# Characteristics of Fibonacci-type Sequences

Yarden Blausapp

May 2018

**Abstract**

This paper presents an exploration of the Fibonacci sequence, as well as "multi-nacci sequences" and the Lucas sequence. We compare and contrast various characteristics of these sequences, in particular the existence and repetition of prime factors. We show that for the Fibonacci sequence, and for multi-nacci sequences with the same initial conditions, it follows that every prime divides an infinite number of terms of the sequence. By contrast, we show that this is not the case for the Lucas numbers. We provide conditions for when a prime does divide a Lucas number and give some examples of primes that do not divide any Lucas number.

## 1 Introduction

The Fibonacci sequence is a famous sequence of integers both in mathematics and in popular culture. It was introduced to the Latin-speaking world in 1202, in Fibonacci's *Liber Abaci*.

Fibonacci, or, Leonardo Pisano, was an Italian mathematician born in 1175. He grew up traveling with his merchant father and was exposed to the Hindu-Arabic arithmetic system in North Africa. He published *Liber Abaci* in 1202, which introduced the Latin-speaking world to the decimal system.

In *Liber Abaci*, he also introduced the Fibonacci sequence:

> How many pairs of rabbits can be bred in one year from one pair? A certain person places one pair of rabbits in a certain place surrounded on all sides by a wall. We want to know how many pairs can be bred from that pair in one year, assuming it is their nature that each month they give birth to another pair, and in the second month, each new pair can also breed (see [3]).

This situation can be represented with the rule,

$$F_n = F_{n-1} + F_{n-2},$$

for $n \geq 2$ with $F_0 = 0$ and $F_1 = 1$. The first few terms of the Fibonacci sequence are:

$$0, 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, \ldots$$

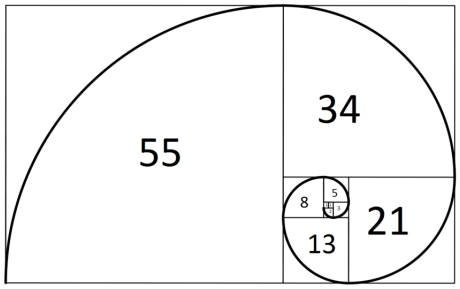


Figure 1: The *golden spiral*

The sequence had been noted by Indian mathematicians as early as the sixth century, but Fibonacci was the first to publish it outside of India.

The Fibonacci numbers are also known for appearing in nature. They appear in the form of a spiral constructed from quarter circles drawn inside an array of squares with the Fibonacci numbers as dimensions. The Fibonacci spiral, sometimes called the *golden spiral*, can be seen in sunflower seeds, hurricanes, and galaxies (see [2]).

## 2 Preliminaries

All of the following results can be found in [4], along with the proofs.

Fermat's Little Theorem is a well-known and useful theorem. It is remarkably short and sweet. We include it here for reference.

**Theorem 2.1** (Fermat's Little Theorem)**.** Suppose that $p$ is a prime and $a$ is an integer. Then

(a) $a^{p-1} \equiv 1 \pmod{p}$ if $a$ and $p$ are relatively prime;

(b) $a^p \equiv a \pmod{p}$ for any $a$.

Another concept we use in our proofs are *quadratic residues*, which take the idea of perfect squares and extend them to spaces $\mathbb{Z}_p$, where $p$ is an odd prime.

**Definition 2.1.** Suppose that $p$ is an odd prime and that $b$ and $p$ are relatively prime. Then $b$ is a quadratic residue modulo $p$ if and only if the equation $x^2 \equiv b \pmod{p}$ has a solution. If the equation has no solution, then we say that $b$ is a quadratic nonresidue modulo $p$.

This definition tells us that if $b$ is a quadratic residue modulo $p$, then it is a perfect square in $\mathbb{Z}_p$. We want to be able to calculate when a number is a quadratic residue modulo $p$. This is easy with small values of $p$ simply by

squaring all the elements in $\mathbb{Z}_p$, but for larger values it is useful to have an arithmetic equation. The notation that we use to say whether $b$ is a quadratic residue modulo $p$ is the *Legendre symbol*, $\left(\frac{b}{p}\right)$, where

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

Euler's Criterion gives us a way to calculate $\left(\frac{b}{p}\right)$.

**Theorem 2.2** (Euler's Criterion)**.** Suppose that $p$ is an odd prime and that $b$ is an integer. If $p$ and $b$ are relatively prime, then

$$\left(\frac{b}{p}\right) = b^{(p-1)/2}.$$

To reduce the work of checking quadratic residues of larger primes, we use the following result.

**Theorem 2.3** (Quadratic Reciprocity Theorem)**.** If $p$ and $q$ are distinct odd primes, then

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) \equiv (-1)^{\frac{1}{2}(p-1)\cdot\frac{1}{2}(q-1)} \pmod{p}.$$

The following corollary helps to further break down large numbers.

**Corollary 2.3.1.** Suppose that $p$ is an odd prime and that $n = \prod_{i=1}^{k} b_i$. If $n$ and $p$ are relatively prime, then

$$\left(\frac{n}{p}\right) = \prod_{i=1}^{k}\left(\frac{b_i}{p}\right).$$

Finally, we have the special case of determining whether 2 is a quadratic residue modulo $p$.

**Theorem 2.4.** If $p$ is an odd prime then,

$$\left(\frac{2}{p}\right) = \begin{cases} 1, & p \equiv \pm 1 \pmod 8; \\ -1 & p \equiv \pm 3 \pmod 8). \end{cases}$$

To see how the Quadratic Reciprocity Theorem helps with large primes, suppose we want to determine whether 607 is a quadratic residue of 2503. Using the above results we obtain,

$$\left(\frac{607}{2503}\right) = -\left(\frac{2503}{607}\right) = -\left(\frac{75}{607}\right) = -\left(\frac{3}{607}\right)\left(\frac{25}{607}\right) = \left(\frac{607}{3}\right) = \left(\frac{1}{3}\right) = 1.$$

With these theorems in mind we continue to an exploration of the Fibonacci numbers.

