The Fibonacci Sequence Under Various Moduli

Marc Renault

May, 1996

A thesis submitted to
Wake Forest University
in partial fulfillment of the degree of
Master of Arts in Mathematics

Contents

Chapter 1

Leonardo of Pisa and the Fibonacci Sequence

Fibonacci, the pen name of Leonardo of Pisa which means son of Bonacci, was born in Pisa, Italy around 1170. Around 1192 his father, Guillielmo Bonacci, became director of the Pisan trading colony in Bugia, Algeria, and some time thereafter they traveled together to Bugia. From there Fibonacci traveled throughout Egypt, Syria, Greece, Sicily, and Provence where he became familiar with Hindu-Arabic numerals which at that time had not been introduced into Europe.

He returned to Pisa around 1200 and produced *Liber Abaci* in 1202. In it he presents some of the arithmetic and algebra he encountered in his travels, and he introduces the place-valued decimal system and Arabic numerals. Fibonacci continued to write mathematical works at least through 1228, and he gained a reputation as a great mathematician. Not much is known of his life after 1228, but it is commonly held that he died some time after 1240, presumably in Italy.

Despite his many contributions to mathematics, Fibonacci is today remembered for the sequence which comes from a problem he poses in *Liber Abaci.* The following is a paraphrase:

> A man puts one pair of rabbits in a certain place entirely surrounded by a wall. The nature of these rabbits is such that every month each pair bears a new pair which from the end of their second month on becomes productive. How many pairs of rabbits will there be at the end of one year?

If we assume that the first pair is not productive until the end of the second month, then clearly for the first two months there will be only one pair. At the start of the third month the first pair will beget a pair giving us a total of two pair. During the fourth month the original pair begets again but the second pair does not, giving us three pair, and so on.

Assuming none of the rabbits die we can develop a recurrence relation. Let there be F_n pairs of rabbits in month n, and F_{n+1} pairs of rabbits in month $n+1$. During month $n+2$, all the pairs of rabbits from month $n+1$ will still be there, and of those rabbits the ones which existed during the n^{th} month will give birth. Hence $F_{n+2} = F_{n+1} + F_n$. The sequence which ensues when $F_1 = F_2 = 1$ is called the Fibonacci sequence and the numbers in the sequence are the Fibonacci numbers.

n:	1	2	3	4	5	6	7	8	9	10	11	12	...
F_n:	1	1	2	3	5	8	13	21	34	55	89	144	...

Thus the answer to Fibonacci's problem is 144.

Interestingly, it was not until 1634 that this recurrence relation was written down by Albert Girard.

Despite its simple appearance the Fibonacci sequence contains a wealth of subtle and fascinating properties. For example,

Theorem 1.1 *Successive terms of the Fibonacci sequence are relatively prime.*

> **Proof:** Suppose that F_n and F_{n+1} are both divisible by a positive integer d. Then their difference $F_{n+1} - F_n = F_{n-1}$ will also be divisible by d. Continuing, we see that $d|F_{n-2}$, $d|F_{n-3}$, and so on. Eventually, we must have $d|F_1$. Since $F_1 = 1$ clearly $d = 1$. Since the only positive integer which divides successive terms of the Fibonacci sequence is 1, our theorem is proved.

One of the purposes of this chapter and the next is to develop many of the identities needed in chapters three and four. All of these can be found in either [4] or [20]. Given the recursive nature of the sequence, proof by induction is often a useful tool in proving identities and theorems involving the Fibonacci numbers. One of the most useful is the following.

Identity 1.2 $F_{m+n} = F_{m-1}F_n + F_mF_{n+1}$.

Proof: Let m be fixed and we will proceed by inducting on n. When $n = 1$, then $F_{m+1} = F_{m-1}F_1 + F_mF_2 = F_{m-1} + F_m$ which is true.

Now let us assume the identity is true for $n = 1, 2, 3, \ldots, k$, and we will show that it holds for $n = k + 1$. By assumption

$$F_{m+k} = F_{m-1}F_k + F_mF_{k+1}$$

and

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

Adding the two we get $F_{m+k} + F_{m+(k-1)} = F_{m-1}(F_k + F_{k-1}) + F_m(F_{k+1} + F_k)$ which implies $F_{m+(k+1)} = F_{m-1}F_{k+1} + F_mF_{k+2}$ which is precisely our identity when $n = k + 1$.

As an example of this identity, we see that $F_{12} = F_{8+4} = F_7F_4 + F_8F_5 = 13(3) + 21(5) = 144$.

It is often useful to extend the Fibonacci sequence backward with negative subscripts. The Fibonacci recurrence can be written as $F_n = F_{n+2} - F_{n+1}$ which allows us to do this.

n:	...	-7	-6	-5	-4	-3	-2	-1	0	1	2	3	4	...
F_n:	...	13	-8	5	-3	2	-1	1	0	1	1	2	3	...

Sequences such as the Fibonacci sequence which can be extended infinitely in both directions are called “bilateral”.

With some inspection another useful identity presents itself:

Identity 1.3 $F_{-n} = (-1)^{n+1}F_n$.

Now we can combine the above two identities to obtain

Identity 1.4 $F_{m-n} = (-1)^n(F_mF_{n+1} - F_{m+1}F_n)$

Another important fact about the Fibonacci sequence is easily tackled with induction.

Theorem 1.5 $F_m|F_{mn}$ *for all integers* m, n.

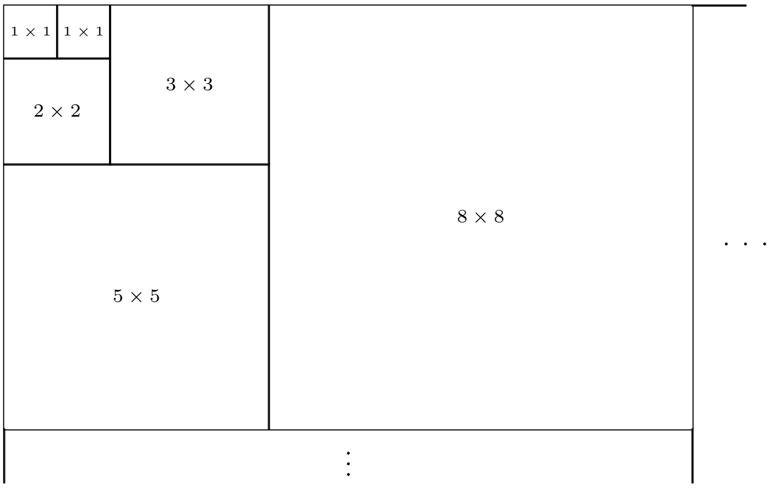
Proof: Let m be fixed and we will induct on n. If either m or n equals zero, then the theorem is true by easy inspection. For $n = 1$ it is clear that $F_m|F_m$.

Now let us assume that the theorem holds for $n = 1, 2, \ldots, k$ and we will show that it also holds for $n = k + 1$. Using identity 1.2 we see $F_{m(k+1)} = F_{mk-1}F_m + F_{mk}F_{m+1}$. By assumption $F_m|F_{mk}$, and so F_m divides the entire right side of the equation. Hence F_m divides $F_{m(k+1)}$ and the theorem is proved for $n \geq 1$. Since F_{mn} differs from F_{-mn} by at most a factor of -1, then $F_m|F_{mn}$ for $n \leq -1$ as well.

A surprising result, with a surprisingly simple geometric proof is demonstrated in the following identity.

Identity 1.6 $F_1^2 + F_2^2 + F_3^2 + \cdots + F_n^2 = F_nF_{n+1}$.

Proof: We can think of the squares of Fibonacci numbers as areas, and then put them together in the manner below.

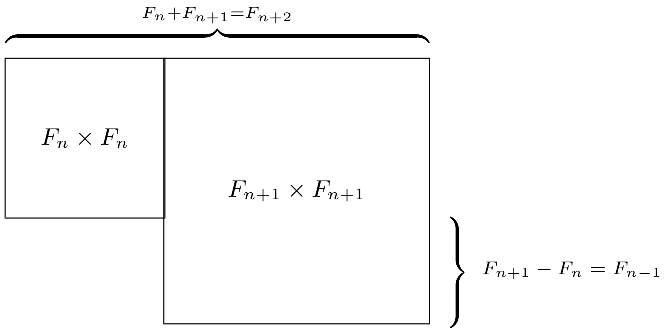


We can find the area of the above rectangle by summing the squares, $F_1^2 + F_2^2 + F_3^2 + F_4^2 + F_5^2 + F_6^2$, or by multiplying height times width, $F_6 \cdot (F_5 + F_6) = F_6 \cdot F_7$. The general case for the sum of the squares of n Fibonacci numbers follows easily.

The following identity will be useful to us and it, too, can be proved geometrically.

Identity 1.7 $F_n^2 + F_{n+1}^2 = F_{2n+1}$.

Proof:



The area above can be represented as $F_{n-1}F_{n+1} + F_nF_{n+2}$. From identity 1.2 this simplifies to $F_{n+(n+1)} = F_{2n+1}$.

Here is another identity involving the square of Fibonacci numbers.

Identity 1.8 $F_{n+1}F_{n-1} - F_n^2 = (-1)^n$.

Proof:

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

We can now repeat the above process on the last line to attain

$$\begin{aligned}
-(F_nF_{n-2} - F_{n-1}^2) &= (-1)^2(F_{n-1}F_{n-3} - F_{n-2}^2) \\
&= (-1)^3(F_{n-2}F_{n-4} - F_{n-3}^2) \\
&\vdots \\
&= (-1)^n(F_1F_{-1} - F_0^2) \\
&= (-1)^n
\end{aligned}$$

It was the 19th century number theorist Edouard Lucas who first attached Fibonacci's name to the sequence we have been studying. He also investigated generalizations of the sequence.

A generalized Fibonacci sequence, G, is one in which the usual recurrence relation $G_{n+2} = G_{n+1} + G_n$ holds, but G_0 and G_1 may take on arbitrary values. The Lucas sequence, L, is an example of a generalized Fibonacci sequence where $L_0 = 2$ and $L_1 = 1$. It continues 2, 1, 3, 4, 7, 11, ... There are many interesting relationships between the Fibonacci and Lucas sequences, and we give two of the most basic here.

Identity 1.9 $L_n = F_{n-1} + F_{n+1}$.

> **Proof:** We will prove the identity by induction. It is easy to see that $L_1 = 1 = 0 + 1 = F_0 + F_2$ and $L_2 = 3 = 1 + 2 = F_1 + F_3$. Now suppose that the identity holds for L_r and L_{r+1}:
>
> $$\begin{aligned} L_r &= F_{r-1} + F_{r+1} \\ L_{r+1} &= F_r + F_{r+2} \end{aligned}$$
>
> Adding the two equations gives us $L_{r+2} = F_{r+1} + F_{r+3}$ and subtracting the top equation from the bottom yields $L_{r-1} = F_{r-2} + F_r$. Thus the identity holds for all positive and negative r.

Identity 1.10 $F_{2n} = F_n L_n$.

> **Proof:** $F_{2n} = F_{n+n} = F_{n-1}F_n + F_nF_{n+1} = F_n(F_{n-1} + F_{n+1}) = F_nL_n$.

We make a distinction between *a* Fibonacci sequence, meaning any generalized Fibonacci sequence, and *the* Fibonacci sequence, meaning the sequence with $G_0 = 0$ and $G_1 = 1$.

Some authors generalize the sequence even more by using the relation $S_{n+2} = bS_{n+1} + aS_n$. A further generalization examines sequences with the relation $S_n = c_1S_{n-1} + c_2S_{n-2} + \cdots + c_kS_{n-k}$ for constants k and c_i. Throughout this paper we will concentrate primarily on the Fibonacci sequence, though we will have occasion to make use of the generalized form $G_{n+2} = G_{n+1} + G_n$. We end this chapter with two identities from [20] involving the generalized Fibonacci sequence.

Identity 1.11 $G_{m+n} = F_{n-1}G_m + F_nG_{m+1}$.

Proof: For the cases $n = 0$ and $n = 1$ we have

$$\begin{aligned} G_m &= F_{-1}G_m + F_0G_{m+1} \\ G_{m+1} &= F_0G_m + F_1G_{m+1} \end{aligned}$$

which is true since $F_{-1} = 1$, $F_0 = 0$, and $F_1 = 1$. By adding the two equations it is easy to see that our identity continues to hold for $n = 2, 3, \ldots$ and so on. Subtracting the first equation from the second indicates that the identity also holds for negative n.

Identity 1.12 $G_{m-n} = (-1)^n(F_nG_{m+1} - F_{n+1}G_m)$

Proof: This identity follows by substituting $-n$ for n in the above identity and then using identity 1.3.

Chapter 2

The Binet Formula

While the recurrence relation and initial values determine every term in the Fibonacci sequence, it would be nice to know a formula for F_n so we wouldn't have to compute all the preceding Fibonacci numbers. Such a formula was discovered by Jacques-Philippe-Marie Binet in 1843. Vajda [20] observes that this was actually a "rediscovery" since Abraham DeMoivre knew about this formula as early as 1718. However, history has favored Binet with the credit. Much of the material in this chapter can be found in [20].

Let us find the values for x which will give us the generalized Fibonacci sequence $x^{n+2} = x^{n+1} + x^n$. Since we are not concerned with the case where $x = 0$ which gives us the trivial sequence, we may divide through by x^n to attain $x^2 = x + 1$, that is, $x^2 - x - 1 = 0$. The two roots of this equation are

$$\tau = \frac{1+\sqrt{5}}{2} \qquad \sigma = \frac{1-\sqrt{5}}{2}. \tag{2.1}$$

Note the following properties of τ and σ:

$$\tau + \sigma = 1 \qquad \tau - \sigma = \sqrt{5} \qquad \tau\sigma = -1 \tag{2.2}$$

Now $1, \tau, \tau^2, \tau^3, \ldots$ and $1, \sigma, \sigma^2, \sigma^3, \ldots$ are in fact generalized Fibonacci sequences since $\tau^{n+2} = \tau^{n+1} + \tau^n$ and $\sigma^{n+2} = \sigma^{n+1} + \sigma^n$. Indeed, any linear combination of τ^n and σ^n forms the n^{th} term of some Fibonacci sequence.

$$G_n = \alpha\tau^n + \beta\sigma^n \tag{2.3}$$

As we see, $(\alpha\tau^n + \beta\sigma^n) + (\alpha\tau^{n+1} + \beta\sigma^{n+1}) = \alpha(\tau^n + \tau^{n+1}) + \beta(\sigma^n + \sigma^{n+1}) = \alpha\tau^{n+2} + \beta\sigma^{n+2}$.

