{n+1}) \geq F_n g(F_{n+1})$

$$\therefore \frac{1}{2}[g(F_{n-1} + 1) + \cdots + g(F_{n+1})] \geq \frac{1}{2}[F_n g(F_{n+1})]$$

Note that $\frac{1}{2}g(1) = \frac{1}{2}F_1 g(F_2)$

Note that $\frac{1}{2}[g(1) + g(2)] \geq \frac{1}{2}F_2 g(F_3)$

By the identity, $\frac{1}{2}[g(2) + g(3)] \geq \frac{1}{2}F_3 g(F_4)$

and $\frac{1}{2}[g(3) + g(4) + g(5)] \geq \frac{1}{2}F_4 g(F_5)$

$$\vdots$$

$$\frac{1}{2}[g(F_{n-1} + 1) + \cdots + g(F_{n+1})] \geq \frac{1}{2}[F_n g(F_{n+1})]$$

The sum of the left of the above statements is $\frac{1}{2}\sum_{n=1}^{\infty} g(n)$

The sum of the right of the above statements is $\frac{1}{2}\sum_{n=2}^{\infty} F_{n-1} g(F_n)$

Note that, by Lemma 6.3.29, $\frac{F_n}{F_{n-1}} \leq 2$ and therefore $\frac{1}{2}F_{n-1} \geq \frac{1}{4}F_n$

$$\therefore \frac{1}{2}F_{n-1} g(F_n) \geq \frac{1}{4}F_n g(F_n)$$

Therefore $\frac{1}{2}\sum_{n=2}^{\infty} F_{n-1} g(F_n) \geq \frac{1}{4}\sum_{n=2}^{\infty} F_n g(F_n)$ and we have $\frac{1}{2}\sum_{n=1}^{\infty} g(n) \geq \frac{1}{4}\sum_{n=2}^{\infty} F_n g(F_n)$

Since by assumption $\sum_{n=1}^{\infty} g(n)$ converges we have that $\sum_{n=1}^{\infty} F_n g(F_n)$ converges.

(⇐, by contrapositive)
Assume $\sum_{n=1}^{\infty} g(n)$ diverges

Let $n > 0$

Then $F_{n+2} \geq 1$

$\therefore F_{n+3} \geq F_{n+1} + 1$

$\therefore F_{n+3} - 1 \geq F_{n+1}$

Therefore, the list $(F_{n+1}), \dots, (F_{n+3} - 1)$ is an increasing list of integers

This list has $(F_{n+3} - 1) - (F_{n+1}) + 1 = F_{n+3} - F_{n+1} = F_{n+2}$ terms.

Since this is an increasing list, we know that each of the numbers in the list is greater than F_{n+1}

Note that since g is a non-increasing positive function $g(k) \geq g(l)$ where $k < l$

Therefore $g(F_{n+1}), \dots, g(F_{n+3} - 1) \leq g(F_{n+1})$

Since there are F_{n+2} terms in the list, we have that

$$g(F_{n+1}) + \cdots + g(F_{n+3} - 1) \leq F_{n+2} g(F_{n+1})$$

Note that $g(1) = F_2 g(F_1)$

By the identity, $g(1) + g(2) \leq F_3 g(F_2)$

By the identity, $g(2) + g(3) + g(4) \leq F_4 g(F_3)$

By the identity, $g(3) + \cdots + g(7) \leq F_5 g(F_4)$

$\vdots$

$g(F_{n+1}) + \cdots + g(F_{n+3} - 1) \leq F_{n+2} g(F_{n+1})$

The sum of the left of these statements is $2 \sum_{n=1}^{\infty} g(n)$

The sum of the right of these statements is $\sum_{n=1}^{\infty} F_{n+1} g(F_n)$

Note that, again by Lemma 6.3.29, $\frac{F_{n+1}}{F_n} \leq 2$ and therefore $2F_n \geq F_{n+1}$

$\therefore F_{n+1} g(F_n) \leq 2F_n g(F_n)$

Therefore $\sum_{n=1}^{\infty} F_{n+1} g(F_n) \leq \sum_{n=1}^{\infty} 2F_n g(F_n)$ and we have $\sum_{n=1}^{\infty} g(n) \leq \sum_{n=1}^{\infty} F_n g(F_n)$

Since by assumption $\sum_{n=1}^{\infty} g(n)$ diverges we have that $\sum_{n=1}^{\infty} F_n g(F_n)$ diverges

■

5.2 Using the Fibonacci Convergence Test

The following example is from [20]. Suppose we wish to determine if the series $\sum_{n=1}^{\infty} g(n)$ where $g(n) = (F_m)^a$ and m is the number such that $F_{m-1} < n \leq F_m$ converges. For example, $g(7) = (F_6)^a$ since $F_5 = 5 < 7 \leq 8 = F_6$.

Solution

Note that by the theorem above, $\sum_{n=1}^{\infty} g(n)$ converges only when $\sum_{n=1}^{\infty} F_n g(F_n)$ does.

Here, $\sum_{n=1}^{\infty} F_n g(F_n) = \sum_{n=1}^{\infty} F_n^{a+1}$ since clearly $g(F_n) = F_n^a$

By [20] we have that $F_n = \left\lceil \frac{(\frac{1+\sqrt{5}}{2})^{n+1}}{\sqrt{5}} \right\rceil$ where $\lceil \ \rceil$ is the greatest integer function.

Therefore $\sum_{n=1}^{\infty} F_n^{a+1} = \sum_{n=1}^{\infty} (\left\lceil \frac{(\frac{1+\sqrt{5}}{2})^{n+1}}{\sqrt{5}} \right\rceil)^{a+1}$ which converges when $\sum_{n=1}^{\infty} ((\frac{1+\sqrt{5}}{2})^{n+1})^{a+1}$ does.

$\sum_{n=1}^{\infty} ((\frac{1+\sqrt{5}}{2})^{n+1})^{a+1} = \sum_{n=1}^{\infty} ((\frac{1+\sqrt{5}}{2})^{a+1})^{n+1}$ and we may apply the geometric series convergence test to see that this converges when $a < -1$.