# 3 Fibonacci numbers

Recall that the Fibonacci sequence is a recursive sequence where each term is defined by

$$F_n = F_{n-1} + F_{n-2}$$

for $n \geq 2$ with the initial condition $F_0 = 0$ and $F_1 = 1$.

It is useful to be able to find a closed-form formula that gives the $n$th term of the Fibonacci sequence so that we do not have to recursively generate every term prior to the term that we want to calculate.

We do this by solving a second order linear difference equation. Taking our recursive Fibonacci equation and transferring all the terms to the left-hand side gives

$$F_n - F_{n-1} - F_{n-2} = 0.$$

We assume that $r^n$ solves the equation, so

$$r^n - r^{n-1} - r^{n-2} = 0$$

and thus

$$r^2 - r - 1 = 0,$$

which is our characteristic equation. By solving the characteristic equation, the two roots are

$$r_1 = \frac{1+\sqrt{5}}{2} := \phi \quad \text{and} \quad r_2 = \frac{1-\sqrt{5}}{2} := 1 - \phi,$$

where $\phi$ is the *golden ratio*. For any $c_1$ substituting $c_1 r_1^n$ for $F_n$ in $F_n - F_{n-1} - F_{n-2}$ yields zero and for any $c_2$ substituting $c_2 r_2^n$ for $F_n$ in $F_n - F_{n-1} - F_{n-2}$ yields zero. This suggests our solution has the form:

$$F_n = c_1 r_1^n + c_2 r_2^n, \tag{1}$$

Using our values for $r_1$ and $r_2$, we now have

$$F_n = c_1 \cdot \phi^n + c_2 \cdot (1-\phi)^n.$$

Incorporating the initial condition of $F_0 = 0$ means that $c_2 = -c_1$ so we have

$$F_n = c_1(\phi^n - (1-\phi)^n).$$

Incorporating the initial condition $F_1 = 1$, we obtain

$$\begin{aligned} 1 &= c_1(\phi - (1-\phi)) \\ &= c_1(2\phi - 1) \\ c_1 &= \frac{1}{2\phi - 1} = \frac{1}{\sqrt{5}}. \end{aligned}$$

So our final closed-form formula for the Fibonacci sequence is:

$$F_n = \frac{\phi^n - (1-\phi)^n}{\sqrt{5}}. \tag{2}$$

Now that we have the closed-form formula for the Fibonacci sequence, we move on to an investigation of its prime factors (see [1]).

## 3.1 Prime factors

An interesting question to consider is when do primes show up as factors of terms in the Fibonacci-type sequences? Do we eventually get every prime? It turns out every prime divides a Fibonacci number, which is a somewhat surprising feature of the Fibonacci numbers.

Looking at the prime factors of some Fibonacci numbers we begin to notice a pattern:

| $n$ | $F_n$ (factored) |
|---|---|
| 8 | $3 \cdot 7$ |
| 10 | $5 \cdot 11$ |
| 14 | $13 \cdot 29$ |
| 18 | $2^3 \cdot 17 \cdot 19$ |
| 24 | $2^5 \cdot 3^2 \cdot 7 \cdot 23$ |
| 28 | $3 \cdot 13 \cdot 29 \cdot 281$ |
| 30 | $2^3 \cdot 5 \cdot 11 \cdot 31 \cdot 61$ |

It appears that for primes of the form $p = 10k \pm 1$, it follows that $p|F_{p-1}$ and for primes of the form $p = 10k \pm 3$, it follows that $p|F_{p+1}$. To show that this is always true, we first look at some specific examples.

First we consider $p|F_{p-1}$ for $p = 31$. We do this by finding a formula for $F_n$ in $\mathbb{Z}_{31}$. We want to find solutions to the characteristic equation $x^2 = x + 1$ in $\mathbb{Z}_{31}$. By multiplying both sides by 4, we obtain

$$\begin{aligned} 4x^2 &= 4x + 4 \\ 4x^2 - 4x + 1 &= 5 \\ (2x-1)^2 &= 5. \end{aligned}$$

We can verify that a solution exists by checking that 5 is a quadratic residue modulo 31. This is obvious since $6^2 \equiv 5 \pmod{31}$.

Performing some algebra in $\mathbb{Z}_{31}$, we get $(2x-1)^2 = 5 \equiv 6^2 \equiv 25^2$ so $2x - 1 \equiv \pm 25$ or $2x \equiv 1 \pm 25$. Our roots are therefore $\alpha = 13$ and $\beta = -12 \equiv 19$. Putting these values back into Equation (1) yields

$$F_n \equiv c_1 \cdot 13^n + c_2 \cdot 19^n \pmod{31}.$$

Using our initial condition $F_0 = 0$ gives us $c_1 = -c_2$ or $F_n = c_1(13^n - 19^n)$. Using the initial condition $F_1 = 1$ gives $c_1(-6) = 1$ or $c_1 = 5$. We now have

$$F_n \equiv 5(13^n - 19^n) \pmod{31}.$$

Using $n = 30$ and Fermat's Little Theorem we see that

$$F_{30} \equiv 5(13^{30} - 19^{30}) \equiv 5(1 - 1) \equiv 0 \pmod{31}.$$

Since $F_{30} \equiv 0 \pmod{31}$, this shows that 31 divides $F_{30}$. The following theorem generalizes this result for all primes of the form $p = 10k \pm 1$.