Any Fibonacci sequence can be expressed this way for particular values of α and β. We show this by expressing α and β in terms of G_0, G_1, τ, and σ.

First, notice that $G_0 = \alpha + \beta$ and $G_1 = \alpha\tau + \beta\sigma$. Since $\beta = G_0 - \alpha$ we can write

$$\begin{aligned} G_1 &= \alpha\tau + (G_0 - \alpha)\sigma \\ &= \alpha(\tau - \sigma) + G_0\sigma \\ &= \alpha\sqrt{5} + G_0\sigma \end{aligned}$$

which implies

$$\alpha = \frac{G_1 - G_0\sigma}{\sqrt{5}}. \tag{2.4}$$

Similarly $\alpha = G_0 - \beta$ and so

$$\begin{aligned} G_1 &= (G_0 - \beta)\tau + \beta\sigma \\ &= G_0\tau + \beta(\sigma - \tau) \\ &= G_0\tau - \beta\sqrt{5} \end{aligned}$$

which implies

$$\beta = \frac{G_0\tau - G_1}{\sqrt{5}}. \tag{2.5}$$

Now, once we know G_0 and G_1 we can use equations 2.4 and 2.5 to determine α and β, and then the formula for G_n follows from equation 2.3.

For example, in the Fibonacci sequence $F_0 = 0$ and $F_1 = 1$, and so $\alpha = 1/\sqrt{5}$ and $\beta = -1/\sqrt{5}$. Thus

$$F_n = \frac{\tau^n - \sigma^n}{\sqrt{5}}. \tag{2.6}$$

In the Lucas sequence $L_0 = 2$ and $L_1 = 1$.

$$\alpha = \frac{1 - 2\sigma}{\sqrt{5}} = \frac{(\tau + \sigma) - 2\sigma}{\sqrt{5}} = \frac{\tau - \sigma}{\sqrt{5}} = 1.$$

$$\beta = \frac{2\tau - 1}{\sqrt{5}} = \frac{2\tau - (\tau + \sigma)}{\sqrt{5}} = \frac{\tau - \sigma}{\sqrt{5}} = 1.$$

Thus

$$L_n = \tau^n + \sigma^n. \tag{2.7}$$

DeMoivre was able to derive the formula for F_n in a different way, using generating functions. We demonstrate this technique next.

Let $g(x) = \sum_{i=0}^{\infty} F_i x^i$. It follows that $g(x) - F_0 x^0 - F_1 x^1 = g(x) - x$. Hence

$$\begin{aligned}
g(x) - x &= \sum_{i=2}^{\infty} F_i x^i = \sum_{i=2}^{\infty} (F_{i-1} x^i + F_{i-2} x^i) \\
&= x \sum_{i=1}^{\infty} F_i x^i + x^2 \sum_{i=0}^{\infty} F_i x^i \\
&= x g(x) + x^2 g(x).
\end{aligned}$$

Now we have $g(x) - xg(x) - x^2 g(x) = x$. That is,

$$\begin{aligned}
g(x) &= \frac{x}{1 - x - x^2} = \frac{x}{1 - (\tau + \sigma)x + \tau\sigma x^2} \\
&= \frac{x}{(1 - \tau x)(1 - \sigma x)} = \frac{(\tau - \sigma)x}{\sqrt{5}(1 - \tau x)(1 - \sigma x)} \\
&= \frac{1 - \sigma x}{\sqrt{5}(1 - \tau x)(1 - \sigma x)} - \frac{1 - \tau x}{\sqrt{5}(1 - \tau x)(1 - \sigma x)} \\
&= \frac{1}{\sqrt{5}(1 - \tau x)} - \frac{1}{\sqrt{5}(1 - \sigma x)}.
\end{aligned}$$

Expressing $\frac{1}{1-\tau x}$ and $\frac{1}{1-\sigma x}$ as the sums of geometric series we get

$$\begin{aligned}
g(x) &= \frac{1}{\sqrt{5}}(1 + \tau x + \tau^2 x^2 + \cdots) - \frac{1}{\sqrt{5}}(1 + \sigma x + \sigma^2 x^2 + \cdots) \\
&= [(\tau - \sigma)x + (\tau^2 - \sigma^2)x^2 + \cdots]/\sqrt{5}
\end{aligned}$$

The coefficient of x^n, in other words F_n, is $(\tau^n - \sigma^n)/\sqrt{5}$, just as we suspected.

We can use the generating function to attain some unusual results. Taking our equation

$$g(x) = \frac{x}{1 - x - x^2} = \sum_{i=0}^{\infty} F_i x^i$$

and dividing through by x we get

$$\frac{1}{1 - x - x^2} = \sum_{i=0}^{\infty} F_i x^{i-1}. \tag{2.8}$$

When $x = 1/2$,

$$4 = \sum_{i=0}^{\infty} \frac{F_i}{2^{i-1}}$$

which implies

$$2 = \sum_{i=0}^{\infty} \frac{F_i}{2^i}. \tag{2.9}$$

Another remarkable summation identity is obtained by differentiating both sides of equation (2.8)

$$\frac{1+2x}{(1-x-x^2)^2} = \sum_{i=0}^{\infty} (i-1)F_i x^{i-2}.$$

When $x = 1/2$,

$$\begin{aligned}
32 &= \sum_{i=0}^{\infty} \frac{(i-1)F_i}{2^{i-2}} \\
8 &= \sum_{i=0}^{\infty} \frac{(i-1)F_i}{2^i} = \sum_{i=0}^{\infty} \frac{iF_i}{2^i} - \sum_{i=0}^{\infty} \frac{F_i}{2^i} \\
8 &= \sum_{i=0}^{\infty} \frac{iF_i}{2^i} - 2 \\
10 &= \sum_{i=0}^{\infty} \frac{iF_i}{2^i}. \qquad (2.10)
\end{aligned}$$

The next identity is clearly more complicated than those we've looked at before, yet its proof yields readily to the Binet formula. The interesting thing about it is that it gives us insight into the recurrence relation governing subsequences of the Fibonacci sequence. This identity shows how every n^{th} term of the Fibonacci sequence is related.

Identity 2.1 $F_{m+n} = L_nF_m + (-1)^{n+1}F_{m-n}$.

Proof:

$$L_nF_m + (-1)^{n+1}F_{m-n} = (\tau^n + \sigma^n)(\frac{\tau^m - \sigma^m}{\sqrt{5}}) + (-1)^{n+1}(\frac{\tau^{m-n} - \sigma^{m-n}}{\sqrt{5}})$$

$$= \frac{\tau^{m+n} - \tau^n\sigma^m + \sigma^n\tau^m - \sigma^{m+n}}{\sqrt{5}} + \frac{(-1)^{n+1}\tau^{m-n} - (-1)^{n+1}\sigma^{m-n}}{\sqrt{5}}$$

$$= \frac{\tau^{m+n} - (-1)^n\sigma^{m-n} + (-1)^n\tau^{m-n} - \sigma^{m+n} - (-1)^n\tau^{m-n} + (-1)^n\sigma^{m-n}}{\sqrt{5}}$$

$$= \frac{\tau^{m+n} - \sigma^{m+n}}{\sqrt{5}}$$

$$= F_{m+n}$$

It is easy to see that when $n = 1$ in the above identity, we get the usual Fibonacci recurrence relation, $F_{m+1} = (1)F_m + (1)F_{m-1}$. When $n = m$ we get identity 1.10: $F_{2n} = L_nF_n$.

Identity 2.2 $F_n = \frac{1}{2^{n-1}}[\binom{n}{1} + \binom{n}{3}5 + \binom{n}{5}5^2 + \binom{n}{7}5^3 + \cdots]$.

Proof:

$$F_n = \frac{\tau^n - \sigma^n}{\sqrt{5}} = \frac{1}{2^n\sqrt{5}}[(1+\sqrt{5})^n - (1-\sqrt{5})^n]$$

Now expand using the binomial theorem:

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

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

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

$$= \frac{1}{2^{n-1}}\left[\binom{n}{1} + \binom{n}{3}5 + \binom{n}{5}5^2 + \binom{n}{7}5^3 + \cdots\right]$$

Lastly in this chapter we use τ and σ to demonstrate some simple greatest-integer identities. Though we will not use these, much research has been done in this area and they are certainly of interest in their own right.

Identity 2.3 $F_n = \lfloor \frac{\tau^n}{\sqrt{5}} + \frac{1}{2} \rfloor$ *for all* n.

Proof: $|F_n - \frac{\tau^n}{\sqrt{5}}| = |\frac{\sigma^n}{\sqrt{5}}| < \frac{1}{2}$ for all n.

Identity 2.4 $F_{n+1} = \lfloor \tau F_n + \frac{1}{2} \rfloor$ *for* $n \geq 2$.

Proof: $|F_{n+1} - \tau F_n| = |\frac{\tau^{n+1} - \sigma^{n+1}}{\sqrt{5}} - \frac{\tau^{n+1} - \sigma^n \tau}{\sqrt{5}}| = |\frac{\sigma^n(\tau - \sigma)}{\sqrt{5}}| = |\sigma^n| < \frac{1}{2}$ for all $n \geq 2$.

Chapter 3

Modular Representations of Fibonacci Sequences

One way to learn some fascinating properties of the Fibonacci sequence is to consider the sequence of least nonnegative residues of the Fibonacci numbers under some modulus. One of the first modern inquiries into this area of research was made by D. D. Wall [22] in 1960, though J. L. Lagrange made some observations on these types of sequences in the eighteenth century. Typically, the variable m will be used only to denote a modulus.

3.1 The Period

Perhaps the first thing one notices when the Fibonacci sequence is reduced mod m is that it is periodic. For example,

$$\begin{aligned} F(\text{mod } 4) &= 0\ 1\ 1\ 2\ 3\ 1\ 0\ 1\ 1\ 2\ 3\ ... \\ F(\text{mod } 5) &= 0\ 1\ 1\ 2\ 3\ 0\ 3\ 3\ 1\ 4\ 0\ 4\ 4\ 3\ 2\ 0\ 2\ 2\ 4\ 1\ 0\ 1\ 1\ 2\ 3\ ... \end{aligned}$$

See appendix C for a list of the Fibonacci sequence under various moduli.

Any (generalized) Fibonacci sequence modulo m must repeat. After all, there are only m^2 possible pairs of residues and any pair will completely determine a sequence both forward and backward. If we ignore the pair 0,0 which gives us the trivial sequence, then we know that the period of any Fibonacci sequence mod m has a maximum length of $m^2 - 1$.

It will always happen that the first pair to repeat will be the pair we started with. Suppose that this were not so. Then we might have the sequence $a, b, ..., x, y, ..., x, y, ...$ where the pair a, b is not contained in the block $x, y, ..., x, y$. However, we know that this block repeats backward as well as forward, and so the pair a, b cannot be in the sequence. This gives us our contradiction.

We can say some things about where the zeros will appear in the modular representation of the Fibonacci sequence. Recall from identities 1.2 and 1.4 that

$$\begin{aligned} F_{s+t} &= F_{s-1}F_t + F_sF_{t+1} \\ F_{s-t} &= (-1)^t(F_sF_{t+1} - F_{s+1}F_t). \end{aligned}$$

If $F_s \equiv F_t \equiv 0$ then clearly $F_{s+t} \equiv 0$ and $F_{s-t} \equiv 0$. Hence all the zeros of $F(\text{mod } m)$ are evenly spaced throughout the sequence. Since $F(\text{mod } m)$ is periodic for any m and $F_0 = 0$ we can say that any integer will divide infinitely many Fibonacci numbers. In addition, all the Fibonacci numbers divisible by a given integer are evenly spaced throughout the sequence.

We know that $F(\text{mod } m)$ is periodic, so the question naturally presents itself: What is the relationship between the modulus of a sequence and its period? We will examine some results in this area.

Each author seems to have his or her own notation, but the following definitions come from Wall. Let $k(m)$ denote the period of the Fibonacci sequence modulo m. Let $h(m)$ denote the period of any generalized Fibonacci sequence modulo m. From our previous example we see that $k(4) = 6$ and $k(5) = 20$. The following are some immediate consequences of the definition.

$$\begin{aligned} F_n &\equiv F_{n+r\cdot k(m)} \pmod{m} \\ G_n &\equiv G_{n+r\cdot h(m)} \pmod{m} \\ F_{k(m)} &\equiv 0 \pmod{m} \qquad (3.1) \\ F_{k(m)-1} &\equiv F_{k(m)+1} \equiv F_{k(m)+2} \equiv 1 \pmod{m} \qquad (3.2) \end{aligned}$$

We will often use the fact that if $F_n \equiv 0 \pmod{m}$ and $F_{n+1} \equiv 1 \pmod{m}$ then $k(m)|n$. This result follows immediately from the periodicity of $F(\text{mod } m)$.

We now demonstrate some very general properties of $F(\text{mod } m)$ using our notation. The following three theorems can be found in [22]. The reader is encouraged to examine the table in appendix B which gives the period of $F(\text{mod } m)$ for $2 \leq m \leq 1000$, and observe the behavior of $k(m)$ as m varies. After noticing that $F(\text{mod } m)$ is periodic one notices that almost all of the periods are even. Though Wall provides the next theorem, the proof is the author's.

Theorem 3.1 *For $m \geq 3$, $k(m)$ is even.*

> **Proof:** For ease of notation let $k = k(m)$, and we will consider all congruences to be taken modulo m. From identity 1.3 we know that if t is odd then $F_t = F_{-t}$ and if t is even then $F_t = -F_{-t}$. We will assume k to be odd and show that m must equal 2.
>
> We know that $F_1 = F_{-1} \equiv F_{k-1}$. Now $k-1$ is even so $F_{k-1} = -F_{1-k} \equiv -F_1$. Thus $F_1 \equiv -F_1$, and as a result $m = 2$.

Another curious feature of $F(\text{mod } m)$ is that $k(n)|k(m)$ whenever $n|m$. Surprisingly, this property is true of generalized Fibonacci sequences as well.

Theorem 3.2 *If $n|m$, then for a given Fibonacci sequence, $h(n)|h(m)$.*

> **Proof:** Let $h = h(m)$. We need to show that $G(\text{mod } n)$ repeats in blocks of length h. We do this by showing that $G_i \equiv G_{i+h} \pmod{n}$ regardless of our choice for i. Certainly we know that $G_i \equiv G_{i+h} \pmod{m}$, so for some $0 \leq a < m$ we have $G_i = a + mx$ and $G_{i+h} = a + my$.
>
> Now say $m = nr$ and let us substitute nr for m in the previous two equations. Then $G_i = a+nrx$ and $G_{i+h} = a+nry$. We can say that $a = a'+nw$ $(0 \leq a' < n)$ and this time substitute for a in the previous equations. Now $G_i = a'+n(w+rx)$ and $G_{i+h} = a'+n(w+ry)$. Of course this implies that $G_i \equiv G_{i+h} \pmod{n}$ which was needed to be shown.