■

Section Six: Appendix

6.1 Definitions

Fibonacci Sequence: a sequence of numbers defined by the sequence relation $F_n = F_{n-2} + F_{n-1}$ where $F_1 = F_2 = 1$

Fibonacci polynomial: A function of x defined as $U_n = xU_{n-1} + U_{n-2}$ where $U_1 = 1$ and $U_2 = x$

Lucas Sequence: a sequence with the same recurrence relation as the Fibonacci Sequence but with initial conditions $L_1 = 1 \ and \ L_2 = 3$

6.2 Useful Tables and Figures

Table of the First 20 Fibonacci Numbers							
n	F_n	n	F_n	n	F_n	n	F_n
1	1	6	8	11	89	16	987
2	1	7	13	12	144	17	1597
3	2	8	21	13	233	18	2584
4	3	9	34	14	377	19	4181
5	5	10	55	15	610	20	6765

Table of the First 20 Lucas Numbers ($\boldsymbol{L_1 = 1, L_2 = 3}$)							
n	L_n	n	L_n	n	L_n	n	L_n
1	1	6	18	11	199	16	2207
2	3	7	29	12	322	17	3571
3	4	8	47	13	521	18	5778
4	7	9	76	14	843	19	9349
5	11	10	123	15	1364	20	15127

Table of the First 20 Values of the Mobius Function $\boldsymbol{\mu(n)}$							
n	$\mu(n)$	n	$\mu(n)$	n	$\mu(n)$	n	$\mu(n)$
1	1	6	1	11	-1	16	0
2	-1	7	-1	12	0	17	-1
3	-1	8	0	13	-1	18	0
4	0	9	0	14	1	19	-1
5	-1	10	1	15	1	20	0

6.3 Lemmas

Lemma 6.3.1 (Quadratic Reciprocity): If p and q are distinct odd primes, then $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}$

Proof

Omitted, see [7, pgs. 186-87]

■

Lemma 6.3.2: For p an odd prime, $r \in Z$ we have that $2F_{p+r} \equiv \left(\frac{p}{5}\right) L_r + F_r (\text{mod } p)$. Note that here we define L_r as the Lucas sequence (see definitions above).

Proof (from [1])

Clearly, $L_r \equiv F_r (\text{mod } 2)$

$\therefore 0 \equiv -L_r + F_r (\text{mod } 2)$

$\therefore 2F_{2+r} \equiv -L_r + F_r (\text{mod } 2)$

$\therefore 2F_{2+r} \equiv \left(\frac{2}{5}\right) L_r + F_r (\text{mod } 2)$ and the statement holds for $p = 2$

Thus, we may assume p is odd.

Similar to the Binet Formula for Fibonacci, the Lucas numbers can be shown to have the formula $L_n = \left(\frac{1+\sqrt{5}}{2}\right)^n + \left(\frac{1-\sqrt{5}}{2}\right)^n$

By selecting $n = p + r$ in the Binet Formula we have

$$F_{p+r} = \frac{1}{2^{p+r}\sqrt{5}}\left(\left(1+\sqrt{5}\right)^{p+r} - \left(1-\sqrt{5}\right)^{p+r}\right)$$

To ease notation, we allow $\left(1+\sqrt{5}\right)^s = a_s + b_s\sqrt{5}$

Note that this implies $\left(1-\sqrt{5}\right)^s = a_s - b_s\sqrt{5}$

It also implies $a_s = \frac{\left(1+\sqrt{5}\right)^s + \left(1-\sqrt{5}\right)^s}{2} = L_s \cdot 2^{s-1}$ and $b_s = F_s \cdot 2^{s-1}$

Therefore, $F_{p+r} = \frac{1}{2^{p+r}\sqrt{5}}\left(\left(1+\sqrt{5}\right)^p(a_r + b_r\sqrt{5}) - \left(1-\sqrt{5}\right)^p(a_r - b_r\sqrt{5})\right)$

Using the binomial theorem,

$$F_{p+r} = \frac{1}{2^{p+r}\sqrt{5}}\left((a_r + b_r\sqrt{5})(\sum_{k=0}^{p}\binom{\mathrm{p}}{\mathrm{k}}\left(\sqrt{5}\right)^k) - (a_r - b_r\sqrt{5})(\sum_{k=0}^{p}\binom{\mathrm{p}}{\mathrm{k}}\left(-\sqrt{5}\right)^k)\right)$$

$$= \frac{1}{2^{p+r}\sqrt{5}}\left(a_r\sum_{k=0}^{p}\binom{\mathrm{p}}{\mathrm{k}}\left(\sqrt{5}\right)^k + b_r\sqrt{5}\sum_{k=0}^{p}\binom{\mathrm{p}}{\mathrm{k}}\left(\sqrt{5}\right)^k - a_r\sum_{k=0}^{p}\binom{\mathrm{p}}{\mathrm{k}}\left(-\sqrt{5}\right)^k - b_r\sqrt{5}\sum_{k=0}^{p}\binom{\mathrm{p}}{\mathrm{k}}\left(-\sqrt{5}\right)^k\right)$$

$$= \frac{1}{2^{p+r}\sqrt{5}}\left(a_r\sum_{k=0}^{p}(\binom{\mathrm{p}}{\mathrm{k}}\left(\sqrt{5}\right)^k - \binom{p}{k}\left(-\sqrt{5}\right)^k) + b_r\sqrt{5}\sum_{k=0}^{p}(\binom{\mathrm{p}}{\mathrm{k}}\left(\sqrt{5}\right)^k - \binom{p}{k}\left(-\sqrt{5}\right)^k)\right)$$

$$= \frac{1}{2^{p+r}\sqrt{5}}\left(a_r\sum_{k=0}^{p}\binom{\mathrm{p}}{\mathrm{k}}\left(\sqrt{5}\right)^k(1-(-1)^k) + b_r\sqrt{5}\sum_{k=0}^{p}\binom{\mathrm{p}}{\mathrm{k}}\left(\sqrt{5}\right)^k(1+(-1)^k)\right)$$

Now note that $p|\binom{\mathrm{p}}{\mathrm{k}}\ for\ k = 1 \ldots p-1$ and therefore

$$F_{p+r} \equiv \frac{1}{2^{p+r}\sqrt{5}}\left(a_r\left(\sqrt{5}\right)^p(1-(-1)^p) + 2b_r\sqrt{5} + b_r\sqrt{5}\left(\sqrt{5}\right)^p(1+(-1)^p)\right) (\mathrm{mod}\ p)$$