**Theorem 3.1.** If $p$ is a prime of the form $p = 10k \pm 1$, then $p|F_{p-1}$.

*Proof.* Suppose $p$ is a prime such that $p = 10k \pm 1$. We want to find a solution to the characteristic equation $x^2 = x + 1$ in $\mathbb{Z}_p$. We can write $x^2 = x + 1$ as $(2x - 1)^2 = 5$. To show that this has a solution in $\mathbb{Z}_p$, we need 5 to be a quadratic residue modulo $p$. Note that by the Quadratic Reciprocity Theorem,

$$\text{when } p = 10k + 1, \quad \left(\frac{5}{p}\right) = \left(\frac{p}{5}\right) = \left(\frac{1}{5}\right) = 1$$

$$\text{and when } p = 10k - 1, \quad \left(\frac{5}{p}\right) = \left(\frac{p}{5}\right) = \left(\frac{-1}{5}\right) = \left(\frac{4}{5}\right) = 1.$$

In either case, 5 is a quadratic residue modulo $p$ so a solution to $(2x - 1)^2 = 5$ exists in $\mathbb{Z}_p$. There are two solutions to $y^2 \equiv 5 \pmod{p}$, namely $y$ and $-y \equiv p - y$. Note that one of these must be odd. Let $y$ be the odd solution. Solving the equation $(2x - 1)^2 = y^2$ yields

$$x = \frac{y + 1}{2} := \alpha \quad \text{and} \quad x = \frac{1 - y}{2} := \beta.$$

Note that $y = \alpha - \beta$. We put these values back into our general Fibonacci equation with initial condition $F_0 = 0$ to obtain

$$F_n \equiv c_1(\alpha^n - \beta^n) \pmod{p}.$$

Using the initial condition $F_1 = 1$ gives $1 = c_1(\alpha - \beta)$ or $c_1 = (\alpha - \beta)^{-1} = y^{-1}$. We now have

$$F_n \equiv y^{-1}(\alpha^n - \beta^n) \pmod{p}.$$

Using $n = p - 1$ and Fermat's Little Theorem we see that

$$F_{p-1} \equiv y^{-1}(\alpha^{p-1} - \beta^{p-1}) \equiv y^{-1}(1 - 1) \equiv 0 \pmod{p}.$$

Since $F_{p-1} \equiv 0 \pmod{p}$, it follows that $p$ divides $F_{p-1}$. □

We have now covered one of two cases of primes. We now look at a specific example of a prime of the form $p = 10k \pm 3$ for $p = 13$.

Note that 5 is not a quadratic residue modulo 13, so there is no solution to $x^2 = x+1$ in $\mathbb{Z}_{13}$. Since $\phi$ is a root of $x^2 = x+1$ in $\mathbb{R}$, we must extend the field $\mathbb{Z}_{13}$ to $\mathbb{Z}_{13}(\phi) = \{a + b\phi | a, b \in \mathbb{Z}_{13}\}$.

We must verify that $\mathbb{Z}_{13}(\phi)$ is a field. It is easy to check that $\mathbb{Z}_{13}$ satisfies the usual properties for addition and multiplication, except perhaps the existence of multiplicative inverses. We must show that each nonzero element in $\mathbb{Z}_{13}(\phi)$ has an inverse in $\mathbb{Z}_{13}(\phi)$. Each element in $\mathbb{Z}_{13}(\phi)$ has the form $a + b\phi$ and we need to find an inverse of the form $c + d\phi$ such that $(a + b\phi)(c + d\phi) = 1$. Recall that since $\phi$ solves the characteristic equation, then $\phi^2 = \phi + 1$. Multiplying out the left side of the equation we get

$$\begin{aligned}(a + b\phi)(c + d\phi) &= ac + bd\phi^2 + (ad + bc)\phi \\ &= ac + bd(\phi + 1) + (ad + bc)\phi \\ &= ac + bd + (ad + bc + bd)\phi.\end{aligned}$$

For this to equate to $1 + 0\phi$ we need to solve the system of equations:

$$\begin{aligned}ac + bd &= 1 \\ bc + (a + b)d &= 0\end{aligned}$$

We solve these two equations for $c$ and $d$ using Cramer's Rule:

$$c = \frac{\begin{vmatrix}1 & b \\ 0 & a+b\end{vmatrix}}{\begin{vmatrix}a & a \\ b & a+b\end{vmatrix}} = (a + b)(a^2 + ab - b^2)^{-1};$$

$$d = \frac{\begin{vmatrix}a & 1 \\ b & 0\end{vmatrix}}{\begin{vmatrix}a & a \\ b & a+b\end{vmatrix}} = -b(a^2 + ab - b^2)^{-1}.$$

Therefore for $c + d\phi$ to be the inverse of $a + b\phi$ we need $(a^2 + ab - b^2)^{-1}$ to always exist. We show that it must exist by way of contradiction.

Suppose that $a^2 + ab - b^2$ does not have an inverse. This occurs if and only if $a^2 + ab - b^2 = 0$ which means $(2a + b)^2 = 5b^2$. However, since 5 is not a quadratic residue modulo 13, this is a contradiction. Therefore $(a^2 + ab - b^2)^{-1}$ exists and each nonzero element of $\mathbb{Z}_{13}(\phi)$ has an inverse in $\mathbb{Z}_{13}(\phi)$.

**Lemma 3.2.** For all $n \in Z^+$, it follows that $\phi^n = F_{n-1} + F_n\phi$.

*Proof.* We prove this by induction over $n$.
For our base case note that $\phi = F_0 + F_1\phi = 0 + \phi$. Suppose that $\phi^n = F_{n-1} + F_n\phi$

for some $n$. Then,

$$\begin{aligned}\phi^{n+1} &= F_{n-1}\phi + F_n\phi^2 \\ &= F_{n-1}\phi + F_n(1+\phi) \\ &= F_{n-1}\phi + F_n + F_n\phi \\ &= F_n + (F_{n-1} + F_n)\phi \\ &= F_n + F_{n+1}\phi.\end{aligned}$$

Therefore by the Principle of Mathematical Induction, $\phi^n = F_{n-1} + F_n\phi$ for all $n \in \mathbb{Z}^+$. □

So by Lemma 3.2,

$$\begin{aligned}\phi^{13} &= F_{12} + F_{13}\phi \\ &= 144 + 233\phi \\ &\equiv 1 - \phi \pmod{13}.\end{aligned}$$

Since $\phi^{13} \equiv F_{12} + F_{13}\phi$, it follows that $F_{12} \equiv 1$ and $F_{13} \equiv -1$. Therefore, $F_{14} \equiv F_{13} + F_{12} \equiv 0 \pmod{13}$.