We can make this theorem more exact by expressing $h(m)$ in terms of $h(p_i^{e_i})$ where m has the prime factorization $m = \prod p_i^{e_i}$.

Theorem 3.3 *Let m have the prime factorization $m = \prod p_i^{e_i}$. Then $h(m) = \text{lcm}[h(p_i^{e_i})]$, the least common multiple of the $h(p_i^{e_i})$.*

Proof: By our previous theorem $h(p_i^{e_i})|h(m)$ for all i. It follows that $\operatorname{lcm}[h(p_i^{e_i})]|h(m)$.

Second, since $h(p_i^{e_i})|\operatorname{lcm}[h(p_i^{e_i})]$ we know $G(\text{mod } p_i^{e_i})$ repeats in blocks of length $\operatorname{lcm}[h(p_i^{e_i})]$. Hence $G_{\operatorname{lcm}[h(p_i^{e_i})]} \equiv G_0$ and $G_{\operatorname{lcm}[h(p_i^{e_i})]+1} \equiv G_1 \pmod{p_i^{e_i}}$ for all i. Since all the $p_i^{e_i}$ are relatively prime, the Chinese Remainder Theorem assures us that $G_{\operatorname{lcm}[h(p_i^{e_i})]} \equiv G_0$ and $G_{\operatorname{lcm}[h(p_i^{e_i})]+1} \equiv G_1 \pmod{m}$. Thus $G(\text{mod } m)$ repeats in blocks of length $\operatorname{lcm}[h(p_i^{e_i})]$ and we can say that $h(m)|\operatorname{lcm}[h(p_i^{e_i})]$. This concludes the proof.

Hence we have reduced the problem of characterizing $k(m)$ into the problem of characterizing $k(p^e)$. Before we develop theorems which speak to this problem, however, we look at a related result. We see in the following theorem that it is not necessary to break a modulus all the way into its prime factorization in order to attain information about $k(m)$.

Theorem 3.4 $h([m,n]) = [h(m), h(n)]$ *where brackets denote the least common multiple function.*

Proof: Since $m|[m,n]$ and $n|[m,n]$ we know that $h(m)|h([m,n])$ and $h(n)|h([m,n])$. It follows that $[h(m), h(n)]|h([m,n])$.

Say we have the prime factorization $[m,n] = p_1^{e_1} \dots p_t^{e_t}$. Then $h([m,n]) = h(p_1^{e_1} \dots p_t^{e_t}) = [h(p_1^{e_1}) \dots h(p_t^{e_t})]$. Since $p_i^{e_i}$ divides m or n for all i, certainly $h(p_i^{e_i})$ divides $h(m)$ or $h(n)$ for all i. Thus $[h(p_1^{e_1}) \dots h(p_t^{e_t})]|[h(m), h(n)]$. In other words, $h([m,n])|[h(m), h(n)]$.

Hence $h([m,n]) = [h(m), h(n)]$.

Now we turn our attention back to the matter of solving $k(p^e)$ in terms of p^e. The general case of this theorem is somewhat involved, so to motivate the ideas we look at a couple of specific cases. We will demonstrate that $k(2^e) = 3 \cdot 2^{e-1}$ and $k(5^e) = 4 \cdot 5^e$. These results can be found in [11], but the proofs there are somewhat incomplete. For example, Kramer and Hoggatt show that $F_{3 \cdot 2^{e-1}} \equiv 0 \pmod{2^e}$ and $F_{3 \cdot 2^{e-1}+1} \equiv 1 \pmod{2^e}$ and they immediately conclude that $k(2^e) = 3 \cdot 2^{e-1}$. However, this only demonstrates that $k(2^e)|3 \cdot 2^{e-1}$. The proof below takes this point into consideration.

Theorem 3.5 $k(2^e) = 3 \cdot 2^{e-1}$.

Proof: By inspection, $k(2) = 3$ and $k(4) = 6$, so the theorem holds for $e = 1, 2$. Suppose $k(2^r) = 3 \cdot 2^{r-1}$, so that $F_{3\cdot 2^{r-1}} \equiv 0$ and $F_{3\cdot 2^{r-1}+1} \equiv 1 \pmod{2^r}$ and we will induct on r.

By identity 1.10,

$$F_{3\cdot 2^r} = (F_{3\cdot 2^{r-1}})(F_{3\cdot 2^{r-1}-1} + F_{3\cdot 2^{r-1}+1})$$

The first factor on the right, $F_{3\cdot 2^{r-1}} \equiv 0 \pmod{2^r}$. It is an easy matter to see that every third Fibonacci number is even and the rest are odd, so the second factor on the right, $F_{3\cdot 2^{r-1}-1} + F_{3\cdot 2^{r-1}+1} \equiv 0 \pmod 2$. Thus their product, $F_{3\cdot 2^r} \equiv 0 \pmod{2^{r+1}}$.

By identity 1.7,

$$\begin{array}{rcccccl} F_{3\cdot 2^r+1} & = & (F_{3\cdot 2^{r-1}})^2 & + & (F_{3\cdot 2^{r-1}+1})^2 & & \\ & \equiv & (0 \text{ or } 2^r)^2 & + & (1 \text{ or } 2^r+1)^2 & & \pmod{2^{r+1}} \\ & \equiv & 0 & + & 1 & & \pmod{2^{r+1}} \\ & \equiv & 1 & & & & \pmod{2^{r+1}} \end{array}$$

Thus we know $k(2^{r+1})|3 \cdot 2^r$.

We know that $k(2^r)|k(2^{r+1})$, and by our induction hypothesis $k(2^r) = 3 \cdot 2^{r-1}$. Thus $k(2^{r+1}) =$ either $3 \cdot 2^{r-1}$ or $3 \cdot 2^r$. We will show that the latter is true by proving $F_{3\cdot 2^{r-1}+1} \not\equiv 1 \pmod{2^{r+1}}$. More precisely, we will prove that $F_{3\cdot 2^{r-1}+1} \equiv 2^r + 1 \pmod{2^{r+1}}$.

Let us add this statement to our induction hypothesis: assume $F_{3\cdot 2^{r-2}} \equiv 0$ and $F_{3\cdot 2^{r-2}+1} \equiv 2^{r-1} + 1 \pmod{2^r}$. By inspection this is the case for $r = 3$. We will induct on r to show that $F_{3\cdot 2^{r-1}+1} \equiv 2^r + 1 \pmod{2^{r+1}}$.

By identity 1.7,

$$F_{3\cdot 2^{r-1}+1} = (F_{3\cdot 2^{r-2}+1})^2 + (F_{3\cdot 2^{r-2}})^2.$$

Let us look at the first term on the right.

$$\begin{array}{rcl} F_{3\cdot 2^{r-2}+1} & \equiv & (2^{r-1}+1) \text{ or } (2^{r-1}+1+2^r) \pmod{2^{r+1}} \\ (2^{r-1}+1)^2 & = & 2^{2r-2} + 2^r + 1 \equiv 2^r + 1 \pmod{2^{r+1}} \\ (2^{r-1}+1+2^r)^2 & = & (3 \cdot 2^{r-1} + 1)^2 \\ & = & 9 \cdot 2^{2r-2} + 3 \cdot 2^r + 1 \equiv 2^r + 1 \pmod{2^{r+1}} \end{array}$$

Thus

$$(F_{3\cdot 2^{r-2}+1})^2 \equiv 2^r + 1 \pmod{2^{r+1}}.$$

Let us look at the second term on the right.

$$\begin{aligned} F_{3\cdot 2^{r-2}} &\equiv 0 \text{ or } 2^r \pmod{2^{r+1}} \\ 0^2 &\equiv 0 \pmod{2^{r+1}} \\ (2^r)^2 &= 2^{2r} \equiv 0 \pmod{2^{r+1}} \end{aligned}$$

Thus

$$(F_{3\cdot 2^{r-2}})^2 \equiv 0 \pmod{2^{r+1}}.$$

Consequently $F_{3\cdot 2^{r-1}+1} \equiv 2^r + 1 \pmod{2^{r+1}}$ and the theorem follows.

Before we prove a similar theorem for $k(5^e)$ we first need to mention a lemma which provides insight into one of the divisibility properties of the Fibonacci sequence.

Lemma 3.6 *Let p be an odd prime and suppose $p^t | F_n$ but $p^{t+1} \not| F_n$ for some $t \geq 1$. If $p \not| v$ then $p^{t+1} | F_{nvp}$ but $p^{t+2} \not| F_{nvp}$.*

The proof of this lemma is too involved to be examined here, but it can be found in [20].

Since $F_5 = 5$, clearly 5 goes into F_5 once. By the the lemma then, 5 goes into $F_{n\cdot 5^t}$ exactly t times if $5 \not| n$.

Theorem 3.7 $k(5^e) = 4 \cdot 5^e$.

Proof: First we will show that for all e, $F_{4\cdot 5^e} \equiv 0$ and $F_{4\cdot 5^e+1} \equiv 1 \pmod{5^e}$. By the lemma above clearly $F_{4\cdot 5^e} \equiv 0 \pmod{5^e}$. From identity 1.7 we have

$$F_{4\cdot 5^e+1} = (F_{2\cdot 5^e})^2 + (F_{2\cdot 5^e+1})^2.$$

Applying our lemma to the first term on the right gives us $(F_{2\cdot 5^e})^2 \equiv 0^2 \equiv 0 \pmod{5^e}$. By identity 1.8, the second term on the right, $(F_{2\cdot 5^e+1})^2 = F_{2\cdot 5^e} F_{2\cdot 5^e+2} + (-1)^{2\cdot 5^e+2} \equiv 1 \pmod{5^e}$.

Thus we know that $F_{4\cdot 5^e} \equiv 0$ and $F_{4\cdot 5^e+1} \equiv 1 \pmod{5^e}$ and it follows that $k(5^e) | 4 \cdot 5^e$ for all e.

We proceed now by induction using the hypothesis $k(5^r) = 4 \cdot 5^r$. By inspection this is the case for $r = 1$. We induct on r to show $k(5^{r+1}) = 4 \cdot 5^{r+1}$.

Since $4 \cdot 5^r = k(5^r)|k(5^{r+1})$ and $k(5^{r+1})|4 \cdot 5^{r+1}$, we know $k(5^{r+1}) =$ either $4 \cdot 5^r$ or $4 \cdot 5^{r+1}$. In the first case, $F_{4 \cdot 5^r}$ contains exactly r factors of 5 and hence $F_{4 \cdot 5^r} \not\equiv 0 \pmod{5^{r+1}}$. Hence we must have $k(5^{r+1}) = 4 \cdot 5^{r+1}$ and our theorem is proved.

We have proved $k(p^e) = p^{e-1}k(p)$ for $p = 2$ and $p = 5$, and we now turn to proving it for all p. While the general theorem is slightly less strict than these special cases, it does give us great insight into the periodic behavior of the Fibonacci sequence. One proof, by Robinson[15], also shows how matrices may be used to discover facts about the Fibonacci sequence. We will be working with the matrix U defined by

$$U = \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}$$

which has the property that

$$U^n = \begin{bmatrix} F_{n-1} & F_n \\ F_n & F_{n+1} \end{bmatrix}. \tag{3.3}$$

This matrix has been called the *Fibonacci matrix* because of this property. Note that $U^{k(m)} = I + mB \equiv I \pmod{m}$ for some 2×2 matrix B. And, if $U^n \equiv I \pmod{m}$ then $k(m)|n$.

Theorem 3.8 *If t is the largest integer such that $k(p^t) = k(p)$ then $k(p^e) = p^{e-t}k(p)$ for all $e \geq t$.*

Proof: Since $U^{k(p^e)} = I + p^eB$ we can write $U^{pk(p^e)} = (I + p^eB)^p = I^p + \binom{p}{1} I^{p-1}(p^eB) + \binom{p}{2} I^{p-2}(p^eB)^2 + \cdots$. Thus $U^{pk(p^e)} \equiv I \pmod{p^{e+1}}$. Clearly $U^{k(p^{e+1})} \equiv I \pmod{p^{e+1}}$ and so we have $k(p^{e+1})|pk(p^e)$. Combine this fact with the knowledge that $k(p^e)|k(p^{e+1})$ and as a result $k(p^{e+1}) = k(p^e)$ or $pk(p^e)$.

Now let us assume that $k(p^{e+1}) = pk(p^e)$ and we will induct on e to arrive at $k(p^{e+2}) = pk(p^{e+1})$.

By assumption $k(p^e) \neq k(p^{e+1})$ and so we know that $U^{k(p^e)} = I + p^eB$ where $p \not| B$. Hence $U^{pk(p^e)} = (I + p^eB)^p = I^p + \binom{p}{1} I^{p-1}(p^eB) + \binom{p}{2} I^{p-2}(p^eB)^2 + \cdots \equiv I + p^{e+1}B \pmod{p^{e+2}}$. (The astute reader may notice that this congruence does not actually hold for $p = 2$, $e = 1$. However, since we have proven the case for $p = 2$ in theorem 3.5 we may assume $p \geq 3$.) That is, $U^{k(p^{e+1})} = U^{pk(p^e)} \equiv I + p^{e+1}B \not\equiv I \pmod{p^{e+2}}$. This implies $k(p^{e+1}) \neq k(p^{e+2})$ so we must have $k(p^{e+2}) = pk(p^{e+1})$ and the induction is complete.

Now let t be the largest e such that $k(p^e) = k(p)$. Then $k(p^e) = k(p)$ for $1 \leq e \leq t$ and $k(p^e) = k(p^{e-t})$ for $e \geq t$.

Remarkably, the conjecture that $t = 1$ for all primes has existed since Wall's paper in 1960, but neither a proof nor a counter example has yet been found. Once again we have been able to reduce the problem of finding the period of the Fibonacci sequence given a modulus. All that remains (other than proving $t = 1$ for all primes, of course) is to characterize $k(p)$ in terms of p. However, this undertaking has proven to be extraordinarily difficult, and the best we can do is to describe some bounds on $k(p)$.

Theorems 3.11 through 3.13 will describe upper bounds on $k(p)$, but we must first take some time to develop certain divisibility properties of the Fibonacci sequence found in [20]. We will make use of these three facts for primes, p:

$$\text{(i)} \quad \binom{p}{n} \equiv 0 \pmod{p} \text{ for } 1 \leq n \leq p-1$$

$$\text{(ii)} \quad \binom{p-1}{n} \equiv (-1)^n \pmod{p} \text{ for } 0 \leq n \leq p-1$$

$$\text{(iii)} \quad \binom{p+1}{n} \equiv 0 \pmod{p} \text{ for } 2 \leq n \leq p-1$$

We will also use the following lemma:

Lemma 3.9 *5 is a quadratic residue modulo primes of the form* $5t \pm 1$ *and a quadratic nonresidue modulo primes of the form* $5t \pm 2$.