Since p is odd,

$$F_{p+r} \equiv \frac{1}{2^{p+r}\sqrt{5}}\left(a_r\left(\sqrt{5}\right)^p(1-(-1)) + 2b_r\sqrt{5}\right) (\mathrm{mod}\ p)$$

$$\equiv \frac{1}{2^{p+r-1}}\left(a_r\left(\sqrt{5}\right)^{p-1} + b_r\right) (\mathrm{mod}\ p)$$

$$\therefore 2^{p+r-1}F_{p+r} \equiv a_r\left(\sqrt{5}\right)^{p-1} + b_r\ (\mathrm{mod}\ p)$$

$$\therefore 2^{p+r-1}F_{p+r} \equiv a_r(5)^{\frac{p-1}{2}} + b_r\ (\mathrm{mod}\ p)$$

Using the Corollary from [7, pg. 172], this implies

$$2^{p+r-1}F_{p+r} \equiv a_r\left(\frac{\mathrm{p}}{5}\right) + b_r\ (\mathrm{mod}\ p)$$

Using quadratic reciprocity (Lemma 6.3.1), it follows that

$$2^{p+r-1}F_{p+r} \equiv a_r\left(\frac{5}{\mathrm{p}}\right) + b_r\ (\mathrm{mod}\ p)$$

Using the fact that $a_s = \frac{\left(1+\sqrt{5}\right)^s + \left(1-\sqrt{5}\right)^s}{2} = L_s \cdot 2^{s-1}$ and $b_s = F_s \cdot 2^{s-1}$ we get that

$$2^{p+r-1}F_{p+r} \equiv L_r \cdot 2^{r-1}\left(\frac{5}{p}\right) + F_r \cdot 2^{r-1}\ (\mathrm{mod}\ p)$$

$$\therefore 2^pF_{p+r} \equiv L_r\left(\frac{5}{p}\right) + F_r\ (\mathrm{mod}\ p)$$

And applying the corollary from [7, pg. 88], we get $2F_{p+r} \equiv L_r\left(\frac{5}{p}\right) + F_r \pmod{p}$ ■

Lemma 6.3.3 (Mobius Inversion Formula): Let F and f be two number theoretic functions related by the formula

$$F(n) = \prod_{d|n} f(d)$$

$$\text{Then } f(n) = \prod_{d|n} F\left(\frac{n}{d}\right)^{\mu(d)}$$

Proof

The analogous sum proof is given in [7, pgs. 113-15] and the proof can be adapted to fit this situation.

■

Lemma 6.3.4 (Pascal's Identity): $\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}$

Proof (from [21, pg. 152])

$$\binom{n-1}{k-1} + \binom{n-1}{k} = \frac{(n-1)!}{(k-1)!\,(n-k)!} + \frac{(n-1)!}{k!\,(n-1-k)!}$$

$$= \frac{k(n-1)!}{k!\,(n-k)!} + \frac{(n-k)(n-1)!}{k!\,(n-k)!}$$

$$= \frac{(k+n-k)(n-1)!}{k!\,(n-k)!}$$

$$= \frac{n(n-1)!}{k!\,(n-k)!}$$

$$= \frac{n!}{k!\,(n-k)!}$$

$$= \binom{n}{k}$$

■

Lemma 6.3.5: $2^{n-1} = \binom{n}{0} + \binom{n}{2} + \cdots$

Proof (by induction)

When $n = 1$ we have $2^{n-1} = 1$ and $\binom{n}{0} + \binom{n}{2} + \cdots = \binom{1}{0} + \binom{1}{2} + \cdots = 1$ and the statement holds.

Assume the statement is true for some natural number n.

First, assume n is odd.

Note that $\binom{n}{0} + \binom{n}{2} + \binom{n}{4} + \cdots + \binom{n}{n-1} = \binom{n}{n} + \binom{n}{n-2} + \cdots + \binom{n}{1}$ using the fact that $\binom{n}{k} = \binom{n}{n-k}$

Now let us examine $\binom{n+1}{0} + \binom{n+1}{2} + \binom{n+1}{4} + \cdots + \binom{n+1}{n+1}$

This equals $\binom{n}{-1} + \binom{n}{0} + \binom{n}{1} + \binom{n}{2} + \binom{n}{3} + \binom{n}{4} + \cdots + \binom{n+1}{n+1}$ by Lemma 6.3.4

$= 2^{n-1} + \binom{n}{-1} + \binom{n}{1} + \binom{n}{3} + \cdots + \binom{n}{n}$

$= 2^{n-1} + \binom{n}{1} + \binom{n}{3} + \cdots + \binom{n}{n}$

$= 2^{n-1} + \binom{n}{0} + \binom{n}{2} + \cdots + \binom{n}{n-1}$ by the note above

$= 2^{n-1} + 2^{n-1}$

$= 2(2^{n-1})$

$= 2^n$

The proof is similar when n is even.

■

Lemma 6.3.6 (Euclidean Algorithm): This is a process for determining $\gcd(a, b)$. First, divide a by b to obtain the unique q and r such that $a = qb + r \; where \; 0 \leq r < b$. Then divide b by r to obtain q_1 and r_1 such that $b = q_1 r + r_1 \; where \; 0 \leq r_1 < r$. Continue dividing and obtaining the statements $r_k = q_{2+k} r_{1+k} + r_{2+k} \; where \; 0 \leq r_{2+k} < r_{1+k}$ until $r_{2+k} = 0$. It then follows that $r_{1+k} = gcd(a, b)$.

Proof

Omitted, see [7, pgs. 26-27]

■

Lemma 6.3.7: $F_{n+5t} > 10^t F_n$

Proof (by induction, from [14, 16])

First, we will show the lemma is true for $t = 1$

By the definition of Fibonacci numbers we have $F_n = 2F_{n-2} + F_{n-3}$

Thus $F_{n+5} = F_{n+4} + F_{n+3}$

$= 2F_{n+3} + F_{n+2}$

$= 3F_{n+2} + 2F_{n+1}$

$= 5F_{n+1} + 3F_n$

$= 8F_n + 5F_{n-1}$

$= 13F_{n-1} + 8F_{n-2}$

$= 21F_{n-2} + 13F_{n-3}$

$> 20F_{n-2} + 10F_{n-3}$

$> 10(2F_{n-2} + F_{n-3})$

$= 10F_n$

Therefore the lemma holds at $t = 1$.

Assume the lemma holds for some natural number t.