**Theorem 3.3.** If $p$ is a prime of the form $p = 10k \pm 3$, then $p|F_{p+1}$.

*Proof.* Suppose $p$ is a prime of the form $p = 10k \pm 3$. We want to find a solution to $x^2 = x + 1$ in $\mathbb{Z}_p$. We can write $x^2 = x + 1$ as $(2x-1)^2 = 5$. First we will show that there is no solution to $(2x-1)^2 = 5$ in $\mathbb{Z}_p$. Noting that,

$$\text{when } p = 10k - 3, \quad \left(\frac{5}{p}\right) = \left(\frac{p}{5}\right) = \left(\frac{2}{5}\right) = -1$$

$$\text{and when } p = 10k + 3, \quad \left(\frac{5}{p}\right) = \left(\frac{p}{5}\right) = \left(\frac{3}{5}\right) = -1,$$

we find that 5 is not a quadratic residue modulo $p$, and hence, $(2x-1)^2 = 5$ will not have a solution in $\mathbb{Z}_p$, therefore we must extend our field to $\mathbb{Z}_p(\phi) = \{a + b\phi | a, b \in \mathbb{Z}_p\}$.

In our specific example of $p = 13$, we already showed that $\mathbb{Z}_{13}(\phi)$ is a field. The only necessary condition for this argument was that 5 was not a quadratic residue modulo 13. Since 5 is not a quadratic residue modulo $p$, by the same argument it follows that $\mathbb{Z}_p(\phi)$ is a field with a generic $p$ of the form $10k \pm 3$.

We now rewrite (2) in $\mathbb{Z}_p(\phi)$ using inverses instead of division and using only numbers in $\mathbb{Z}_p(\phi)$. Since $\phi = \frac{1+\sqrt{5}}{2}$, then $\sqrt{5} = 2\phi - 1$. We now have the formula:

$$(-1 + 2\phi)F_n \equiv (\phi^n - (1-\phi)^n) \pmod{p}.$$

Now note that

$$(\phi^p)^2 = \phi^{2p} = (\phi^2)^p = (\phi + 1)^p,$$

and

$$(\phi+1)^p = \sum_{k=0}^{p} \binom{p}{k}\phi^k = 1 + \binom{p}{1}\phi + \binom{p}{2}\phi^2 + \ldots + \phi^p.$$

Since $p|\binom{p}{k}$ for $1 \leq k \leq p-1$ and we are working in $\mathbb{Z}_p(\phi)$, it follows that all of the terms besides 1 and $\phi^p$ disappear, so $(\phi+1)^p \equiv \phi^p + 1$. It follows that $(\phi^p)^2 = \phi^p + 1$. Therefore, $\phi^p$ is a solution to $x^2 = x + 1$.

However, we already know that the only solutions to $x^2 = x + 1$ are $\phi$ and $1 - \phi$, so $\phi^p$ must be equivalent to one of them.

Suppose $\phi^p \equiv \phi$. Then $\phi^p - \phi \equiv 0$, so $\phi$ is a solution to $x^p - x = 0$. We know that polynomials of degree $p$ have at most $p$ roots in a field. Since $x^p \equiv x \pmod{p}$ for all $x \in \mathbb{Z}_p$ by Fermat's Little Theorem, so we already have all $p$ roots. Therefore, $\phi$ is not a root and $\phi^p \neq \phi$. It follows that $\phi^p \equiv 1 - \phi$.

Now note that

$$(1-\phi)^p \equiv 1 - \phi^p \equiv 1 - (1-\phi) \equiv \phi.$$

Using our substitutions of $\phi^p \equiv 1 - \phi$ and $(1-\phi)^p \equiv \phi$, we obtain

$$\begin{aligned}(-1+2\phi)F_{p+1} &= (\phi^{p+1} - (1-\phi)^{p+1}) \\ &= (\phi^p \cdot \phi - (1-\phi)^p \cdot (1-\phi)) \\ &= ((1-\phi)\cdot\phi - \phi\cdot(1-\phi)) = 0.\end{aligned}$$

It follows that $p$ divides $F_{p+1}$. □

Since all primes besides 2 and 5 are of the form $10k \pm 1$ or $10k \pm 3$, it follows that all primes divide a Fibonacci number.

When we look at the prime factorizations of the Fibonacci terms we see that while the above theorems tell us when a prime divides a Fibonacci number, they do not necessarily tell us the first time that a prime divides a Fibonacci number. For example, $17 = 20 - 3$, so it is a prime of the form $p = 10k \pm 3$. It is true that $17|F_{18}$ but also that $17|F_9$. Note that 18 is a multiple of 9. The following lemmas bring us to the result that $p|F_n$ if and only if $z(p)|n$, where $z(p)$ is the smallest positive index such that $p|F_{z(p)}$.

From here on we will define a sequence $S_n$ such that,

$$S_n = S_{n-1} + qS_{n-2},$$

where $q$ is some integer and the initial conditions are $S_0 = 0$ and $S_1 = 1$.

**Lemma 3.4.** If $n$ and $r$ are positive integers, it follows that $S_{n+r} = S_{r+1}S_n + qS_rS_{n-1}$.

*Proof.* We will prove this using strong induction over $r$. We first show that the equality is valid for $r = 1$.
Let $n \in Z^+$. Note that $S_{n+1} = S_2S_n + qS_1S_{n-1} = S_n + qS_{n-1}$ which is how we define our Fibonacci-type sequences, so the equation is valid for $r = 1$.
Now suppose that the equality is valid for all integers up to $r$. That is, assume $S_{n+r} = S_{r+1}S_n + qS_rS_{n-1}$. Noting that

$$\begin{aligned} S_{n+r+1} &= S_{n+r} + qS_{n+r-1} \\ &= S_{r+1}S_n + qS_rS_{n-1} + q(S_rS_n + qS_{r-1}S_{n-1}) \\ &= S_n(S_{r+1} + qS_r) + qS_{n-1}(S_r + qS_{r-1}) \\ &= S_{r+2}S_n + qS_{r+1}S_{n-1}, \end{aligned}$$

we find that the equation is valid for $r+1$. Therefore, by the Principle of Strong Induction, $S_{n+r} = S_{r+1}S_n + qS_rS_{n-1}$ is valid for all $r \in \mathbb{Z}^+$. □