Proof: Using the Legendre symbol and the law of quadratic reciprocity we know that $(\frac{5}{p}) = (\frac{p}{5})$ since 5 is a prime of the form $4t + 1$. Then,

$$\left(\frac{5}{5t+1}\right) = \left(\frac{5t+1}{5}\right) = \left(\frac{1}{5}\right) = 1$$

$$\left(\frac{5}{5t-1}\right) = \left(\frac{5t-1}{5}\right) = \left(\frac{4}{5}\right) = 1.$$

However,

$$\left(\frac{5}{5t+2}\right) = \left(\frac{5t+2}{5}\right) = \left(\frac{2}{5}\right) = -1$$

$$\left(\frac{5}{5t-2}\right) = \left(\frac{5t-2}{5}\right) = \left(\frac{3}{5}\right) = -1.$$

Using identity 2.2 we have $2^{p-1}F_p = \binom{p}{1} + \binom{p}{3}5 + \cdots + \binom{p}{p}5^{\frac{p-1}{2}}$. Applying (i) above and Fermat's theorem we get $F_p \equiv 5^{\frac{p-1}{2}} \pmod{p}$. Now from the lemma we know that $5^{\frac{p-1}{2}} \equiv 1 \pmod{p}$ if and only if $p = 5t \pm 1$, and $5^{\frac{p-1}{2}} \equiv -1 \pmod{p}$ if and only if $p = 5t \pm 2$. Hence,

If a prime p is of the form $5t \pm 1$ then $F_p \equiv 1 \pmod{p}$.
If a prime p is of the form $5t \pm 2$ then $F_p \equiv -1 \pmod{p}$.

The converse of these statements is not true, for in fact $F_{22} = 17711 = 85(22) + 1 \equiv 1 \pmod{22}$, and quite clearly, 22 is not prime.

Again we use identity 2.2 and see $2^{p-2}F_{p-1} = \binom{p-1}{1} + \binom{p-1}{3}5 + \cdots + \binom{p-1}{p-2}5^{\frac{p-3}{2}}$. By (ii) above, $2^{p-2}F_{p-1} \equiv -(1 + 5 + 5^2 + \cdots + 5^{\frac{p-3}{2}}) \pmod{p}$. Summing the geometric series yields,

$$2^{p-2}F_{p-1} \equiv -\frac{5^{\frac{p-1}{2}} - 1}{4} \pmod{p}.$$

Clearly if $5^{\frac{p-1}{2}} \equiv 1 \pmod{p}$ then $2^{p-2}F_{p-1} \equiv 0 \pmod{p}$. Certainly $2^{p-2} \not\equiv 0 \pmod{p}$ so it would have to be that $F_{p-1} \equiv 0 \pmod{p}$. Hence,

If a prime p is of the form $5t \pm 1$ then $F_{p-1} \equiv 0 \pmod{p}$.

Finally, identity 2.2 gives us $2^pF_{p+1} = \binom{p+1}{1} + \binom{p+1}{3}5 + \cdots + \binom{p+1}{p}5^{\frac{p-1}{2}}$. By (iii) above, $2^pF_{p+1} \equiv \binom{p+1}{1} + \binom{p+1}{p}5^{\frac{p-1}{2}} = (p+1) + (p+1)5^{\frac{p-1}{2}} \equiv 1 + 5^{\frac{p-1}{2}} \pmod{p}$. Now when $5^{\frac{p-1}{2}} \equiv -1 \pmod{p}$ we will have $2^pF_{p+1} \equiv 0 \pmod{p}$. Since $2^p \equiv 2 \pmod{p}$, it would have to be that $F_{p+1} \equiv 0 \pmod{p}$. Thus,

If a prime p is of the form $5t \pm 2$ then $F_{p+1} \equiv 0 \pmod{p}$.

Collecting our results provides us with the following theorem.

Theorem 3.10 *If a prime p is of the form $5t \pm 1$ then $F_{p-1} \equiv 0$ and $F_p \equiv 1 \pmod{p}$. If a prime p is of the form $5t \pm 2$ then $F_p \equiv -1$ and $F_{p+1} \equiv 0 \pmod{p}$.*

Now at last we can present some theorems concerning the character of $k(p)$.

Theorem 3.11 *If p is a prime, $p \neq 5$, then $k(p)|p^2-1$.*

Proof: By inspection, $k(2) = 3$, and the theorem holds for $p = 2$. Now let us assume p odd. To prove the theorem we will show that $F_{p^2-1} \equiv 0$ and $F_{p^2} \equiv 1 \pmod{p}$.

If $p = 5t \pm 1$ then $p|F_{p-1}$. We know that $p-1|p^2-1$ and so $F_{p-1}|F_{p^2-1}$. Hence $p|F_{p^2-1}$. If $p = 5t \pm 2$ then $p|F_{p+1}$. We know that $p+1|p^2-1$ and so $F_{p+1}|F_{p^2-1}$. Hence $p|F_{p^2-1}$. Thus for all $p \neq 5$, $F_{p^2-1} \equiv 0 \pmod{p}$.

To prove $F_{p^2} \equiv 1 \pmod{p}$, we first note that $2^{p^2-1}F_{p^2} = \binom{p^2}{1} + \binom{p^2}{3}5 + \cdots + \binom{p^2}{p^2}5^{\frac{p^2-1}{2}}$. Now $2^{p^2-1} = (2^{p-1})^{p+1} \equiv 1 \pmod{p}$ and $\binom{p^2}{n} \equiv 0 \pmod{p}$ for $1 \leq n \leq p^2-1$. Hence $F_{p^2} \equiv (5^{\frac{p-1}{2}})^{p+1} \equiv (\pm 1)^{p+1} \equiv 1 \pmod{p}$.

Thus the theorem is proved.

Theorem 3.12 *If a prime p is of the form $5t \pm 1$ then $k(p)|p-1$.*

Proof: Since $p = 5t \pm 1$, theorem 3.10 tells us that $F_{p-1} \equiv 0$ and $F_p \equiv 1 \pmod{p}$. Hence $F(\text{mod } p)$ repeats in blocks of length $p-1$. Thus $k(p)|p-1$.

Theorem 3.13 *If a prime p is of the form $5t \pm 2$ then $k(p)|2p+2$.*

Proof: Suppose $p = 5t \pm 2$. By theorem 3.10 then, $F_{p+1} \equiv 0 \pmod{p}$. Since $p+1|2p+2$ and the zeros of $F(\text{mod } p)$ are evenly spaced, we can say $F_{2p+2} \equiv 0 \pmod{p}$.

We also know that $F_p \equiv -1 \pmod{p}$. By the usual recurrence relation then, $F_{p+2} \equiv F_{p+3} \equiv -1 \pmod{p}$. Now we can write $F_{2p+3} = F_{(p+1)+(p+2)} = F_pF_{p+2} + F_{p+1}F_{p+3} \equiv (-1)(-1) + (0)(-1) \equiv 1 \pmod{p}$.

Thus $k(p)|2p+2$.

We now consider upper and lower bounds for $k(m)$ where m can be any integer $m \geq 2$. It was noted earlier that $k(m) \leq m^2 - 1$, but can we do better than this? One method of determining an upper bound is to use the two preceding theorems to show that $k(p) = p^2 - 1$ if and only if $p = 2$ or 3. Then by application of theorem 3.8 it can be proved that $k(p^e) < (p^e)^2 - 1$ for $e \geq 2$. Finally, we can use theorem 3.4 to demonstrate that $k(m) < m^2 - 1$ for all composite m.

However, the author would like to propose a more elegant way of proving this inequality. If $k(m) = m^2 - 1$ for some m, then every possible pair of residues except $0, 0$ appears in $F(\text{mod } m)$. It will be seen in section 3.3 that a single period of $F(\text{mod } m)$ contains at most four zeros. Consequently, $F(\text{mod } m)$ contains at most four $0, r$ pairs where $1 \leq r < m$. Hence, for $m \geq 6$ there is some $0, r$ pair not represented in $F(\text{mod } m)$ and we must have $k(m) < m^2 - 1$. It is a simple matter to check the remaining cases. When $m = 2$ or 3, $k(m) = m^2 - 1$ and when $m = 4$ or 5, $k(m) < m^2 - 1$.

Unfortunately, empirical evidence indicates that this upper bound becomes less and less precise as m increases. For $2 \leq m \leq 299$ we find by inspection that $k(m) \leq 6m$. For $300 \leq m \leq 1000$ we find $k(m) \leq 4m$. There does not appear to be any other material published concerning upper bounds on $k(m)$.

A sharp lower bound on $k(m)$ was given by Paul Catlin[5] in 1974. We see here an interesting interaction between the Lucas and Fibonacci numbers. We present his theorem without proof.

Theorem 3.14 *Given a modulus $m > 2$, let t be any natural number such that $L_t \leq m$. Then $k(m) \geq 2t$ with equality if and only if $L_t = m$ and t is odd.*

In the beginning of the section we saw some results which helped to define the overall character of $h(m)$ and thus of $k(m)$. In the last part of this section we present some results due to Wall on the relationship between $h(m)$ and $k(m)$. The first of these is strikingly simple.

Theorem 3.15 *$h(m)|k(m)$.*

> **Proof:** For ease of notation, let $k = k(m)$. Applying identity 1.11 and then equations 3.1 and 3.2 we get $G_k = F_{k-1}G_0 + F_kG_1 \equiv G_0 \pmod{m}$ and $G_{k+1} = F_kG_0 + F_{k+1}G_1 \equiv G_1 \pmod{m}$. Thus $G(\mathrm{mod}\ m)$ repeats in blocks of length $k(m)$. From this we can conclude $h(m)|k(m)$.

We can elicit equality between $h(m)$ and $k(m)$ by putting stricter conditions on m.

Theorem 3.16 *If a prime p is of the form $5t \pm 2$ then $h(p^e) = k(p^e)$.*

Proof: For ease of notation, let $h = h(p^e)$. Certainly,

$$\begin{aligned} G_h - G_0 &\equiv 0 \pmod{p^e}, \text{ and} \\ G_{h-1} - G_1 &\equiv 0 \pmod{p^e}. \end{aligned}$$

By identity 1.11 the above is equivalent to

$$\begin{aligned} (F_{h-1}G_0 + F_hG_1) - G_0 &= G_1F_h + G_0(F_{h-1} - 1) \equiv 0 \pmod{p} \\ (F_{h-1}G_1 + F_{h+1}G_2) - G_1 &= G_2F_h + G_1(F_{h-1} - 1) \equiv 0 \pmod{p} \end{aligned}$$

We now have a system of equations which we may treat as a matrix with determinant $D = G_1^2 - G_0G_2$. We will assume that $D \equiv 0 \pmod{p}$ and arrive at a contradiction.

When $D \equiv 0 \pmod{p}$ then $G_1^2 - G_0G_2 = G_1^2 - G_0(G_0 + G_1) = G_1^2 - G_0G_1 - G_0^2 \equiv 0 \pmod{p}$. This last congruence is impossible if $p = 2$ (we ignore the trivial case $G_0 = G_1 = 0$) so we may assume p to be odd. Multiply both sides by -4.

$$4G_0^2 + 4G_0G_1 - 4G_1^2 \equiv 0 \pmod{p}$$

Add $5G_1^2$ to both sides.

$$4G_0^2 + 4G_0G_1 + G_1^2 = (2G_0 + G_1)^2 \equiv 5G_1^2 \pmod{p}$$

Now multiply both sides by G_1^{p-3} and apply Fermat's theorem to the right.

$$G_1^{p-3}(2G_0 + G_1)^2 \equiv 5 \pmod{p}$$

Since p is odd, this implies that 5 is a quadratic residue modulo p. However, by lemma 3.9, this contradicts our hypothesis that $p = 5t \pm 2$. Therefore, $D \not\equiv 0 \pmod{p}$, and this implies that $D \not\equiv 0 \pmod{p^e}$.

Since the determinant of our matrix is not congruent to zero $\pmod{p^e}$, it must have a unique solution modulo p^e. Certainly $F_h \equiv 0$ and $(F_{h-1} - 1) \equiv 0 \pmod{p^e}$ satisfy the system, and so $F_h \equiv 0$ and $F_{h-1} \equiv 1 \pmod{p^e}$. From the recurrence relation, $F_{h+1} \equiv 1 \pmod{p^e}$ as well.

Since $h = h(p^e)$ our results tell us that $k(p^e)|h(p^e)$. By theorem 3.15 we know $h(p^e)|k(p^e)$. Hence $h(p^e) = k(p^e)$.

Wall proved several other results regarding the relationship between $h(m)$ and $k(m)$. We present some of these here without proof. As usual, p denotes a prime number.

Theorem 3.17 *Let $D = G_1^2 - G_0G_1 - G_0^2$. If $\gcd(D, m) = 1$ then $h(m) = k(m)$.*

Theorem 3.18 *If $h(p^e) = 2t + 1$ for some generalized Fibonacci sequence, then $k(p^e) = 4t + 2$.*

Theorem 3.19 *If $p > 2$ and $k(p^e) = 4t + 2$ then there exists some generalized Fibonacci sequence where $h(p^e) = 2t + 1$.*

Theorem 3.20 *Let p be odd and $p \neq 5$. If $h(p^e)$ is even then $h(p^e) = k(p^e)$.*

We end the section with two curious theorems pertaining to the period of $F \pmod{m}$ which did not seem to fit logically elsewhere within this section. We defer their proofs to the end of section 3.3 where we will have developed other ideas sufficiently to make their proofs easy. The curious feature here is that the modulus of the sequence is an actual Fibonacci or Lucas number. Theorem 3.45 can be found in [7] and theorem 3.46 can be found in [17].

Theorem 3.45 *If $n \geq 5$ is odd then $k(F_n) = 4n$. If $n \geq 4$ is even then $k(F_n) = 2n$.*

Theorem 3.46 *If $n \geq 3$ is odd then $k(L_n) = 2n$. If $n \geq 2$ is even then $k(L_n) = 4n$.*

These theorems indicate that for any even $t \geq 6$ there is some m such that $k(m) = t$. Also, $k(m)$ can not equal 4, otherwise $F_4 = 3 \equiv 0$ and $F_3 = 2 \equiv 1 \pmod{m}$ which is not possible. Hence the range of $k(m)$ is 3 union the set of all even numbers greater than or equal to 6.