$F_{n+5(t+1)} = F_{n+5t+5}$

$= F_{n+5t+4} + F_{n+5t+3}$

$= 2F_{n+5t+3} + F_{n+5t+2}$

$= 3F_{n+5t+2} + 2F_{n+5t+1}$

$= 5F_{n+5t+1} + 3F_{n+5t}$

$= 8F_{n+5t} + 5F_{n+5t-1}$

$= 13F_{n+5t-1} + 8F_{n+5t-2}$

$= 21F_{n+5t-2} + 13F_{n+5t-3}$

$> 20F_{n+5t-2} + 10F_{n+5t-3}$

$> 10(2F_{n+5t-2} + F_{n+5t-3})$

$= 10F_{n+5t}$

$> 10(10^t F_n)$

$= 10^{t+1}F_n$

■

Lemma 6.3.8: F_n has at least k digits for $5(k-1) < n \leq 5k$

Proof (by induction on k, from [14, 16])

By inspection, we can see that the statement holds true for $k = 1$.

Now we assume the statement holds true for some natural number k.

Let n be such that $5k < n \leq 5k + 5$

Therefore $5k - 5 < n - 5 \leq 5k$ and we know F_{n-5} has at least k digits

By Lemma 6.3.7, we know $10^t F_n < F_{n+5t}$ and therefore $10^t F_{n-5} < F_{n+5(t-1)}$

We choose $t = 1$ and it follows that $10F_{n-5} < F_n$

Since F_{n-5} has at least k digits we conclude that F_n has at least $k+1$ digits

■

Note that by this lemma, for $n \in (5k-5\,,5k]$ it follows that $F_n \geq k$ and since $n \leq 5k$ we know that $F_n \geq n/5$

Lemma 6.3.9: The Fibonacci sequence (mod m) is periodic.

Proof (from [28])

Modulo m a term will be equivalent to some value from 0 to $m-1$, or one of m possible values

Therefore, when adding two terms (mod m) we can have m^2 possible outcomes.

Since this is a finite number of outcomes, we can guarantee that at some point the pairs will repeat and the sequence will start over again.

■

Lemma 6.3.10: $\begin{pmatrix} F_{j-1} & F_j \\ F_j & F_{j+1} \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}^j$

Proof (by induction on j, from [22])

If $j = 1$ then $\begin{pmatrix} F_{j-1} & F_j \\ F_j & F_{j+1} \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$ and the statement holds.

Now assume the statement holds for some natural number j.

Let us examine $\begin{pmatrix} F_j & F_{j+1} \\ F_{j+1} & F_{j+2} \end{pmatrix}$.

$$\begin{pmatrix} F_j & F_{j+1} \\ F_{j+1} & F_{j+2} \end{pmatrix} = \begin{pmatrix} F_j & F_{j-1}+F_j \\ F_{j+1} & F_j+F_{j+1} \end{pmatrix}$$

$$= \begin{pmatrix} F_{j-1} & F_j \\ F_j & F_{j+1} \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$$

$$= \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}^j \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \text{ by the induction hypothesis}$$

$$= \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}^{j+1}$$

■

Lemma 6.3.11: $F_{is+j} \equiv F_j {F_{s+1}}^i (\text{mod } F_s)$

Proof (from [22])

From Lemma 6.3.10 we have $\begin{pmatrix} F_{a+b-1} & F_{a+b} \\ F_{a+b} & F_{a+b+1} \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}^{a+b}$

$$= \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}^{a} \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}^{b}$$

$$= \begin{pmatrix} F_{a-1} & F_a \\ F_a & F_{a+1} \end{pmatrix} \begin{pmatrix} F_{b-1} & F_b \\ F_b & F_{b+1} \end{pmatrix}$$

Therefore $F_{a+b} = F_{a-1}F_b + F_aF_{b+1}$

Let $a = j$ and $b = is$ and we have that $F_{is+j} = F_{j-1}F_{is} + F_jF_{is+1}$

Since $F_s | F_{is}$ by Lemma 6.3.12, it follows that $F_{is+j} \equiv F_jF_{is+1} (\text{mod } F_s)$

From Lemma 6.3.10 we have $\begin{pmatrix} F_{ab-1} & F_{ab} \\ F_{ab} & F_{ab+1} \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}^{ab}$

$$= \left(\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}^{a} \right)^{b}$$

$$= \begin{pmatrix} F_{a-1} & F_a \\ F_a & F_{a+1} \end{pmatrix}^{b}$$

Therefore $\begin{pmatrix} F_{ab-1} & F_{ab} \\ F_{ab} & F_{ab+1} \end{pmatrix} \equiv \begin{pmatrix} F_{a-1} & 0 \\ 0 & F_{a+1} \end{pmatrix}^{b} (\text{mod } F_a)$

$$\equiv \begin{pmatrix} {F_{a-1}}^{b} & 0 \\ 0 & {F_{a+1}}^{b} \end{pmatrix} (\text{mod } F_a)$$

Let $a = s$ and $b = i$

It follows that $F_{is+1} \equiv (F_{s+1})^i (\text{mod } F_s)$

Thus, $F_{is+j} \equiv F_j(F_{s+1})^i (\text{mod } F_s)$

■

Lemma 6.3.12: $F_n | F_l$ iff $n | l$ (for $n, l > 2$)

Proof (from [22, 29])

(⇐)

Let $l = nk$

Note that by the Binet Formula, $F_n = \frac{\left(\frac{1+\sqrt{5}}{2}\right)^n - \left(\frac{1-\sqrt{5}}{2}\right)^n}{\sqrt{5}}$ and $F_{nk} = \frac{\left(\frac{1+\sqrt{5}}{2}\right)^{nk} - \left(\frac{1-\sqrt{5}}{2}\right)^{nk}}{\sqrt{5}}$

Since we know $(a-b) | (a^k - b^k)$, choose $a = \left(\frac{1+\sqrt{5}}{2}\right)^n$ and $b = \left(\frac{1-\sqrt{5}}{2}\right)^n$ and the result follows.