**Lemma 3.5.** For each positive integer $n$, we find that $S_n|S_{kn}$ for all $n, k \in \mathbb{Z}^+$.

*Proof.* We prove this using induction over $k$. For our base case note that by Lemma 3.4, we have

$$S_{2n} = S_{n+n} = S_{n+1}S_n + qS_nS_{n-1} = S_n(S_{n+1} + qS_{n-1}),$$

so $S_n|S_{2n}$. Now we assume that $S_n|S_{kn}$ for some $k$ and note that

$$S_{(k+1)n} = S_{n+kn} = S_{kn+1}S_n + qS_{kn}S_{n-1}.$$

Since $S_n|S_{kn}$ and $S_n|S_n$, we see that $S_n|S_{(k+1)n}$. By the Principle of Mathematical Induction, it follows that $S_n|S_{kn}$ for all $n, k \in \mathbb{Z}^+$. □

**Lemma 3.6.** Every pair of consecutive Fibonacci numbers $F_n, F_{n+1}$ are relatively prime.

*Proof.* We prove this using induction. For our base case when $n = 1$ note that $\gcd(F_1, F_2) = \gcd(1, 1) = 1$. Now we assume that $\gcd(F_n, F_{n+1}) = 1$ for some $n \in \mathbb{Z}^+$ and show that $\gcd(F_{n+1}, F_{n+2}) = 1$. Since $\gcd(F_n, F_{n+1}) = 1$, there exist integers $x$ and $y$ such that $F_nx + F_{n+1}y = 1$. Also note that since $F_{n+2} = F_n + F_{n+1}$, then $F_n = F_{n+2} - F_{n+1}$. Making this substitution for $F_n$ we have

$$\begin{aligned} 1 &= (F_{n+2} - F_{n+1})x + F_{n+1}y \\ &= F_{n+2}x - F_{n+1}x + F_{n+1}y \\ &= F_{n+2}x + F_{n+1}(y - x). \end{aligned}$$

Since $y - x$ is an integer, $F_{n+1}$ and $F_{n+2}$ are relatively prime. By the Principle of Mathematical Induction, every pair of consecutive Fibonacci numbers are relatively prime. □

**Theorem 3.7.** Let $p$ be a prime. Then $p|F_n$ if and only if $z(p)|n$, where $z(p)$ is the smallest positive index such that $p|F_{z(p)}$.

*Proof.* The existence of $z(p)$ is guaranteed by the well-ordering property, since we know that the set $\{n : n \in Z^+ \text{ and } p|F_n\}$ is nonempty for each prime $p$.

Suppose that $z(p)|n$. Then $p|F_n$ easily follows from Lemma 3.5.

Now suppose that $p|F_n$.By the Division Algorithm, there exist integers $q$ and $r$ such that $n = z(p)q + r$ and $0 \leq r < z(p)$. Note that by Lemma 3.4,

$$F_n = F_{z(p)q+r} = F_{r+1}F_{z(p)q} + F_rF_{z(p)q-1}.$$

We know that $p|F_n$ and also that $p|F_{z(p)q}$ by Lemma 3.5, so it must be that $p|F_rF_{z(p)q-1}$. By Lemma 3.6 we know that $p$ does not divide $F_{z(p)q-1}$, since the Fibonacci numbers $F_{z(p)q}$ and $F_{z(p)q-1}$ are consecutive. Therefore $p|F_r$. Since $0 \leq r < z(p)$ and $z(p)$ is the smallest positive integer such that $p|F_z(p)$, it must be that $r = 0$. It follows that $n = z(p)q$, so $z(p)|n$. □

We have now shown that not only does every prime divide a Fibonacci number, but that every prime does so an infinite number of times.

## 3.2 Periodicity

We now know that in our Fibonacci sequence modulo $p$, the zeros repeat at a certain interval. However, this is not necessarily the same interval that the entire sequence repeats. For example, take the terms of $F_n \pmod 7$:

$$1, 1, 2, 3, 5, 1, 6, 0, 6, 6, 5, 4, 2, 6, 1, 0, 1, 1, 2, 3, 5 \ldots$$

We see that a zero appears after just 8 terms, but the entire sequence doesn't repeat until 16 terms. This motivates the following two theorems, which give the period of a Fibonacci sequence modulo $p$.

**Theorem 3.8.** If $p$ is a prime of the form $10k \pm 1$, then the Fibonacci sequence modulo $p$ repeats after $p - 1$ terms.

*Proof.* Once again we use the equation $F_n \equiv y^{-1}(\alpha^n - \beta^n) \pmod p$ in $\mathbb{Z}_p$. By Fermat's Little Theorem,

$$\begin{aligned} F_{n+(p-1)} &\equiv y^{-1}(\alpha^{n+(p-1)} - \beta^{n+(p-1)}) \\ &\equiv y^{-1}(\alpha^n\alpha^{p-1} - \beta^n\beta^{p-1}) \\ &\equiv y^{-1}(\alpha^n - \beta^n) \equiv F_n \pmod p. \end{aligned}$$

Since $F_{n+(p-1)} \equiv F_n \pmod p$, the sequence repeats after $p - 1$ terms. □

**Theorem 3.9.** If $p$ is a prime of the form $10k \pm 3$, where $k \in \mathbb{Z}^+$, then the Fibonacci sequence modulo $p$ repeats after $2(p + 1)$ terms.

*Proof.* We use the equation $F_n = (\phi^n - (1-\phi)^n)(-1+2\phi)^{-1} \pmod p$ in $\mathbb{Z}_p(\phi)$, along with the equivalences $\phi^p \equiv 1 - \phi$ and $(1 - \phi)^p \equiv \phi$ to obtain:

$$\begin{aligned} \phi^p &\equiv 1 - \phi \\ \phi^{p+1} &\equiv -\phi^2 \equiv -1 \\ \phi^{2(p+1)} &\equiv 1, \end{aligned}$$

and,

$$\begin{aligned}(1-\phi)^p &\equiv \phi\\ (1-\phi)^{p+1} &\equiv -1\\ (1-\phi)^{2(p+1)} &\equiv 1.\end{aligned}$$

Using these substitutions, note that:

$$\begin{aligned}F_{n+2(p+1)} &\equiv (\phi^{n+2(p+1)} - (1-\phi)^{n+2(p+1)})(-1+2\phi)^{-1}\\ &\equiv (\phi^n\phi^{2(p+1)} - (1-\phi)^n(1-\phi)^{2(p+1)})(-1+2\phi)^{-1}\\ &\equiv (\phi^n - (1-\phi)^n)(-1+2\phi)^{-1} \equiv F_n \pmod{p}.\end{aligned}$$

Since $F_{n+2(p+1)} \equiv F_n \pmod{p}$, the sequence repeats after $2(p+1)$ terms. □

Note that the above theorems give a "period" in which the Fibonacci sequence modulo $p$ will repeat, but it is not necessarily the shortest period.