3.2 The Distribution Of Residues

In this section we look at what is known about the distribution of residues within a single period of $F(\text{mod } m)$. That is, how frequently each residue is expected to appear. We start off with a more specific question: for which moduli will all the residues appear with equal frequency within a single period? If $F(\text{mod } m)$ exhibits this property it is said to be *uniform* or *uniformly distributed*. Kuipers and Shiue[12] proved that the only time $F(\text{mod } m)$ can possibly be uniform is when $m = 5^e$.

It is not difficult to see that if $F(\text{mod } m)$ is uniform, then necessarily $m|k(m)$. We use this requirement to prove that 5 is the only prime for which $F(\text{mod } p)$ is uniform.

We first note that by inspection $F(\text{mod } 2)$ is not uniform but $F(\text{mod } 5)$ is, with each residue appearing four times per period. Let us consider odd primes p.

If $p = 5t \pm 1$ then $F(\text{mod } p)$ cannot be uniform. For such p, we know $k(p)|p-1$, but $p \not| p-1$ and so $p \not| k(p)$.

If $p = 5t \pm 2$ then $F(\text{mod } p)$ cannot be uniform. In this case $k(p)|2p+2$, but for odd p we know $p \not| 2p+2$. Hence $p \not| k(p)$. Thus 5 is the only prime for which $F(\text{mod } p)$ is uniform.

Now we mention a second fact about uniform distribution: if $F(\text{mod } m)$ is uniform and $n|m$, then $F(\text{mod } n)$ is also uniform. Suppose $m = nr$. Then in one period of $F(\text{mod } m)$ each of the residues 0, 1,..., $n-1$ occurs with equal frequency as do the residues n, $n+1$,...,

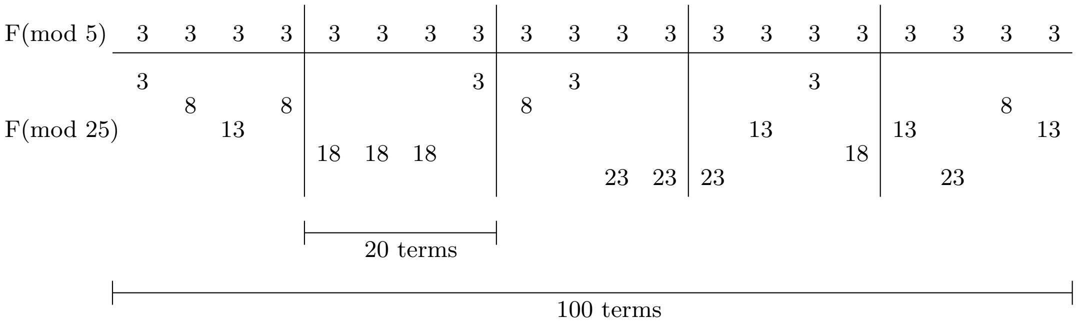


Figure 3.1: Comparing residues mod 5 and mod 25. The residues mod 25 are "stratified" to display them more clearly.

$2n-1$, and so on until $(r-1)n$, $(r-1)n+1$,..., $rn-1$. Thus within $k(m)$ terms of $F(\text{mod } n)$ the residues 0, 1, 2, ..., $(n-1)$ appear with equal frequency, say t times. Since $k(n)|k(m)$ we can find these $k(m)$ terms by simply repeating the first $k(n)$ terms. If $\frac{k(m)}{k(n)} = u$, then within $k(n)$ terms each residue appears $\frac{t}{u}$ times. Hence $F(\text{mod } n)$ is uniform.

Putting these two facts together provides us with the following theorem.

Theorem 3.21 *The only possible values of* m *for which* $F(\textit{mod } m)$ *is uniform are* $m = 5^e$.

It takes a very clever proof to finally settle the issue as we will demonstrate next. Niederreiter provided such a proof in [14].

Theorem 3.22 $F(\textit{mod } 5^e)$ *is uniform for all integers* $e \geq 1$.

Before we start in earnest, we present the basic idea behind the proof. We know that $k(5^e) = 4 \cdot 5^e$ and so "it will suffice to show that among the first $4 \cdot 5^e$ elements of the sequence, we find exactly four elements, or, equivalently, at most four elements from each residue class mod 5^e."

For example, modulo 5 we see that the residue 3 appears exactly four times per period. Modulo 25, the residues 3, 8, 13, 18, and 23 each appear exactly four times in one period. Each of the five sections in figure 3.1 represents one period mod 5, and the bottom portion shows where the residues 3, 8, 13, 18, and 23 appear in relation to the threes.

Proof: Let us assume that $F(\text{mod } 5^{r-1})$ is uniform and we will use induction on r. We have seen that the hypothesis holds for $r = 2$.

Consider integers a and b such that $0 \leq a < 5^{r-1}$ and $0 \leq b < 5^r$. (In the figure we show $a = 3$ and $r = 2$.) $F_n \equiv a \pmod{5^{r-1}}$ has four solutions: $n = c_1$, c_2, c_3, c_4, with $0 \leq c_1, c_2, c_3, c_4 < 4 \cdot 5^{r-1}$. Suppose $b \equiv a \pmod{5^{r-1}}$ and $n = d$ is a solution to $F_n \equiv b \pmod{5^r}$ where $0 \leq d < 4 \cdot 5^r$. Then $F_d \equiv a \pmod{5^{r-1}}$. Hence by periodicity we must have $d \equiv c_i \pmod{4 \cdot 5^{r-1}}$ for some i. We will show that there is only one solution d such that $d \equiv c_i \pmod{4 \cdot 5^r}$ for each i.

Suppose $m \equiv n \pmod{4 \cdot 5^{r-1}}$ and $F_m \equiv F_n \pmod{5^r}$. Let $0 \leq m, n < 4 \cdot 5^r$, and without loss of generality, say $m \leq n$. We will prove that, in fact, $m = n$.

From identity 2.2, $F_n \equiv F_m \pmod{5^r}$ implies

$$\sum_{j=0} 5^j \binom{n}{2j+1} \equiv 2^{n-m} \sum_{j=0} 5^j \binom{m}{2j+1} \pmod{5^r}.$$

Now $4 \cdot 5^{r-1} | n - m$ and by the Euler-Fermat theorem, $\phi(5^r) = 5^r - 5^{r-1} = 4 \cdot 5^{r-1}$. Thus $2^{n-m} \equiv 1 \pmod{5^r}$. Hence we have,

$$\sum_{j=0} 5^j \left[\binom{n}{2j+1} - \binom{m}{2j+1} \right] \equiv 0 \pmod{5^r} \qquad (3.4)$$

Here we use the known identity $\binom{s+t}{u} = \sum_{i=0}^{u} \binom{s}{i} \binom{t}{u-i}$ to obtain $\binom{n}{2j+1} = \sum_{i=0}^{2j+1} \binom{n-m}{i} \binom{m}{2j+1-i}$. That is,

$$\binom{n}{2j+1} = \binom{m}{2j+1} + \sum_{i=1}^{2j+1} \binom{n-m}{i} \binom{m}{2j+1-i}.$$

Substituting this result into equation (3.4) gives us

$$\sum_{j=0} \left[\sum_{i=1}^{2j+1} 5^j \binom{n-m}{i} \binom{m}{2j+1-i} \right] \equiv 0 \pmod{5^r}.$$

We claim that for $j \geq 1$ each term in brackets is divisible by 5^r. Consider $5^j \binom{n-m}{i} = \frac{5^j (n-m)!}{i!(n-m-i)!}$. Cancelling out 5's from $i!$ against 5^j always leaves at least one power of 5 in the latter. This is so since the largest value for i is $2j+1$ and the largest exponent t such that 5^t divides $(2j+1)!$ is given by

$$t = \sum_{i=1}^{\infty} \lfloor \frac{2j+1}{5^i} \rfloor < \sum_{i=1}^{\infty} \frac{2j+1}{5^i} = \frac{2j+1}{4} < j.$$

(The above identity can be found in [4]).

Since there is a factor of 5^{r-1} in $n - m$ we get the desired divisibility property. Hence only the term corresponding to $j = 0$ remains. That is, $n - m \equiv 0 \pmod{5^r}$. Now we can say that $5^r | n - m$ and $4 \cdot 5^{r-1} | n - m$. Thus $4 \cdot 5^r | n - m$. We know that $0 \leq m, n < 4 \cdot 5^r$, and so we must conclude that $n = m$.

Therefore any residue mod 5^r appears at most four times, which implies that each residue must appear exactly four times, which gives us $F(\text{mod } 5^r)$ is uniform. The induction is complete and the theorem proved.

While $F(\text{mod } m)$ is uniformly distributed only for $m = 5^e$, one wonders if there is at least a predictable distribution of residues under different moduli. In 1992 E. T. Jacobson[10] fully described the distribution of residues in $F(\text{mod } 2^e)$ and $F(\text{mod } 2^i \cdot 5^j)$ for $i \geq 5$, and $j \geq 0$. We present his results below without proof.

Let $v(m, b)$ be the number of occurrences of b as a residue in one period of $F(\text{mod } m)$. We have seen that $v(5^e, b) = 4$ for all $b \pmod{5^e}$.

Theorem 3.23 *For F(mod 2^e) the following is true:*

For $1 \leq e \leq 4$:

$$\begin{array}{l}
v(2,0) = 1 \\
v(2,1) = 2 \\
v(4,0) = v(4,2) = 1 \\
v(8,0) = v(8,2) = v(16,0) = v(16,8) = 2 \\
v(16,2) = 4 \\
v(2^e, b) = 1 \text{ if } b \equiv 3 \pmod{4} \text{ and } 2 \leq e \leq 4 \\
v(2^e, b) = 3 \text{ if } b \equiv 1 \pmod{4} \text{ and } 2 \leq e \leq 4 \\
v(2^e, b) = 0 \text{ in all other cases.}
\end{array}$$

For $e \geq 5$:

$$v(2^e, b) = \begin{cases} 1, & \text{if } b \equiv 3 \pmod{4} \\ 2, & \text{if } b \equiv 0 \pmod{8} \\ 3, & \text{if } b \equiv 1 \pmod{4} \\ 8, & \text{if } b \equiv 2 \pmod{32} \\ 0, & \text{for all other residues.} \end{cases}$$

For F(mod $2^i \cdot 5^j$) where $i \geq 5$, and $j \geq 0$, the following is true:

$$v(2^i \cdot 5^j, b) = \begin{cases} 1, \text{ if } b \equiv 3 \pmod{4} \\ 2, \text{ if } b \equiv 0 \pmod{8} \\ 3, \text{ if } b \equiv 1 \pmod{4} \\ 8, \text{ if } b \equiv 2 \pmod{32} \\ 0, \text{ for all other residues.} \end{cases}$$

It does not appear that any other work has been published on the distribution of residues for other moduli.

3.3 The Zeros Of F(mod m)

The previous section indicates that the problem of describing all the residues for a given modulus can be quite difficult, but when we restrict our attention to the behavior of the zeros, many fascinating relationships become readily apparent.

Let $\alpha(m)$ denote the subscript of the first positive term of the Fibonacci sequence which is divisible by m. Vinson calls this the restricted period of $F(\text{mod } m)$. Since the subscripts of the terms for which $F_n \equiv 0 \pmod{m}$ form a simple arithmetic progression, it is clear that $\alpha(m)|k(m)$. In fact one sees without too much difficulty that $\alpha(m)|n$ if and only if $m|F_n$. We use this idea in the following theorem.

Theorem 3.24 *$\alpha(m)|\alpha(mn)$.*

> **Proof:** By definition, we know that $mn|F_{\alpha(mn)}$. Clearly then $m|F_{\alpha(mn)}$, and so $\alpha(m)|\alpha(mn)$.

Let $s(m)$ be the least residue of $F_{\alpha(m)+1}$ modulo m. Because of the relationship $(F_{\alpha(m)}, F_{\alpha(m)+1}) = s(m)(0,1) \pmod{m}$ we call $s(m)$ the multiplier of $F(\text{mod } m)$.

Finally, let $\beta(m)$ denote the order of $s(m)$ modulo m. In other words, $s(m)^{\beta(m)} \equiv 1 \pmod{m}$, and if $n < \beta(m)$ then $s(m)^n \not\equiv 1 \pmod{m}$.

Note the table in appendix B which compares the values of m, $k(m)$, $\alpha(m)$, and $\beta(m)$. The next theorem ties together these three functions nicely. Robinson[15] states and proves it, but also mentions that is a well known property. The proof presented here is the author's.

Theorem 3.25 *$k(m) = \alpha(m)\beta(m)$.*

Proof: Suppose that a single period of $F(\text{mod } m)$ is partitioned into smaller, finite subsequences $A_0, A_1, A_2, \ldots$ as shown below:

$$\underbrace{0\ 1 \cdots s_1}_{A_0}\underbrace{0\ s_1 \cdots s_2}_{A_1}\underbrace{0\ s_2 \cdots s_3}_{A_2}0\ s_3 \cdots\cdots\cdots 0\ 1 \tag{3.5}$$

Each subsequence A_i has $\alpha(m)$ terms, it contains exactly one zero, and $s_1 = s(m)$.

Every subsequence A_i for $i \geq 1$ is a multiple of A_0. More precisely, the following congruences hold modulo m.

$$\begin{aligned} A_1 &\equiv s_1 A_0 \\ A_2 &\equiv s_2 A_0 \\ &\vdots \\ A_{n-1} &\equiv s_{n-1} A_0 \\ A_n &\equiv s_n A_0 \\ &\vdots \end{aligned}$$

Now the last term in A_{n-1} is s_n, and the last term in A_0 is s_1. Thus

$$\begin{aligned} s_n &\equiv (s_{n-1}) \cdot s_1 \\ &\equiv (s_{n-2}) \cdot s_1 \cdot s_1 \\ &\equiv (s_{n-3}) \cdot s_1 \cdot s_1 \cdot s_1 \\ &\vdots \\ &\equiv s_1^n \end{aligned}$$

with congruences modulo m. Since $\beta(m)$ is the order of s_1, sequence (3.5) can be rewritten as

$$0\ 1 \cdots 0\ s_1 \cdots 0\ s_1^2 \cdots 0\ s_1^3 \cdots\cdots\cdots 0\ s_1^{\beta(m)-1} \cdots 0\ 1$$

Thus $\beta(m)$ can be interpreted in a different way: it is the number of zeros in a single period of $F(\text{mod } m)$. Clearly it follows that $k(m) = \alpha(m)\beta(m)$.

There is an identity which follows from the proof.

Identity 3.26 $F_{n\cdot\alpha(m)+r} \equiv F^n_{\alpha(m)+1} \cdot F_r \pmod{m}$.

> **Proof:** The identity comes from the fact that $A_n \equiv s_1^n A_0$. More specifically, the r^{th} term of A_n is congruent to s_1^n times the r^{th} term of A_0 modulo m.