(⇒)

Assume $F_n | F_l$

Let $l = nk + m$ where $m < n$

By Lemma 6.3.11 we have that $F_{nk+m} \equiv F_m F_{n+1}^k (\text{mod } F_n)$

$\therefore F_l \equiv F_m F_{n+1}^k (\text{mod } F_n)$

Since $F_n | F_l$ we have $F_n | F_m F_{n+1}^k$

By the note at the end of Theorem 3.4.2 we know that $(F_n, F_{n+1}) = 1$

Thus $F_n | F_m$

Since $m < n$ we have $m = 0$

Therefore $l = nk$ and we conclude $n | l$

■

Lemma 6.3.13: $2F_{n+m} = F_n L_m + F_m L_n$

Proof (from [23])

Using the Binet formulas for F_n and L_n (see Lemma 6.3.2) we obtain

$$F_n L_m = \frac{1}{\sqrt{5}}\left(\left(\frac{1+\sqrt{5}}{2}\right)^n - \left(\frac{1-\sqrt{5}}{2}\right)^n\right)\left(\left(\frac{1+\sqrt{5}}{2}\right)^m + \left(\frac{1-\sqrt{5}}{2}\right)^m\right)$$

$$= \frac{1}{\sqrt{5}}\left(\left(\frac{1+\sqrt{5}}{2}\right)^{n+m} + \left(\frac{1+\sqrt{5}}{2}\right)^n\left(\frac{1-\sqrt{5}}{2}\right)^m - \left(\frac{1-\sqrt{5}}{2}\right)^n\left(\frac{1+\sqrt{5}}{2}\right)^m - \left(\frac{1-\sqrt{5}}{2}\right)^{n+m}\right)$$

$$F_m L_n = \frac{1}{\sqrt{5}}\left(\left(\frac{1+\sqrt{5}}{2}\right)^m - \left(\frac{1-\sqrt{5}}{2}\right)^m\right)\left(\left(\frac{1+\sqrt{5}}{2}\right)^n + \left(\frac{1-\sqrt{5}}{2}\right)^n\right)$$

$$= \frac{1}{\sqrt{5}}\left(\left(\frac{1+\sqrt{5}}{2}\right)^{n+m} + \left(\frac{1+\sqrt{5}}{2}\right)^m\left(\frac{1-\sqrt{5}}{2}\right)^n - \left(\frac{1-\sqrt{5}}{2}\right)^m\left(\frac{1+\sqrt{5}}{2}\right)^n - \left(\frac{1-\sqrt{5}}{2}\right)^{n+m}\right)$$

Therefore,

$$F_n L_m + F_m L_n = \frac{1}{\sqrt{5}}\left(2\left(\frac{1+\sqrt{5}}{2}\right)^{n+m} - 2\left(\frac{1-\sqrt{5}}{2}\right)^{n+m}\right)$$

This is clearly equivalent to $2F_{n+m}$.

■

Lemma 6.3.14: $\gcd(F_l, F_k) = F_{\gcd(l,k)}$

Proof (from [23])

To ease notation, let $h = \gcd(F_l, F_k)$ and $d = \gcd(l, k)$

Therefore $h | F_l$ and $h | F_k$ and also $d | l$ and $d | k$

By [7, pg 21] we know $\exists r, s \in \mathbb{Z}$ such that $d = rk + sl$

By Lemma 6.3.12, $F_k|F_{nk}$ for natural numbers n, k

$\therefore F_l|F_{sl}$ and $F_k|F_{rk}$

Using the fact that $h|F_l$ and $F_l|F_{sl}$ we know that $h|F_{sl}$

Using the fact that $h|F_k$ and $F_k|F_{rk}$ we know that $h|F_{rk}$

By Lemma 6.3.13 we have $F_{rk}L_{sl} + F_{sl}L_{rk} = 2F_{rk+sl} = 2F_d$

Since $h|F_{rk}L_{sl}$ and $h|F_{sl}L_{rk}$ we know $h|2F_d$

If h is odd then clearly $h|F_d$

If h is even then since $h = \gcd(F_l, F_k)$ it follows that F_l and F_k are even and thus F_{sl} and F_{rk} are even

Note that F_n and L_n always have the same parity and therefore L_{sl} and L_{rk} are even

Therefore, using Lemma 6.3.13, we have $\frac{1}{2}F_{rk}L_{sl} + \frac{1}{2}F_{sl}L_{rk} = F_{rk+sl} = F_d$ which we may write as $F_{rk} \cdot \frac{1}{2}L_{sl} + F_{sl} \cdot \frac{1}{2}L_{rk} = F_d$

Since $h|F_{rk}$ and $h|F_{sl}$ we have that $h|(F_{rk} \cdot \frac{1}{2}L_{sl} + F_{sl} \cdot \frac{1}{2}L_{rk})$ and $h|F_d$

Now since $d|l$ and $d|k$ we know $F_d|F_l$ and $F_d|F_k$ by Lemma 6.3.12

Therefore $F_d|\gcd(F_l, F_k) = h$

■

Lemma 6.3.15: ${F_{n+1}}^2 - F_{n+1}F_n - {F_n}^2 = (-1)^n$

Proof (by induction, from [19])

Let $n = 1$. Then ${F_2}^2 - F_2F_1 - {F_1}^2 = 1 - 1 - 1 = -1$ and the formula holds.

Now suppose the formula holds for some n.

Let us examine ${F_{n+2}}^2 - F_{n+2}F_{n+1} - {F_{n+1}}^2$.

This is $(F_n + F_{n+1})^2 - (F_n + F_{n+1})F_{n+1} - {F_{n+1}}^2$ by the sequence definition

Reducing gives $-\left({F_{n+1}}^2 - F_{n+1}F_n - {F_n}^2\right)$

Using the induction hypothesis, this is $-(-1)^n = (-1)^{n+1}$

■

Lemma 6.3.16: $\forall x, y \in Z^+$, if $y^2 - xy - x^2 = 1$ then $\exists n \in Z^+$ such that $x = F_{2n}$ and $y = F_{2n+1}$

Proof (by induction on x, from [19])

If $x = 1$ then $y = 2$ and $n = 1$ and the statement holds.

Now suppose the statement holds for some natural number $x > 1$

It follows that $y \geq 2$.

Assume the statement holds for all pairs (x', y')

Set $x' = 2x - y$ and $y' = y - x$

Since $y \geq 2$ it follows that $(x+1)^2 = x^2 + 2x + 1 \leq x^2 + xy + 1 = y^2$

Therefore $y > x + 1 > x$

Since $x > 1$ it follows that

$$y^2 = xy + x^2 + 1 < xy + x^2 + x = xy + (x+1)x \leq xy + xy = 2xy$$

Therefore $y < 2x$

Thus $0 < x' < x$ and $0 < y'$

$\therefore y'^2 - x'y' - x'^2 = (y-x)^2 - (y-x)(2x-y) - (2x-y)^2 = y^2 - xy - x^2 = 1$

The induction hypothesis implies that $\exists\ m \in Z^+$ such that $x' = F_{2m}\ and\ y' = F_{2m+1}$.