# 4 Multi-nacci numbers

The Fibonacci sequence was considered in a math problem where a mature pair of rabbits bears one pair of baby rabbits per month. Imagine if instead, a mature pair of rabbits bears two pairs of baby rabbits per month. Then each month, we would count the number of pairs by the number of pairs from the last month in addition to two pairs for each pair from two months earlier that has now "matured." We call this sequence the "Beta-nacci sequence" and define it recursively by

$$B_n = B_{n-1} + 2B_{n-2}$$

where $n \geq 2$ with $B_0 = 0$ and $B_1 = 1$. Note that this is a version of our generic multi-nacci sequence,

$$S_n = S_{n-1} + qS_{n-2}.$$

The first seven terms in some of these multi-nacci sequences is given in Table 1 (see [5]).

As with the Fibonacci sequence, we want to determine if every prime divides a term of a multi-nacci sequence. We take the Gamma-nacci sequence as an example.

The Gamma-nacci sequence is defined by

$$G_n = G_{n-1} + 3G_{n-2}.$$

To prove that a prime $p$ divides the $G_{p-1}$ term, we need a solution to $x^2-x-3 = 0$ in $\mathbb{Z}_p$, or, $(2x-1)^2 = 13$. For this to have a solution, we need 13 to be a quadratic residue in $\mathbb{Z}_p$. By the Division Algorithm we can write $p = 13q + r$

| n | Fibonacci | $\beta$ | $\gamma$ | $\delta$ | $\epsilon$ | $\zeta$ |
|---|---|---|---|---|---|---|
| $n$ | $F_n$ | $B_n$ | $G_n$ | $D_n$ | $E_n$ | $Z_n$ |
| 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| 2 | 1 | 1 | 1 | 1 | 1 | 1 |
| 3 | 2 | 3 | 4 | 5 | 6 | 7 |
| 4 | 3 | 5 | 7 | 9 | 11 | 13 |
| 5 | 5 | 11 | 19 | 29 | 41 | 55 |
| 6 | 8 | 21 | 40 | 65 | 96 | 133 |
| 7 | 13 | 43 | 97 | 181 | 301 | 463 |

Table 1: The first 7 terms of some multi-nacci sequences

where $0 \leq r < 13$. Using Euler's Criterion, we want $\left(\frac{13}{p}\right) = 1$. By the Quadratic Reciprocity Theorem,

$$\begin{aligned}\left(\frac{13}{p}\right) &= (-1)^{\frac{p-1}{2}\cdot\frac{13-1}{2}}\left(\frac{p}{13}\right)\\ &= (-1)^{3(p-1)}\left(\frac{p}{13}\right)\\ &= \left(\frac{p}{13}\right)\\ &= \left(\frac{r}{13}\right).\end{aligned}$$

Therefore we just need $r$ to be a quadratic residue modulo 13. The quadratic residues in $\mathbb{Z}_{13}$ are $r = 1, 3, 4, 9, 10, 12$. So for primes $p$ of the form $13k \pm 1$, $13k \pm 3$, and $13k \pm 4$, $p$ will divide the $G_{p-1}$ term. For other primes $p$, it follows that $r$ will not be a quadratic residue modulo $p$. This is all we need for the proof that $p$ divides the $G_{p+1}$ term. The following theorem generalizes the proof that $p|G_{p+1}$ to all multi-nacci sequences.

**Theorem 4.1.** For sequences of the form $S_n = S_{n-1} + qS_{n-2}$, let $b = 4q+1$. For all $r$ such that $r$ is a quadratic residue modulo $b$, primes of the form $p = bk + r$ divides the $S_{p-1}$ and for all other primes $p > 4q + 1$, it follows that $p$ divides the $S_{p+1}$ term.

A proof for Theorem 4.1 is identical to the proofs of Theorems 3.1 and 3.3 where $b = 5$.

Two special cases of the prime division are for the Beta-nacci sequence defined by

$$B_n = B_{n-1} + 2B_{n-2},$$

and the Zeta-nacci sequence defined by

$$Z_n = Z_{n-1} + 6Z_{n-2}.$$

The reason that these two sequences are unique is that their characteristic equations are $r^2 - r - 2 = 0$ and $r^2 - r - 6 = 0$ respectively, which each have two integer roots. This means that for $p > 3$ and $p > 5$ respectively, these equations always have a solution in $\mathbb{Z}_p$, so for all $p > 3$ and $p > 5$ respectively, it is true that $p|B_{p-1}$ and $p|Z_{p-1}$.

We can also see this by using the closed form formulas for the Beta-nacci and Zeta-nacci sequences. The closed form formula for the Beta-nacci sequence is:

$$B_n = \frac{2^n - (-1)^n}{3}.$$

When $n = p - 1$, Fermat's Little Theorem yields

$$3B_{p-1} \equiv 2^{p-1} - (-1)^{p-1} \equiv 1 - 1 \equiv 0,$$

which shows that $p|B_{p-1}$.

The closed form formula for the Zeta-nacci sequence is:

$$Z_n = \frac{3^n - (-2)^n}{5}.$$

When $n = p - 1$, Fermat's Little Theorem once again yields

$$5Z_{p-1} = 3^{p-1} - (-2)^{p-1} = 3^{p-1} - 2^{p-1} \equiv 1 - 1 \equiv 0 \pmod{p},$$

which shows that $p|Z_{p-1}$.