As a point of interest, note the property that $\gcd(m, s_i) = 1$ for all i. This must be the case since $(s_i)^{\beta(m)} = (s_1^i)^{\beta(m)} = (s_1^{\beta(m)})^i \equiv 1 \pmod{m}$. We could also draw this conclusion from theorem 1.1, realizing that if $m|F_n$ then m and F_{n+1} have no nontrivial divisors in common.

The following theorem doesn't appear to give us any immediate insight into $F(\text{mod } m)$, but a couple of nice corollaries follow from it. The proof comes from Robinson [15], but he acknowledges that Morgan Wood knew the result in the early 1930's.

Theorem 3.27 *$k(m) = \gcd(2, \beta(m)) \cdot \text{lcm}[\alpha(m), \gamma(m)]$ where $\gamma(2) = 1$ and $\gamma(m) = 2$ for $m > 2$.*

Proof: By identity 1.8, $F_n^2 - F_{n+1}F_{n-1} = (-1)^{n+1}$ so

$$F^2_{\alpha(m)} - F_{\alpha(m)+1}F_{\alpha(m)-1} = (-1)^{\alpha(m)+1}.$$

Since $F_{\alpha(m)} \equiv 0$ and $F_{\alpha(m)+1} \equiv F_{\alpha(m)-1} \pmod{m}$,

$$-F^2_{\alpha(m)+1} \equiv (-1)^{\alpha(m)+1} \pmod{m}.$$

That is,

$$(s(m))^2 \equiv (-1)^{\alpha(m)} \pmod{m}. \tag{3.6}$$

Thus $(s(m))^2$ and $(-1)^{\alpha(m)}$ have the same order modulo m. Specifically,

$$\frac{\beta(m)}{\gcd(2, \beta(m))} = \frac{\gamma(m)}{\gcd(\alpha(m), \gamma(m))}$$

where $\gamma(m)$ is the order of -1 modulo m. Thus

$$\begin{aligned} k(m) &= \alpha(m)\beta(m) = \alpha(m)\frac{\gcd(2, \beta(m)) \cdot \gamma(m)}{\gcd(\alpha(m), \gamma(m))} \\ &= \gcd(2, \beta(m)) \cdot \text{lcm}[\alpha(m), \gamma(m)]. \end{aligned}$$

Corollary 3.28 *$k(m)$ is even for $m > 2$.*

Proof: By the proceeding theorem, if $k(m)$ is odd we must have $\text{lcm}[\alpha(m), \gamma(m)]$ odd. For that to happen $\gamma(m)$ must be odd. By the nature of $\gamma(m)$ then $m = 2$. Hence the contrapositive (for applicable values of m): If $m > 2$ then $k(m)$ is even.

One of the more surprising properties of $F(\text{mod } m)$ is demonstrated in the following corollary.

Corollary 3.29 *$\beta(m)$ = 1, 2, or 4.*

Proof:

$$\begin{aligned} k(m) &= \gcd(2, \beta(m)) \cdot \text{lcm}[\alpha(m), \gamma(m)] \\ &= (1 \text{ or } 2) \cdot (\alpha(m) \text{ or } 2\alpha(m)) \\ &= \alpha(m),\ 2\alpha(m),\ \text{or } 4\alpha(m). \end{aligned}$$

Therefore $\beta(m) = 1$, 2, or 4.

Recall that it is this theorem which allows us to say that $k(m) < m^2 - 1$ for $m \geq 6$.

We have already seen that $\alpha(m)$ shares a property with $k(m)$ in that $\alpha(m)|\alpha(mn)$. We will demonstrate that some other properties of $k(m)$ are also exhibited in $\alpha(m)$. Like $k(m)$, Vinson[21] shows we can express $\alpha(m)$ in terms of $\alpha(p_i^{e_i})$ where $m = \prod p_i^{e_i}$ is the prime factorization of m.

Theorem 3.30 *If m has the prime factorization $m = \prod p_i^{e_i}$ then $\alpha(m) = \text{lcm}[\alpha(p_i^{e_i})]$.*

Proof: Notice,

$$\begin{aligned} m|F_n &\iff p_i^{e_i}|F_n \text{ for all } i \\ &\iff \alpha(p_i^{e_i})|n \text{ for all } i. \end{aligned}$$

The smallest n which satisfies the last condition, and hence all of them, is $n = \text{lcm}[\alpha(p_i^{e_i})]$. Thus according to the first condition, F_n is the smallest Fibonacci number divisible by m. That is, $\alpha(m) = n = \text{lcm}[\alpha(p_i^{e_i})]$.

Again, like $k(m)$, we can express $\alpha(m)$ in a slightly more convenient form.

Theorem 3.31 $\alpha([m,n]) = [\alpha(m), \alpha(n)]$, *where brackets denote the least common multiple function.*

Proof:

$$\begin{aligned} F_t \equiv 0 \pmod{[m,n]} &\iff F_t \equiv 0 \pmod{m} \text{ and } F_t \equiv 0 \pmod{n} \\ &\iff \alpha(m)|t \text{ and } \alpha(n)|t \end{aligned}$$

The smallest t for which the first condition is true is $t = \alpha([m,n])$. the smallest t for which the last condition is true is $t = [\alpha(m), \alpha(n)]$. The theorem follows.

A third similarity exists: if p is an odd prime and t is the largest integer such that $\alpha(p^t) = \alpha(p)$ then $\alpha(p^e) = p^{e-t}\alpha(p)$. This result exists as a corollary to yet another surprising theorem from [15].

Theorem 3.32 *For p any odd prime, $\beta(p^e) = \beta(p)$.*

Proof: We again make use of the Fibonacci matrix, U. By equation (3.3) we know that

$$U^{\alpha(p^{e+1})} \equiv s(p^{e+1})I \pmod{p^{e+1}}.$$

Furthermore,

$$U^{\alpha(p^e)} \equiv s(p^e)I \pmod{p^e}$$

which implies

$$U^{p\alpha(p^e)} \equiv (s(p^e)I + p^eB)^p \equiv (s(p^e))^pI \pmod{p^{e+1}}.$$

Hence $\alpha(p^{e+1})|p\alpha(p^e)$. Since $\alpha(m)|\alpha(mn)$ we also know $\alpha(p^e)|\alpha(p^{e+1})$. Consequently, $\alpha(p^{e+1}) = \alpha(p^e)$ or $p\alpha(p^e)$. It follows that $\frac{\alpha(p^e)}{\alpha(p)} = p^i$ and similarly we can say $\frac{k(p^e)}{k(p)} = p^j$. Clearly,

$$\frac{k(p^e)}{\alpha(p)} \cdot \frac{\alpha(p^e)}{\alpha(p^e)} = \frac{k(p^e)}{\alpha(p)} \cdot \frac{k(p)}{k(p)}$$

and so

$$\frac{\alpha(p^e)}{\alpha(p)} \cdot \frac{k(p^e)}{\alpha(p^e)} = \frac{k(p)}{\alpha(p)} \cdot \frac{k(p^e)}{k(p)}.$$

Since $\frac{k(p^e)}{\alpha(p^e)} = \beta(p^e)$ and $\frac{k(p)}{\alpha(p)} = \beta(p)$,

$$p^i(1, 2, \text{ or } 4) = (1, 2, \text{ or } 4)p^j.$$

Since we assumed p to be odd, we must have $p^i = p^j$. That is, $\frac{\alpha(p^e)}{\alpha(p)} = \frac{k(p^e)}{k(p)}$ which implies $\frac{k(p)}{\alpha(p)} = \frac{k(p^e)}{\alpha(p^e)}$. In other words, $\beta(p) = \beta(p^e)$.

Corollary 3.33 *If p is an odd prime and t is the largest integer such that $\alpha(p^t) = \alpha(p)$ then $\alpha(p^e) = p^{e-t}\alpha(p)$. In fact, this t is also the largest integer such that $k(p^t) = k(p)$.*

Proof: This follows directly from the previous proof where $\frac{\alpha(p^e)}{\alpha(p)} = \frac{k(p^e)}{k(p)}$.

The case where $p = 2$ exists as a corollary to theorem 3.36.

We will now examine the function $\beta(m)$ more closely. The next three theorems present some useful relationships between $\beta(m)$, $\alpha(m)$, and $k(m)$.

Theorem 3.34 *For $m \geq 3$, $\beta(m) = 4$ if and only if $\alpha(m)$ is odd.*

Proof: Assume $\beta(m) = 4$. Then $(s(m))^2$ is the residue after the second zero and by equation (3.6) we know $(s(m))^2 \equiv (-1)^{\alpha(m)}$. Clearly, $(s(m))^2 \not\equiv 1$ and so $\alpha(m)$ must be odd.

Assume $\alpha(m)$ is odd. In this case, equation (3.6) tells us that $(s(m))^2 \equiv -1$. The only possible value for $\beta(m)$ now is 4.

In order to show some necessary and sufficient conditions for when $\beta(m) = 1$, we rely on the identity $F_{k(m)-j} \equiv F_{-j} = (-1)^{j+1}F_j \pmod{m}$.

Theorem 3.35 *$\beta(m) = 1$ if and only if $4 \not| \, k(m)$.*

Proof: We will prove the contrapositive of the theorem in both directions. First, assume that $4|k(m)$. Then if we let $j = \frac{k(m)}{2} + 1$ in the identity preceding the theorem, and make note that this j is odd, we get $F_{\frac{k(m)}{2}-1} \equiv F_{\frac{k(m)}{2}+1} \pmod{m}$. By the Fibonacci recurrence relation this implies $F_{\frac{k(m)}{2}} \equiv 0 \pmod{m}$, which in turn implies $\beta(m) \neq 1$.

If $\beta(m) \neq 1$ then $\beta(m) = 2$ or 4. We know that $k(m) = \alpha(m)\beta(m)$, so if $\beta(m) = 4$ then clearly $4|k(m)$. If $\beta(m) = 2$, then by the previous theorem $\alpha(m)$ is even, and once again $4|k(m)$.

Since theorems 3.34 and 3.35 are if and only if, the next theorem appears as a natural consequence.

Theorem 3.36 *$\beta(m) = 2$ if and only if $4|k(m)$ and $\alpha(m)$ is even.*

Corollary 3.37 *If $4|\alpha(m)$ then $\beta(m) = 2$.*

Corollary 3.38 *If $8|k(m)$ then $\beta(m) = 2$.*

Corollary 3.39 *$\beta(2) = \beta(4) = 1$. For $e \geq 3$, $\beta(2^e) = 2$.*

> **Proof:** By inspection, $\beta(2) = \beta(4) = 1$ and $\beta(8) = 2$. From theorem 3.5 we know that $k(2^e) = 3 \cdot 2^{e-1}$. Since $k(16) = 24$ we see $8|k(2^e)$ for $e \geq 4$, and we can apply the preceding corollary.

We must be careful when we try to apply theorem 3.36. We can *not* conclude that if $\beta(m) = 2$ then $4|\alpha(m)$. For example, $\beta(40) = 2$, yet $\alpha(40) = 30$. However, when the modulus is a prime or a power of a prime, theorem 3.36 can be strengthened. The following theorem found in [21] will be used later.

Theorem 3.40 *Let p be an odd prime. If $\beta(p^e) = 2$ then $4|\alpha(p^e)$.*

> **Proof:** First we show that the theorem is true for $e = 1$. When $\beta(p) = 2$, theorem 3.34 assures us that $\alpha(p)$ is even. In identity 3.26, let $n = 1$ and $r = -\frac{1}{2}\alpha(p)$ to attain
>
> $$F_{\frac{1}{2}\alpha(p)} \equiv F_{\alpha(p)+1}F_{-\frac{1}{2}\alpha(p)} \pmod{p}.$$
>
> Noting that $F_{\alpha(p)+1} = s(p)$ and that $s(p)^2 \equiv (-1)^{\alpha(p)} \pmod{p}$, we can multiply both sides of the above congruence by $F_{\alpha(p)+1}$ and apply identity 1.3 to achieve
>
> $$F_{\alpha(p)+1}F_{\frac{1}{2}\alpha(p)} \equiv (-1)^{\alpha(p)}(-1)^{\frac{1}{2}\alpha(p)+1}F_{\frac{1}{2}\alpha(p)} \pmod{p}.$$
>
> We recall that $\alpha(p)$ is even, then multiply both sides by $F_{\frac{1}{2}\alpha(p)}^{p-2}$ and apply Fermat's theorem to get
>
> $$F_{\alpha(p)+1} \equiv (-1)^{\frac{1}{2}\alpha(p)+1} \pmod{p}.$$

Since $\beta(p) = 2$ we know that $F_{\alpha(p)+1} \not\equiv 1$. Thus $(-1)^{\frac{1}{2}\alpha(p)+1} = -1$ which implies $4|\alpha(p)$ and we have proved the theorem for $e = 1$.

Since p is odd, $\beta(p^e) = 2$ implies that $\beta(p) = 2$. We have seen that this implies $4|\alpha(p)$, and so by theorem 3.24, $4|\alpha(p^e)$. Thus the theorem is proved.

So far we have been able to find $\beta(m)$ only by analyzing $k(m)$ or $\alpha(m)$. The next theorem gives us a method for finding $\beta([m, n])$ if we know $\beta(m)$ and $\beta(n)$. Vinson does not state this theorem explicitly, but the author was able to construct it from the information given by him.

Theorem 3.41 *Given $\beta(m)$ and $\beta(n)$, the table below determines the value of $\beta([m, n])$. Once again, brackets denote the least common multiple function.*

$\underline{\beta([m, n])}$

$\beta(n)$

		1	*2*	*4*
$\beta(m)$	*1*	*1*	*2*	*4 if* $m = 2$ *2 otherwise*
	2	*2*	*2*	*2*
	4	*4 if* $n = 2$ *2 otherwise*	*2*	*4*

Proof: Let

$$\begin{array}{lll} \alpha(m) = 2^r a & \beta(m) = 2^s & k(m)2^t a \\ \alpha(n) = 2^w b & \beta(n) = 2^x & k(n)2^y b \end{array}$$

where a, b are odd integers. Hence

$$[k(m), k(n)] = 2^{\max(t,y)} \cdot [a, b]$$

$$\text{and} \quad [\alpha(m), \alpha(n)] = 2^{\max(r,w)} \cdot [a, b].$$

Then

$$\beta([m, n]) = \frac{k([m, n])}{\alpha([m, n])} = \frac{[k(m), k(n)]}{[\alpha(m), \alpha(n)]} = 2^{\max(t,y)-\max(r,w)}.$$

Notice that $r + s = t$ and $w + x = y$. We now address four cases.