Then $x = x' + y' = F_{2m} + F_{2m+1} = F_{2(m+1)}$ and $y = y' + x = F_{2m+1} + F_{2m+2} = F_{2(m+1)+1}$

and we have found $n = m + 1$ such that $x = F_{2n}\ and\ y = F_{2n+1}$

■

Lemma 6.3.17: $\forall x, y \in Z^+$, if $y^2 - xy - x^2 = -1$ then $\exists n \in Z^+$ such that $x = F_{2n-1}$ and $y = F_{2n}$

Proof (from [19])

Let x and y be given.

Then

$$\begin{aligned}(x+y)^2 - (x+y)(y) - y^2 &= x^2 + 2xy + y^2 - xy - y^2 - y^2 \\ &= -(y^2 - xy - x^2) \\ &= -(-1) \\ &= 1\end{aligned}$$

Based on Lemma 6.3.16, $\exists$ a positive integer n such that y= F_{2n} and $x + y = F_{2n+1}$

Therefore, $x = F_{2n+1} - F_{2n} = F_{2n-1}$ and $y = F_{2n}$

■

Lemma 6.3.18: y is Fibonacci iff $\exists x \in Z^+$ such that $(y^2 - xy - x^2)^2 = 1$

Proof (from [19])

($\Longrightarrow$)

If $y = F_1 = 1$ then let $x = 1$ and the statement holds.

Assume that $y = F_n$ for some $n \geq 2$

Let $x = F_{n-1}$

By Lemma 6.3.15, it follows that $y^2 - xy - x^2 = (-1)^{n-1}$

Therefore, $(y^2 - xy - x^2)^2 = 1$

($\Longleftarrow$)

Assume $\exists x \in Z^+$ such that $(y^2 - xy - x^2)^2 = 1$ where $y \in Z^+$

It follows that $(y^2 - xy - x^2) = \pm 1$

By Lemmas 6.3.16 and 6.3.17, $\exists n \in Z^+$ such that $y = F_{2n}$ *or* F_{2n+1} and we may conclude y is Fibonacci.

■

Lemma 6.3.19: If $x, y \in Z^+$then $y^2 - xy - x^2 \neq 0$

Proof (by contradiction, from [19])

Assume $y^2 - xy - x^2 = 0$

Then $4y^2 - 4xy - 4x^2 = 0$

$\therefore (2y - x)^2 - 5x^2 = 0$

$\therefore (2y - x)^2 = 5x^2$

$\therefore (2y - x)^2 = (\sqrt{5}x)^2$

Since $2y - x \in \mathbb{Q}$ it follows that $\sqrt{5}x \in \mathbb{Q}$, and by extension, $\sqrt{5} \in \mathbb{Q}$, a contradiction

■

Lemma 6.3.20: $Y_{3,j} = F_{2j}$ and $Y_{2,j} = j$ where Y is defined as in Theorem 3.7.1.

Proof (by strong induction on j)

First, we will show that $Y_{3,j} = F_{2j}$.

Using the definition from Theorem 3.7.1 we have that $Y_{3,0} = 0, Y_{3,1} = 1$ and $Y_{3,j} = 3Y_{3,j-1} - Y_{3,j-2}$

Momentarily ignoring the extraneous subscript we have $Y_0 = 0, Y_1 = 1$ and $Y_j = 3Y_{j-1} - Y_{j-2}$

We now note that $F_0 = Y_0 = 0$ (since $F_0 = F_2 - F_1 = 0$) and $F_2 = Y_1 = 1$

Assume the statement holds for all natural numbers less than some $j \geq 1$

Now examine Y_{j+1}

$Y_{j+1} = 3Y_j - Y_{j-1}$ by definition

$= 3F_{2j} - F_{2j-2}$ by induction hypothesis

$= 2F_{2j} + (F_{2j} - F_{2j-2})$

$= 2F_{2j} + F_{2j-1}$

$= (F_{2j} + F_{2j-1}) + F_{2j}$

$= F_{2j+1} + F_{2j}$

$= F_{2j+2}$

Now we will prove that $Y_{2,j} = j$

Using the definition from Theorem 3.7.1 we have that $Y_{2,0} = 0, Y_{2,1} = 1$ and $Y_{2,j} = 2Y_{2,j-1} - Y_{2,j-2}$

We will again ignore the extraneous subscript.

Clearly the statement holds at $j = 1$ since $Y_1 = 1 = j$

Assume the statement holds for all natural numbers less than some $j \geq 1$

Now we will examine Y_{j+1}

$Y_{j+1} = 2Y_j - Y_{j-1}$ by definition

$= 2j - (j - 1)$ by induction hypothesis

$= j + 1$

■

Lemma 6.3.21: Let Y be defined as in Theorem 3.7.1. For $m \geq 2$ ift $(m-1)^{n-1} \leq Y_{m,n} < m^n$

Proof (by induction on n, from [22])

By [22] we know for $m \geq 2$ it holds that $Y_{m,n+1} > Y_{m,n} \geq 0$

If $n = 1$ then the statement holds.

Now assume that the statement holds for some n.

It follows that $Y_{m,n+1} = mY_{m,n} - Y_{m,n-1}$

$= mY_{m,n} - Y_{m,n-1} + Y_{m,n} - Y_{m,n}$

$= (m-1)Y_{m,n} + Y_{m,n} - Y_{m,n-1}$

$> (m-1)Y_{m,n}$

$\geq (m-1)^n$ by the induction hypothesis

Also, $Y_{m,n+1} = mY_{m,n} - Y_{m,n-1}$

$\leq mY_{m,n}$

$< m^{n+1}$ by the induction hypothesis

Thus $(m-1)^n < Y_{m,n+1} < m^{n+1}$ and the statement holds for $n+1$

■

Lemma 6.3.22: If ${F_s}^2 | F_q$ then $F_s | q$

Proof (from [22])