# 5 Lucas numbers

A sequence related to the Fibonacci sequence is the Lucas sequence. It is another sequence defined recursively where each term is given by

$$L_n = L_{n-1} + L_{n-2}$$

but the initial conditions are $L_0 = 2$ and $L_1 = 1$. The first few terms of the Lucas Sequence are

$$2, 1, 3, 4, 7, 11, 18, 29, 47, 76, \ldots$$

Note that the only differences between the Lucas and Fibonacci sequences are the initial conditions, in particular the initial condition on the 0 term.

Looking at the prime factorizations of the Lucas numbers, it appears that some primes divide $L_{(p-1)/2}$, some divide $L_{(p+1)/2}$, and some do not divide any Lucas numbers. The following theorems tell us when some primes divide a Lucas number.

**Theorem 5.1.** If $p$ is a prime of the form $20k+11$ or $20k+19$, then $p|L_{(p-1)/2}$.

*Proof.* The conditions for a prime to divide the $L_{(p-1)/2}$ term of the Lucas sequence are that 5 is a quadratic residue modulo $p$ and that $-1$ is a quadratic nonresidue modulo $p$. Note that $-1$ is a quadratic nonresidue modulo $p$ when $p = 4k + 3$ because by Euler's Criterion,

$$\left(\frac{-1}{p}\right) \equiv (-1)^{\frac{p-1}{2}} \equiv -1,$$

since $\frac{p-1}{2}$ is odd for $p = 4k + 3$.

To add in the condition that 5 is a quadratic residue modulo $p$, we want $4k + 3 \equiv 1 \pmod 5$ or $4k + 3 \equiv 4 \pmod 5$. So, we have:

$$\begin{aligned} 4k + 3 &\equiv 1 \pmod 5 \\ 4k &\equiv -2 \\ k &\equiv 2, \end{aligned}$$

or,

$$\begin{aligned} 4k + 3 &\equiv 4 \pmod 5 \\ -k &\equiv 1 \\ k &\equiv 4. \end{aligned}$$

So $k = 5j + 2$ or $k = 5m + 4$ where $k, m \in \mathbb{Z}$. We now have

$$p = 4(5j + 2) + 3 = 20j + 11,$$

or,

$$p = 4(5j + 4) + 3 = 20j + 19.$$

To get a formula for $L_n$ in $\mathbb{Z}_p$ we once again solve the characteristic equation $x^2 - x - 1 = 0$ or $(2x-1)^2 = 5$. Solving the equation $(2x-1)^2 = y^2$ and choosing the odd solution $y$, once again yields $x = \frac{1+y}{2}, \frac{1-y}{2}$. The general solution for our Lucas number formula in $\mathbb{Z}_p$ then looks like

$$L_n = c_1 \left(\frac{1+y}{2}\right)^n + c_2 \left(\frac{1-y}{2}\right)^n.$$

To find our constants, we use the initial conditions $L_0 = 2$ and $L_1 = 1$ to obtain the system of equations

$$\begin{aligned} 2 &= c_1 + c_2 \\ 1 &= c_1 \left(\frac{1+y}{2}\right) + c_2 \left(\frac{1-y}{2}\right), \end{aligned}$$

which yield $c_1 = 1$ and $c_2 = 1$. We now have

$$L_n = \left(\frac{1+y}{2}\right)^n + \left(\frac{1-y}{2}\right)^n.$$

Using $n = (p-1)/2$ we have

$$L_{(p-1)/2} = \left(\frac{1+y}{2}\right)^{(p-1)/2} + \left(\frac{1-y}{2}\right)^{(p-1)/2}.$$

Note that by Euler's Criterion, this is equivalent to

$$L_{(p-1)/2} = \left(\frac{\frac{1+y}{2}}{p}\right) + \left(\frac{\frac{1-y}{2}}{p}\right).$$

Since $-1$ is a quadratic nonresidue modulo $p$, we see that

$$\left(\frac{\frac{1+y}{2}}{p}\right)\left(\frac{\frac{1-y}{2}}{p}\right) = \left(\frac{\frac{1-y^2}{4}}{p}\right) = \left(\frac{\frac{1-5}{4}}{p}\right) = \left(\frac{-1}{p}\right) = -1.$$

Therefore, $\left(\frac{\frac{1+y}{2}}{p}\right)$ and $\left(\frac{\frac{1-y}{2}}{p}\right)$ must be of opposite signs and it follows that $L_{(p-1)/2} \equiv 0$, as required. □

**Theorem 5.2.** If $p$ is a prime of the form $20k+3$ or $20k+7$, then $p|L_{(p+1)/2}$.

*Proof.* Suppose $p$ is a prime such that $p = 20k+3$ or $p = 20k+7$. To get a formula for $L_n$ in $\mathbb{Z}_p$, we want a solution to the characteristic $x^2 = x+1$ in $\mathbb{Z}_p$. First we show that there is no solution to $(2x-1)^2 = 5$ in $\mathbb{Z}_p$. Note that,

$$\text{when } p = 20k+3, \quad \left(\frac{5}{p}\right) = \left(\frac{p}{5}\right) = \left(\frac{3}{5}\right) = -1$$

$$\text{and when } p = 20k+7, \quad \left(\frac{5}{p}\right) = \left(\frac{p}{5}\right) = \left(\frac{2}{5}\right) = -1.$$

In either case, 5 is not a quadratic residue modulo $p$. We therefore have to do a field extension like we did with the Fibonacci sequence. Our formula for $L_n$ in $\mathbb{Z}_p(\phi)$ is

$$L_n \equiv \phi^n + (1-\phi)^n \pmod{p}.$$

When we substitute $n = (p+1)/2$, which is an even number, and use the identities $\phi^p \equiv 1-\phi$ and $(1-\phi)^p \equiv \phi$ we obtain:

$$\begin{aligned}
L_{(p+1)/2} &\equiv \phi^{(p+1)/2} + (1-\phi)^{(p+1)/2} \\
L^2_{(p+1)/2} &\equiv (\phi^{(p+1)/2} + (1-\phi)^{(p+1)/2})^2 \\
&\equiv \phi^{p+1} + 2(\phi^{(p+1)/2}(1-\phi)^{(p+1)/2}) + (1-\phi)^{p+1} \\
&\equiv \phi \cdot \phi^p + 2(\phi - \phi^2)^{(p+1)/2} + (1-\phi)(1-\phi)^p \\
&\equiv \phi \cdot (1-\phi) + 2 + (1-\phi) \cdot \phi \\
&\equiv -1 + 2 - 1 \equiv 0 \pmod{p}.
\end{aligned}$$

It follows that $p$ divides $L_{(p+1)/2}$. □

Although we have just proved two cases of prime division in the Lucas numbers, not all primes divide a Lucas number. Since the only thing different about the Lucas sequence is the initial conditions, the sequence has the same "period" modulo $p$ as the Fibonacci sequence. That is, for primes of the form $10k \pm 1$ the "period" is $p-1$ and for primes of the form $10k \pm 3$ the "period" is $2(p+1)$. If $p$ divides a Lucas number we will see a 0 in one "period" of the Lucas sequence modulo $p$.