Case 1: To describe the diagonal of the table, suppose $\beta(m) = \beta(n)$, that is, $s = x$. Then $\max(t, y) - \max(r, w) = \max(r + s, w + x) - \max(r, w) = s = x$. Hence $\beta([m, n]) = 2^s = 2^x = \beta(m) = \beta(n)$.

In order to prove the remaining three cases it is helpful to translate theorems 3.35, 3.36, and 3.34 into statements about r, s, and t:

If $s = 0$ then $t = 0$ (for $m = 2$) or $t = 1$ (for $m > 2$).
Respectively, $r = 0$ or $r = 1$.
If $s = 1$ then $t \geq 2$ and $r \geq 1$.
If $s = 2$ then $r = 0$ and hence, $t = 2$.

Analogous statements hold for w, x, and y.

Case 2: Suppose $\beta(m) = 4$ and $\beta(n) = 1$, that is, $s = 2$ and $x = 0$. Since $s = 2$ we know that $r = 0$ and $t = 2$. Also, since $x = 0$ we know that either $w = 0$ or $w = 1$.

Case 2a. Say $x = 0$, $w = 0$, and so $y = 0$. Then $\max(t, y) - \max(r, w) = 2 - 0 = 2$. Hence $\beta([m, n]) = 2^2 = 4$.

Case 2b. Say $x = 0$, $w = 1$, and so $y = 1$. Then $\max(t, y) - \max(r, w) = 2 - 1 = 1$. Hence $\beta([m, n]) = 2^1 = 2$.

Case 3: Suppose $\beta(m) = 2$ and $\beta(n) = 1$, that is, $s = 1$ and $x = 0$. Since $s = 1$ we know that $t \geq 2$ and $r \geq 1$. Again, since $x = 0$ either $w = 0$ or $w = 1$.

Case 3a. Say $x = 0$, $w = 0$, and so $y = 0$. Then $\max(t, y) - \max(r, w) = t - r = s = 1$. Hence $\beta([m, n]) = 2^1 = 2$.

Case 3b. Say $x = 0$, $w = 1$, and so $y = 1$. Then $\max(t, y) - \max(r, w) = t - r = s = 1$. Hence $\beta([m, n]) = 2^1 = 2$.

Case 4: Suppose $\beta(m) = 4$ and $\beta(n) = 2$, that is, $s = 2$ and $x = 1$. Then $r = 0$, $t = 2$, and $w \geq 1$, $y \geq 2$. Then $\max(t, y) - \max(r, w) = y - w = x = 1$. Hence $\beta([m, n]) = 2^1 = 2$.

This completes the proof.

There are two interesting corollaries that follow.

Corollary 3.42 *If* $3|m$ *then* $\beta(m) = 2$.

Proof: Since $\beta(3) = 2$ we know that $\beta(3^e) = 2$. Let m be expressed as $3^e n$ where $3 \not| n$. By the previous theorem, then $\beta(m) = \beta([3^e, n]) = 2$.

Corollary 3.43 $\beta(m) = 1$ *if and only if* $8 \not| m$ *and* $\alpha(p) \equiv 2 \pmod 4$ *for all odd primes* p *that divide* m.

Proof: Let m have the prime factorization $m = \prod p_i^{e_i}$. Suppose $\beta(m) = 1$. By theorem 3.41 it is easy to see that we must have $\beta(p_i^{e_i}) = 1$ for all i. If p_1 is the smallest prime in the prime factorization of m and $p_1 = 2$ then by corollary 3.39, $e_1 \leq 2$ and thus $8 \not| m$. Recall that for odd p, $\beta(p_i^{e_i}) = \beta(p_i)$. Theorem 3.36 tells us that if $\alpha(p_i) \equiv 1$ or $3 \pmod 4$ then $\beta(p_i) = 4$. Theorem 3.34 tells us that if $\alpha(p_i) \equiv 0 \pmod 4$ then $\beta(p_i) = 4$. Hence when $\beta(m) = 1$ we must have $\alpha(p_i) \equiv 2 \pmod 4$ for all i.

Suppose that $8 \not| m$. Thus if 2^e is a factor of m, then $e \leq 2$ and $\beta(2^e) = 1$. For odd p, if $\alpha(p) \equiv 2 \pmod 4$ then $\beta(p) = 1$ by theorems 3.35 and 3.40. Hence if we suppose that $\alpha(p_i^{e_i}) \equiv 2 \pmod 4$ for all i we have $\beta(p_i^{e_i}) = 1$ for all i and then theorem 3.41 indicates that $\beta(m) = 1$.

We now know that for composite m, $\beta(m)$ can be determined by factoring m into smaller moduli. We also know that for odd primes p, $\beta(p^e) = \beta(p)$. Can we determine $\beta(p)$ for odd primes p? While $k(p)$ and $\alpha(p)$ have strongly resisted this analysis, we can make some progress on $\beta(p)$. The four results are grouped together in the following theorem found in [21].

Theorem 3.44 *For odd primes p,*

(i) *If* $p \equiv 11$ *or* $19 \pmod{20}$ *then* $\beta(p^e) = 1$.

(ii) *If* $p \equiv 3$ *or* $7 \pmod{20}$ *then* $\beta(p^e) = 2$.

(iii) *If* $p \equiv 13$ *or* $17 \pmod{20}$ *then* $\beta(p^e) = 4$.

(iv) *If* $p \equiv 21$ *or* $29 \pmod{40}$ *then* $\beta(p^e) \neq 2$.

Proof: Since we are assuming p odd, we need only prove each part for $e = 1$ and the conclusion will follow. Before looking at the individual cases we take some time to develop a couple useful facts. First, since $\beta(p)$ is the order of $s(p)$, we know that $(s(p))^{\beta(p)} \equiv 1 \pmod{p}$. In addition, we know by Fermat's theorem that $(s(p))^{p-1} \equiv 1 \pmod{p}$. Thus $\beta(p)|p-1$ and it follows that if $p \equiv 3 \pmod{4}$ then $\beta(p) \neq 4$.

Secondly, if $p = 5t \pm 2$ then $F_p \equiv -1$ and $F_{p+1} \equiv 0 \pmod{p}$. We see that $\alpha(p)|p+1$ but $k(p)\not|p+1$. Hence $\alpha(p) \neq k(p)$ and consequently $\beta(p) \neq 1$. Now we turn our attention to the four results.

(i) Here $p \equiv 3 \pmod{4}$, so $\beta(p) \neq 4$. Assume $\beta(p) = 2$. Then by theorem 3.36, $4|k(p)$. Since $p = 5t \pm 1$ we have $k(p)|p-1$, and so $4|p-1$. However, this is a contradiction since $p - 1 \equiv 10$ or $18 \pmod{20}$. Thus $\beta(p) = 1$.

(ii) Again, $p \equiv 3 \pmod{4}$, so $\beta(p) \neq 4$. Now $p = 5t \pm 2$ and we have seen that this implies $\beta(p) \neq 1$. Thus $\beta(p) = 2$.

(iii) As in the previous part, $p = 5t \pm 2$ and so $\beta(p) \neq 1$. Also, we know $\alpha(p)|p+1$. In this case $p \equiv 1 \pmod{4}$ so $4 \not| p+1$. Hence $4 \not| \alpha(p)$. Applying theorem 3.40 we have $\beta(p) \neq 2$. Hence $\beta(p) = 4$.

(iv) Suppose $\beta(p) = 2$. By theorem 3.40, $4|\alpha(p)$ and so consequently $8|k(p)$. Furthermore, since $p = 5t \pm 1$, theorem 3.12 assures us that $k(p)|p-1$. It follows that $8|p-1$. However, $p - 1 \equiv 20$ or $28 \pmod{40}$ so clearly $8 \not| p-1$. Thus we have our contradiction and we can say $\beta(p) \neq 2$.

We would like to know if anything can be said about the primes not covered by the theorem, namely $p \equiv 1$ or $9 \pmod{40}$. Also, can we be more exact about primes where $p \equiv 21$ or $29 \pmod{40}$? Vinson provides the following examples to show that his theorem is "complete":

For $p \equiv 1 \pmod{40}$:	$\beta(521) = 1$,	$\beta(41) = 2$,	$\beta(761) = 4$
For $p \equiv 9 \pmod{40}$:	$\beta(809) = 1$,	$\beta(409) = 2$,	$\beta(89) = 4$
For $p \equiv 21 \pmod{40}$:	$\beta(101) = 1$,	$\beta(61) = 4$	
For $p \equiv 29 \pmod{40}$:	$\beta(29) = 1$,	$\beta(109) = 4$	

We finish section 3.3 with a couple of theorems promised at the end of section 3.1. While they speak to the character of the period, their proofs are made easy by the theory developed in this section.

Theorem 3.45 *(i) If $n \geq 5$ is odd then $k(F_n) = 4n$.*

(ii) If $n \geq 4$ is even then $k(F_n) = 2n$.

Proof: We first note that if F_n is used for the modulus, then naturally $\alpha(F_n) = n$.

(i) This result follows from the fact that for $m \geq 3$, $\alpha(m)$ odd implies $\beta(m) = 4$. For $n \geq 5$ and odd, $F_n \geq 3$ and $\alpha(F_n) = n$ is odd. Thus $k(F_n) = 4n$.

(ii) Here, $\alpha(F_n) = n$ is even so $\beta(F_n) = 1$ or 2. If $\beta(F_n) = 1$ then $F_{n-1} \equiv F_{n+1} \equiv 1 \pmod{F_n}$. However, $F_1, F_2, F_3, \ldots, F_{n-1}$ is non decreasing and $F_3 \equiv 2 \pmod{F_n}$, hence our contradiction. Therefore, $\beta(F_n) = 2$ and $k(F_n) = 2n$.

Theorem 3.46 *(i) If $n \geq 3$ is odd then $k(L_n) = 2n$.*

(ii) If $n \geq 2$ is even then $k(L_n) = 4n$.

Proof: First we establish that $\alpha(L_n) = 2n$. From identity 1.10, $F_n L_n = F_{2n}$ which implies $F_{2n} \equiv 0 \pmod{L_n}$ so certainly $\alpha(L_n)|2n$. Now if $\alpha(L_n) \neq 2n$ then $\alpha(L_n) \leq n$. In other words, $L_n|F_t$ for some $t \leq n$. However, $L_n > F_t$ for $2 \leq t \leq n$, so clearly $L_n \not| F_t$. Hence $\alpha(L_n) = 2n$.

(i)

$$\begin{aligned}
F_{n+1}L_n &= F_{n+1}(F_{n+1} + F_{n-1}) \\
&= F_{n+1}^2 + F_{n+1}F_{n-1} \\
&= F_{n+1}^2 + F_n^2 + (-1)^n \text{ (by identity 1.8)} \\
&= F_{2n+1} - 1 \text{ (by identity 1.7 and } n \text{ odd)}
\end{aligned}$$

Thus $F_{2n+1} \equiv 1 \pmod{L_n}$ and we can say $\beta(L_n) = 1$. Therefore $k(L_n) = \alpha(L_n) = 2n$.

(ii) When n is even, $4|\alpha(L_n)$ and so by corollary 3.37, $\beta(L_n) = 2$. Hence $k(L_n) = \alpha(L_n) \cdot 2 = 4n$.

Chapter 4

Personal Findings

During my survey of known Fibonacci properties I was fortunate enough to stumble across a few areas where apparently very little research had been done. Upon examining these areas more closely I was able to discover yet more astounding properties of the Fibonacci sequence.

4.1 Spirolaterals And The Fibonacci Sequence

Spirolaterals, invented in 1973 by Frank C. Odds, are simple graphical representations of finite integer sequences. The rules for creating a spirolateral from a given sequence are simple, and the spirolateral can easily be drawn on a sheet of ordinary graph paper. Suppose we have a sequence $x_1, x_2, x_3, \ldots, x_n$. To create the spirolateral draw a line from left to right x_1 units long, turn right 90°, draw a line x_2 units long, turn right 90° and continue in this manner. When the end of the sequence has been reached, start over again with x_1.

Figure 4.1: Some simple spirolaterals. The circle indicates the starting point.

Eventually, either the line will return to its starting point heading in the initial direction, or else the pattern will wander off the page. It is known that when $n \equiv 1$ or 3 (mod 4) then the spirolateral exhibits 4-fold symmetry. When $n \equiv 2 \pmod 4$ then then spirolateral exhibits 2-fold symmetry, and when $n \equiv 0 \pmod 4$ the spirolateral does not exhibit symmetry and usually glides off the page in some diagonal direction.

I wrote a short computer program that randomly generated sequences and then drew them as spirolaterals. After playing with the spirolateral program for a while, viewing hundreds of spirolaterals, I was accustomed to seeing interesting symmetries and curious patterns fly off the screen at some diagonal. Then, when I used a period of residues of the Fibonacci sequence under various moduli to generate spirolaterals I was surprised that typically the results were not symmetric and often did not translate off the screen.

Figure 4.2: Some spirolaterals using Fibonacci residues. Here, $F(\text{mod } 5)$ and $F(\text{mod } 8)$ are both asymmetric and nontranslating. Circles indicate starting points.

Apparently, after only one time through the period, the line had returned to the starting point and was heading in the initial direction. That is, the sum of the lines drawn to the right equaled the sum of the lines drawn to the left, and the sum of the lines drawn up equaled the sum of the lines drawn down. This seemed a fairly remarkable occurrence, for it indicated a truth about the alternating sum of the residues themselves. After studying many examples, a conjecture was made and eventually a proof was given showing when the alternating sum will be zero.

In order to express clearly the idea of working with the residues themselves, let us introduce some notation. Let f_n represent the least nonnegative residue of F_n modulo m. As we would expect, $f_n = f_{n+r\cdot k(m)}$ for any integer r. When n is odd, $F_{-n} = F_n$ and so $f_{-n} = f_n$. When n is even, $F_{-n} = -F_n$ which implies $F_{-n} + F_n \equiv 0 \pmod{m}$ and so either $f_{-n} = f_n = 0$ or else $f_{-n} + f_n = m$

Theorem 4.1 $4|k(m)$ *if and only if*

$$\sum_{i=0}^{\frac{k(m)}{2}-1} (-1)^i f_{2i+1} = 0.$$

Proof: Let $k = k(m)$ and rewrite the above summation as

$$\begin{aligned} & f_1 - f_3 + f_5 - \cdots - f_{k-5} + f_{k-3} - f_{k-1} \\ = \quad & (f_1 - f_{k-1}) - (f_3 - f_{k-3}) + \cdots - (f_{\frac{k}{2}-1} - f_{\frac{k}{2}+1}). \end{aligned}$$

First suppose that $4|k$. When n is odd $f_n = f_{-n} = f_{k-n}$. Hence each term in parentheses equals zero, implying the entire summation equals zero.