Let ${F_s}^2 | F_q$

By Lemma 6.3.12 we know that $s|q$

Let $q = st$

By [22, pg. 11] we know $F_{st} \equiv tF_s F_{s+1}^{t-1} (\text{mod } F_s^2)$

Thus, $F_q \equiv tF_s F_{s+1}^{t-1} (\text{mod } F_s^2)$

This, and the fact that ${F_s}^2 | F_q$ implies that $F_s^2 |\ tF_s F_{s+1}^{t-1}$

$\therefore F_s |\ tF_{s+1}^{t-1}$

Since we know adjacent Fibonacci numbers are relatively prime by the note at the end of Theorem 3.4.2, we have $(F_s, F_{s+1}) = 1$ and therefore $F_s |\ t$

$\therefore F_s | st$

$\therefore F_s | q$

■

Lemma 6.3.23: Let Y be defined as in Theorem 3.7.1. If $m \geq 2, j^2 - mjk + k^2 = 1$, and $j \leq k$ then $\exists i$ such that $j = Y_{m,i}$ and $k = Y_{m,i+1}$

Proof

Omitted, see [22, pg. 15]

■

Lemma 6.3.24: Let Y be defined as in Theorem 3.7.1. When $m \geq 2$, if $l | m-2$ then $Y_{m,j} \equiv j (\text{mod } l)$ and if $d | m-3$ then $Y_{m,j} \equiv F_{2j} (\text{mod } d)$

Proof (from [22])

By [22] we note that $Y_{m,j} \equiv Y_{a,j} (\text{mod } m-a)$

Choose $a = 2$

By Lemma 6.3.20 it follows that $Y_{m,j} \equiv j (\text{mod } m-2)$

If $l | m-2$ then $Y_{m,j} \equiv j (\text{mod } l)$

Now choose $a = 3$

By Lemma 6.3.20 it follows that $Y_{m,j} \equiv F_{2j} (\text{mod } m-3)$

If $d|m-3$ then $Y_{m,j} \equiv F_{2j} (\text{mod } d)$

■

Lemma 6.3.25: $F_{2((2k+1)i+j)} \equiv F_{2j} (\text{mod } F_{2k} + F_{2k+2})$

Proof (from [22])

A lemma from [22, pg.12] shows that $\begin{pmatrix} F_{2(2k+1)-1} & F_{2(2k+1)} \\ F_{2(2k+1)} & F_{2(2k+1)+1} \end{pmatrix} \equiv I (\text{mod} F_{2k} + F_{2k+2})$ where I is the identity matrix.

Using reasoning similar to that in Lemma 6.3.11 we determine

$$\begin{pmatrix} F_{2((2k+1)i+j)-1} & F_{2((2k+1)i+j)} \\ F_{2((2k+1)i+j)} & F_{2((2k+1)i+j)+1} \end{pmatrix} = \begin{pmatrix} F_{2(2k+1)-1} & F_{2(2k+1)} \\ F_{2(2k+1)} & F_{2(2k+1)+1} \end{pmatrix}^i \begin{pmatrix} F_{2j-1} & F_{2j} \\ F_{2j} & F_{2j+1} \end{pmatrix}$$

Therefore $\begin{pmatrix} F_{2((2k+1)i+j)-1} & F_{2((2k+1)i+j)} \\ F_{2((2k+1)i+j)} & F_{2((2k+1)i+j)+1} \end{pmatrix} = \begin{pmatrix} F_{2j-1} & F_{2j} \\ F_{2j} & F_{2j+1} \end{pmatrix} (\text{mod } F_{2k} + F_{2k+2})$ and we may conclude $F_{2((2k+1)i+j)} \equiv F_{2j} (\text{mod } F_{2k} + F_{2k+2})$

■

Lemma 6.3.26: If $j \leq 2k+1$ then $F_{2(2k+1-j)} \equiv -F_{2j} (\text{mod } F_{2k} + F_{2k+2})$

Proof

Omitted, see [22, pg. 13]

■

Lemma 6.3.27: If $F_s|t$ then ${F_s}^2|F_{st}$

Proof (from [22])

Using methods similar to those in Lemma 6.3.11, [22] shows that $F_{st} \equiv tF_sF_{s+1}^{t-1} (\text{mod } F_s^2)$

Assume $F_s|t$

It follows that ${F_s}^2|F_st$ and therefore $F_{st} \equiv 0 (\text{mod } F_s^2)$

We conclude ${F_s}^2|F_{st}$

■

Lemma 6.3.28: Let Y be defined as in Theorem 3.7.1. Then ${Y_{m,j}}^2 - mY_{m,j}Y_{m,j+1} + {Y_{m,j+1}}^2 = 1$

Proof (by induction on j, from [22])

If $j = 0$ then ${Y_{m,0}}^2 - mY_{m,0}Y_{m,1} + {Y_{m,1}}^2 = 0 - 0 + 1^2 = 1$ and the statement holds

Now assume the statement holds for some natural number j

${Y_{m,j+1}}^2 - mY_{m,j+1}Y_{m,j+2} + {Y_{m,j+2}}^2$

$= {Y_{m,j+1}}^2 - mY_{m,j+1}(mY_{m,j+1} - Y_{m,j}) + \left(mY_{m,j+1} - Y_{m,j}\right)^2$

$= {Y_{m,j+1}}^2 - \left(mY_{m,j+1}\right)^2 + mY_{m,j+1}Y_{m,j} + \left(mY_{m,j+1} - Y_{m,j}\right)^2$

$= {Y_{m,j+1}}^2 - \left(mY_{m,j+1}\right)^2 + mY_{m,j+1}Y_{m,j} + \left(mY_{m,j+1}\right)^2 - 2mY_{m,j+1}Y_{m,j} + \left(Y_{m,j}\right)^2$

$= {Y_{m,j+1}}^2 - mY_{m,j+1}Y_{m,j} + \left(Y_{m,j}\right)^2$

$= 1$ by the induction hypothesis

■

Lemma 6.3.29: $\frac{F_n}{F_{n-1}} \leq 2$

Proof

Clearly $F_{n-2} \leq F_{n-1}$

Therefore $F_{n-1} + F_{n-2} \leq 2\, F_{n-1}$

By definition $F_n = F_{n-1} + F_{n-2}$ and therefore $F_n \leq 2\, F_{n-1}$

Conclude $\frac{F_n}{F_{n-1}} \leq 2$

■

Lemma 6.3.30: $j \leq F_{2j}$

Proof

By Lemmas 6.3.20 and 6.3.21 we see that $2^{j-1} \leq Y_{3,j} = F_{2j}$

Note that for sufficiently large j we have $j < 2^{j-1}$

We conclude that for sufficiently large j it holds that $j \leq F_{2j}$

■

References

[1] Andrica, Dorin, Vlad Crişan, and Fawzi Al-Thukair. “On Fibonacci and Lucas Sequences modulo a Prime and Primality Testing.” *Arab Journal of Mathematical Sciences* 24, no. 1 (January 2018): 9–15. https://doi.org/10.1016/j.ajmsc.2017.06.002.