To show that not all primes divide a Lucas number we only need to show an example of a prime that never divides a Lucas number. We take $p = 5$ and note that the period is 4. In one period of the Lucas sequence modulo 5, the terms are

$$2, 1, 3, 4, \ldots$$

Since there is no 0 in this period, which repeats for the entire sequence, then 5 does not divide a Lucas number. For our next example we use $p = 13$, which is a prime of the form $10k \pm 3$. Therefore its period is $2(p+1) = 28$, so we only need to look at 28 terms of the Lucas sequence modulo 13.

Observe that since $F_n = (\phi^n - (1-\phi)^n)(-1+2\phi)^{-1}$ and $L_n = \phi^n + (1-\phi)^n$, it follows that $F_{2n} = F_n L_n$. Therefore if $13|L_n$, then $13|F_{2n}$. We know that $F_7 = 13$, so $7|2n$, by Theorem 3.7. Since 7 does not divide 2, 7 divides $n$. Therefore we only need to look at $L_n \pmod{13}$ up to 28 where $n$ is a multiple of 7. If we check these terms we see that $L_7 \equiv 3$, $L_{14} \equiv 11$, and $L_{21} \equiv 10$. Since none of these values are 0, it follows that 13 does not divide a Lucas number.

Similarly for 17, we only need to check $L_9$, $L_{18}$, and $L_{27}$ in $\mathbb{Z}_{17}$. Since $L_9 \equiv 8$, $L_{18} \equiv 15$, and $L_{27} \equiv 9$, it follows that 17 does not divide a Lucas number.

The fact that not all primes divide a Lucas number suggests that there is something unique about the Fibonacci sequence and other multi-nacci sequences with the same initial conditions. Particularly, to get the result that all sufficiently large primes divide every term of a sequence $S_n$, it is necessary that $S_0 = 0$.

The following fact is another interesting characteristic of the Lucas numbers.

**Theorem 5.3.** For all primes $p$, $L_p \equiv 1 \pmod{p}$.

*Proof.* For the case when $\left(\frac{5}{p}\right) \equiv 1$, we see that in $\mathbb{Z}_p$, the solutions to the equation $(2x-1)^2 = 5$ are $x = \frac{1+y}{2}, \frac{1-y}{2}$. Let $a = \frac{1+y}{2}$ and $b = \frac{1+y}{2}$. Then by Fermat's Little Theorem,

$$L_p \equiv a^p + b^p \equiv a + b \equiv 1 \pmod{p}.$$

For the case when $\left(\frac{5}{p}\right) \equiv -1$, we see that in $\mathbb{Z}_p(\phi)$,

$$L_p \equiv \phi^p + (1-\phi)^p \equiv 1 - \phi + \phi = 1 \pmod{p}.$$

For the case when $p = 5$ we see that $L_5 = 11 \equiv 1 \pmod 5$. Therefore, for all primes $p$, it follows that $L_p \equiv 1 \pmod p$. □

The following result combines our knowledge of the Fibonacci and Lucas numbers.

**Theorem 5.4.** If $z(p)$ is even, where $z(p)$ is the smallest integer such that $p|F_{z(p)}$, then $p|L_{z(p)/2}$.

*Proof.* Suppose $z(p)$ is even. Then $z(p) = 2n$ for some $n \in \mathbb{Z}^+$. Note that $F_{2n} = F_n L_n$. Since $z(p)$ is the smallest integer such that $p|F_{z(p)}$, $p$ does not divide $F_n$. Therefore $p|L_n = L_{z(p)/2}$. □

# 6 Conclusion

In this paper we explored characteristics of the Fibonacci numbers and multinacci numbers, contrasted with the Lucas numbers. In particular we focused on prime factors and repetition in these sequences.

There are many opportunities for future study on this topic. For example, we could look at recursive sequences that are non-homogeneous. We also could look at recursive sequences that depend on 3 previous terms rather than two. Another question we left unanswered is whether or not there exists a prime $p$ such that $z(p) = z(p^2)$.

We explored the prime factors of Fibonacci-type sequences, and when a sequence repeats modulo $p$, but we could also investigate when $m$ divides $S_n$ for a generic $m$ that is not necessarily prime. It turns out that when $m = pq$, where $p$ and $q$ are prime, then the "period" of the sequence modulo $m$ is the least common multiple of $p$ and $q$. This can be used to show when a Fibonacci-type sequence repeats in the ones digit, since this is equivalent to showing when the sequence repeats modulo 10.

Our exploration of Fibonacci-type sequences has shown that the initial condition $S_0 = 0$ leads to many interesting results. There is much to be explored in these numbers and they lead to many questions about other sequences.

# References


[1] Mathematical methods for economic theory. `https://mjo.osborne.economics.utoronto.ca/index.php/tutorial/index/1/sod/t`.

[2] Elaine J. Hom. What is the fibonacci sequence? `https://www.livescience.com/37470-fibonacci-sequence.html`, 2018.

[3] V. Katz. *A history of mathematics, an introduction.* Addison-Wesley, second edition, 1998.

[4] Patrick Keef and David Guichard. *An Introduction to Higher Mathematics.* Whitman College.

[5] Shari Lynn Levine. Suppose more rabbits are born. *The Fibonacci Quarterly*, 26:306–311, 1988.