[2] Bach, Eric, and Jeffrey Outlaw Shallit. *Algorithmic Number Theory*. Vol. 1. Cambridge, MA: MIT Press, 1997.

[3] Boase, Mansur S. “A Result about the Primes Dividing Fibonacci Numbers.” *Fibonacci Quarterly* 39, no. 5 (November 2001): 386–91. https://www.fq.math.ca/Scanned/39-5/boase.pdf.

[4] Brillhart, John, D. H. Lehmer, and J. L. Selfridge. “New Primality Criteria and Factorizations of $2^m \pm 1$.” *Mathematics of Computation* 29, no. 130 (1975): 620–47. https://doi.org/10.1090/S0025-5718-1975-0384673-1.

[5] Brillhart, John. “Note on Fibonacci Primality Testing.” *Fibonacci Quarterly* 36, no. 3 (1998): 222–28. https://www.fq.math.ca/Scanned/36-3/brillhart.pdf.

[6] Brillhart, John, Peter L. Montgomery, and Robert D. Silverman. "Tables of Fibonacci and Lucas Factorizations." *Mathematics of Computation* 50, no. 181 (January 1988): 251-60. doi:10.2307/2007928.

[7] Burton, David M. *Elementary Number Theory*. 7th ed. McGraw-Hill, n.d.

[8] Davis, Martin, Hilary Putnam, and Julia Robinson. "The Decision Problem for Exponential Diophantine Equations." Annals of Mathematics, Second Series, 74, no. 3 (1961): 425-36. Accessed May 10, 2020. doi:10.2307/1970289.

[9] Davis, Martin. "Hilbert's Tenth Problem Is Unsolvable." The American Mathematical Monthly 80, no. 3 (1973): 233-69. Accessed May 10, 2020. doi:10.2307/2318447.

[10] Dubner, Harvey, and Wilfrid Keller. "New Fibonacci and Lucas Primes." Mathematics of Computation 68, no. 225 (1999): 417-27. www.jstor.org/stable/2585123.

[11] Fibonacci, Leonardo, and L. E. Sigler. *Fibonacci's Liber Abaci: a Translation into Modern English of Leonardo Pisano's Book of Calculation*. Springer, n.d.

[12] Garnier, N., and O. Ramare. “Fibonacci Numbers and Trigonometric Identities.” *Fibonacci Quarterly* 46/47, no. 1 (February 2008/2009): 56–61. https://www.fq.math.ca/Papers1/46_47-1/Ramare_Garnier_11-08.pdf.

[13] Grimaldi, Ralph P. *Fibonacci and Catalan Numbers*. John Wiley & Sons, Inc., 2012.

[14] Grossman, H. "Discussions: On the Number of Divisions in Finding a G.C.D." The American Mathematical Monthly 31, no. 9 (1924): 443. doi:10.2307/2298146.

[15] Hoggart, Verner E., and Calvin T. Long. “Divisibility Properties of Generalized Fibonacci Polynomials.” *Fibonacci Quarterly* 12, no. 2 (April 1974): 113–20. https://www.fq.math.ca/Scanned/12-2/hoggatt1.pdf.

[16] Honsberger, Ross. *Mathematical Gems*. Vol. 2. The Mathematical Association of America, 1976.

[17] Horner, Walter W. “Fibonacci and Pascal.” *Fibonacci Quarterly* 2, no. 3 (October 1964): 228. https://www.fq.math.ca/Scanned/2-3/horner.pdf.

[18] Jarden, Dov. “On the Greatest Primitive Divisors of Fibonacci and Lucas Numbers with Prime-Power Subscripts.” Fibonacci Quarterly 1, no. 3 (October 1963): 15-20. https://www.fq.math.ca/1-3.html

[19] Jones, James P. “Diophantine Representation of the Fibonacci Numbers.” Fibonacci Quarterly 13, no. 1 (February 1975): 84–88. https://www.fq.math.ca/Scanned/13-1/jones.pdf.

[20] Jordan, James H. “A Fibonacci Test for Convergence.” *Fibonacci Quarterly* 2, no. 1 (February 1964): 39–41. https://www.fq.math.ca/Scanned/2-1/jordan.pdf.

[21] Koshy, Thomas. *Fibonacci and Lucas Numbers with Applications*. John Wiley & Sons, Inc., n.d.

[22] Matijasevič, Ju V. “Diophantine Representation of Enumerable Predicates.” *Mathematics of the USSR-Izvestiya* 5, no. 1 (1971): 1–28. https://doi.org/10.1070/im1971v005n01abeh001004.

[23] Moll, Victor H. *Numbers and Functions: From a Classical-Experimental Mathematicians Point of View*. American Mathematical Society, 2012.

[24] Moser, Bernard. “A Novel Fibonacci Pattern in Pascal's Triangle.” *International Journal of Contemporary Mathematical Sciences* 9, no. 4: 175–86. https://arxiv.org/abs/1811.02085.

[25] Ribenboim, Paulo. *My Numbers, My Friends: Popular Lectures on Number Theory*. New York: Springer, 2000.

[26] Shane, Harold D. “A Fibonacci Probability Function.” *Fibonacci Quarterly* 11, no. 5 (December 1973): 517–22. https://www.fq.math.ca/Scanned/11-5/shane.pdf.

[27] Tucker, Alan. *Applied Combinatorics*. 6th ed. Wiley, 2012.

[28] Wall, D. D. "Fibonacci Series Modulo M." The American Mathematical Monthly 67, no. 6 (1960): 525-32. Accessed May 10, 2020. doi:10.2307/2309169.

[29] Webb, W. A. and Parberry, E. A. “Divisibility Properties of Fibonacci Polynomials.” Fibonacci Quarterly 7, no. 5 (December 1969): 457–63. https://www.fq.math.ca/Scanned/7-5/webb.pdf