On the other hand, since $f_n = f_{k-n}$ for odd n we know that each parenthesized term must equal zero, and in particular $f_{\frac{k}{2}-1} = f_{\frac{k}{2}+1}$. By the recurrence relation we know then $f_{\frac{k}{2}} = 0$. Clearly now $\beta(m) \neq 1$ and by theorem 3.35 we can say $4|k$.

It turns out that the same conditions do not ensure that the alternating sum of the evenly subscripted residues will be zero. However, the conditions needed in this case are not very different. First, though, we need a lemma.

Lemma 4.2 *Suppose $4|k(m)$ for some m and let j be even. If j is a multiple of $\frac{k(m)}{2}$ then $f_j = f_{k-j} = 0$ otherwise $f_j + f_{k-j} = m$.*

Proof: Let $k = k(m)$ and take all congruences (mod m). When j is even $F_{k-j} \equiv (-1)^{j+1}F_j \equiv -F_j$. Thus if $F_j \not\equiv 0$ then $f_j + f_{k-j} = m$. Since $4|k$ we know by theorem 3.35 that $F_{\frac{k}{2}} \equiv 0$ and consequently if j is a multiple of $\frac{k}{2}$ then $f_j = 0$. Also, $k - j$ will be a multiple of $\frac{k}{2}$ so $f_{k-j} = 0$. Suppose $F_t \equiv 0$ for some $0 < t < \frac{k}{2}$. Then $\beta(m) = 4$ and $\alpha(m) = t$ is necessarily odd. Thus the only time $F_j \equiv 0$ and j is even is when j is a multiple of $\frac{k}{2}$. The lemma follows.

Theorem 4.3 *If $k(m) \equiv 4 \pmod 8$ then*

$$\sum_{i=0}^{\frac{k(m)}{2}-1} (-1)^i f_{2i} = 0.$$

Proof: The summation above is

$$\begin{aligned} & f_0 - f_2 + f_4 - f_6 + \cdots + f_{k-4} - f_{k-2} \\ = \quad & f_0 - (f_2 + f_{k-2}) + (f_4 + f_{k-4}) - \cdots - (f_{\frac{k}{2}-2} + f_{\frac{k}{2}+2}) + f_{\frac{k}{2}}. \end{aligned}$$

By our lemma $f_0 = f_{\frac{k}{2}} = 0$ and each quantity in parentheses equals m. There are $\frac{1}{2}(\frac{k}{2} - 2) = \frac{k}{4} - 1$ parenthesized terms and since $k \equiv 4 \pmod 8$ we know $\frac{k}{4} - 1$ is even. Hence the entire summation is zero.

We can extend our idea of the spirolateral and instead of restricting ourselves to just 90° turns we can make spirolaterals with 60° turns or 45° etc... If 60° turns are used, hexagonal type patterns emerge. Occasionally these pattern will return to their starting place when $F(\text{mod } m)$ for some m is used as the generating sequence. Since every third line is parallel in these pictures, this result indicates that the alternating sum of every third term in these sequences is zero, regardless of where we start to take our sum. The following conjecture expresses this notion.

Conjecture 4.4 *If* $k(m) \equiv 12 \pmod{24}$ *and* $\beta(m) = 4$ *for some* m*, then*

$$\sum_{i=0}^{k(m)/3-1} (-1)^i f_{3i+j} = 0$$

for $j = 0, 1, 2$.

After only a cursory investigation it appears that this conjecture may yield to a proof if given a couple hours of thought. Also, many times the alternating sum of every fourth, fifth, and so on, residue in a period equals zero. This area seems to be quite open for research.

After trying for a while to find results pertaining to the summation of the residues themselves I turned to a related question. If I take the sum (or alternating sum) of every n^{th} term of the Fibonacci sequence within a period of $F(\text{mod } m)$, what will the result be, modulo m? For example, $k(5) = 20$, so what is the sum modulo 5 of every fourth term starting with, say, F_2? Or what can I expect of $F_3 - F_8 + F_{13} - F_{18} \pmod 5$? To this end the following two identities are vital. The following identity is due to Siler[16].

Identity 4.5 *For* $0 \le j < n$ *and* $t \ge 0$*, we have*

$$\sum_{i=0}^{t} F_{ni+j} = \frac{F_{nt+n+j} - F_j + (-1)^{j+1}F_{n-j} + (-1)^{n+1}F_{nt+j}}{L_n - 1 + (-1)^{n+1}}.$$

Proof: The identity $\sigma\tau = -1$ will be used several times in the proof.

$$\sum_{i=0}^{t} F_{ni+j} = \sum_{i=0}^{t} \frac{1}{\sqrt{5}}(\tau^{ni+j} - \sigma^{ni+j})$$

$$= \frac{1}{\sqrt{5}}\left[\tau^j\sum_{i=0}^{t}(\tau^n)^i - \sigma^j\sum_{i=0}^{t}(\sigma^n)^i\right]$$

$$= \frac{1}{\sqrt{5}}\left[\frac{\tau^j(1-(\tau^n)^{t+1})}{1-\tau^n} - \frac{\sigma^j(1-(\sigma^n)^{t+1})}{1-\sigma^n}\right]$$

$$= \frac{1}{\sqrt{5}}\left[\frac{\tau^j(1-\sigma^n) - \tau^{nt+n+j}(1-\sigma^n) - \sigma^j(1-\tau^n) + \sigma^{nt+n+j}(1-\tau^n)}{(1-\tau^n)(1-\sigma^n)}\right]$$

$$= \frac{1}{\sqrt{5}}\left[\frac{(\tau^j-\sigma^j) + (-1)^j(\tau^{n-j}-\sigma^{n-j}) - (\tau^{nt+n+j}-\sigma^{nt+n+j}) + (-1)^n(\tau^{nt+j}-\sigma^{nt+j})}{1+(\tau\sigma)^n - (\tau^n+\sigma^n)}\right]$$

$$= \frac{F_j + (-1)^j F_{n-j} - F_{nt+n+j} + (-1)^n F_{nt+j}}{1+(-1)^n - L_n}.$$

By multiplying the numerator and denominator by -1 we obtain the identity.

The second identity is similar, but concerns alternating sums. I have been unable to find this identity published anywhere, and the proof below is due to Fredric Howard.

Identity 4.6 *For* $0 \le j < n$ *and* $t \ge 0$*, we have*

$$\sum_{i=0}^{t}(-1)^i F_{ni+j} = \frac{F_j + (-1)^{j+1}F_{n-j} + (-1)^t F_{nt+n+j} + (-1)^{t+n}F_{nt+j}}{1+(-1)^n + L_n}.$$

Proof:

$$\sum_{i=0}^{t}(-1)^i F_{ni+j} = \sum_{i=0}^{t}\frac{(-1)^i}{\sqrt{5}}(\tau^{ni+j}-\sigma^{ni+j})$$

$$= \frac{1}{\sqrt{5}}\left[\tau^j\sum_{i=0}^{t}(-\tau^n)^i - \sigma^j\sum_{i=0}^{t}(-\sigma^n)^i\right]$$

$$= \frac{1}{\sqrt{5}}\left[\frac{\tau^j(1-(-\tau^n)^{t+1})}{1-(-\tau^n)} - \frac{\sigma^j(1-(-\sigma^n)^{t+1})}{1-(-\sigma^n)}\right]$$

$$= \frac{1}{\sqrt{5}}\left[\frac{\tau^j(1+\sigma^n) + (-1)^t\tau^{nt+n+j}(1+\sigma^n) - \sigma^j(1+\tau^n) - (-1)^t\sigma^{nt+n+j}(1+\tau^n)}{(1+\tau^n)(1+\sigma^n)}\right]$$

$$\begin{aligned}
&= \frac{1}{\sqrt{5}}\left[\frac{\begin{array}{r}(\tau^j-\sigma^j)+(-1)^{j+1}(\tau^{n-j}-\sigma^{n-j})+\\(-1)^t(\tau^{nt+n+j}-\sigma^{nt+n+j})+(-1)^{t+n}(\tau^{nt+j}-\sigma^{nt+j})\end{array}}{1+(\tau\sigma)^n+(\tau^n+\sigma^n)}\right]\\
&= \frac{F_j+(-1)^{j+1}F_{n-j}+(-1)^tF_{nt+n+j}+(-1)^{t+n}F_{nt+j}}{1+(-1)^n+L_n}.
\end{aligned}$$

If we fix n and j and sum up (using either identity) all terms of the form F_{ni+j} within a single period of the Fibonacci sequence ($F_0 \leq F_{ni+j} < F_{k(m)}$) what will the result be? In particular, for what values of n, j, and m will the sum be congruent to zero modulo m?

We will only consider those n such that $n|k(m)$. We are not especially interested in looking at, say, every seventh term if the period is not a multiple of seven. When $t = \frac{k(m)}{n} - 1$ let $\overset{+}{S_n}$ denote the summation of identity 4.5 and let $\overset{+/-}{S_n}$ denote the alternating summation of identity 4.6.

Hence, letting $k = k(m)$,

$$\overset{+}{S_n} = \sum_{i=0}^{\frac{k}{n}-1} F_{ni+j} = \frac{F_{k+j} - F_j + (-1)^{j+1}F_{n-j} + (-1)^{n+1}F_{k-n+j}}{L_n - 1 + (-1)^{n+1}}.$$

Since $F_j \equiv F_{k+j} \pmod{m}$,

$$\begin{aligned}
\overset{+}{S_n}(L_n - 1 + (-1)^{n+1}) &\equiv (-1)^{j+1}F_{n-j} + (-1)^{n+1}F_{k-(n-j)}\\
&\equiv (-1)^{j+1}F_{n-j} + (-1)^{n+1+(n-j)+1}F_{n-j}\\
&\equiv 0 \pmod{m}.
\end{aligned}$$

Quite surprisingly, j has dropped out of our equation and the following is then true for all j:

Theorem 4.7 *If* $\gcd(m, L_n - 1 + (-1)^{n+1}) = 1$ *then* $\overset{+}{S_n} \equiv 0 \pmod{m}$.

We will now look at some examples to demonstrate the surprising results this theorem gives us.

When $n = 1$, $L_n - 1 + (-1)^{n+1} = 1$, and so for any modulus m, $\overset{+}{S_1} \equiv 0 \pmod{m}$. In other words, $F_0 + F_1 + F_2 + \cdots + F_{k(m)-1} \equiv 0 \pmod{m}$ for all m.

When $n = 2$, $L_n - 1 + (-1)^{n+1} = 1$, and so for any modulus m, $\overset{+}{S_2} \equiv 0 \pmod{m}$.

Consider $n = 4$. Here $L_n - 1 + (-1)^{n+1} = 5$. Thus if $4|k(m)$ but $5 \not| \, m$ then $\overset{+}{S_4} \equiv 0 \pmod{m}$. Recall that this means $\sum_{i=0}^{k/4-1} F_{4i} \equiv \sum_{i=0}^{k/4-1} F_{4i+1} \equiv \sum_{i=0}^{k/4-1} F_{4i+2} \equiv$

$\sum_{i=0}^{k/4-1} F_{4i+3} \equiv 0 \pmod{m}$. Again, it does seem remarkable that the point where we start to take every fourth term does not matter at all. Finding some values for m which satisfy the above conditions is easy to do. By inspection we look for an m such that $4|k(m)$ then using the fact that $k(m)|k(mr)$ we let r be any integer except multiples of 5. We see $k(3) = 8$ so some viable choices for m are 3, 6, 9, 12, 18, 21, 24, 27, 33, ... Notice the omission of 15 and 30. Of course, these aren't the only possible values for m. We find $k(7) = 16$, so 7, 14, 21, 28, 42, ... are all valid choices as well. Amazingly, for all these values of m (and many more), $S_4^{+} \equiv 0 \pmod{m}$.

Next we fix $m = 17$ and find all n such that $S_n^{+} \equiv 0 \pmod{17}$. Now $k(17) = 36$ so we will only consider those n which divide 36. It just happens that $\gcd(17, L_n - 1 + (-1)^{n+1}) = 1$ for all those n and so $S_n^{+} \equiv 0 \pmod{17}$ for $n = 1$, 2, 3, 4, 6, 9, 12, and 18. Truly amazing!

When $m = 9$, $k(m) = 24$. We find that $\gcd(9, L_n - 1 + (-1)^{n+1}) = 1$ for all divisors, n, of 24 except $n = 8$. Hence $S_n^{+} \equiv 0 \pmod{9}$ for $n = 1$, 2, 3, 4, 6, and 12.

It should be noted that we need not always use the first $k(m)$ terms of the Fibonacci sequence in our summations. This comes from the fact that we are summing over a single period of the Fibonacci sequence and the value of j in identities 4.5 and 4.6 is inconsequential. Considering the last example, we can take *any* 24 consecutive Fibonacci numbers, then add up, say, every third, and our total will continue to be a multiple of 9.

Now we turn our attention to the alternating sum, $S_n^{+/-}$. Again we want $\frac{k(m)}{n}$ to be an integer, but two cases arise: $\frac{k(m)}{n}$ is either even or odd. The case where $\frac{k(m)}{n}$ is even is explored here. In this case the number of positive terms in the summation is the same as the number of negative terms. The case where $\frac{k(m)}{n}$ is odd does not appear to give nice results (probably because it lacks the "symmetry" of the first case) and has not been explored a great deal.

As before, we will now try to find out when $S_n^{+/-} \equiv 0 \pmod{m}$. Let $k = k(m)$. By identity 4.6:

$$S_n^{+/-} = \sum_{i=0}^{\frac{k}{n}-1} (-1)^i F_{ni+j} = \frac{F_j + (-1)^{j+1}F_{n-j} + (-1)^{\frac{k}{n}-1}F_{k+j} + (-1)^{\frac{k}{n}-1+n}F_{k-n+j}}{L_n + 1 + (-1)^n}.$$

Assuming $\frac{k}{n}$ is even, and noting $F_j \equiv F_{k+j} \pmod{m}$,

$$S_n^{+/-}(L_n + 1 + (-1)^n) \equiv (-1)^{j+1}F_{n-j} + (-1)^{\frac{k}{n}-1+n}(-1)^{n-j+1}F_{n-j}$$

$$\begin{aligned} &\equiv (-1)^{j+1}F_{n-j} + (-1)^j F_{n-j} \\ &\equiv 0 \pmod{m} \end{aligned}$$

Once again j has dropped out and we are left with the following result.

Theorem 4.8 *If* $\frac{k(m)}{n}$ *is even and* $\gcd(m, L_n + 1 + (-1)^n) = 1$ *then* $S_n^{+/-} \equiv 0 \pmod{m}$.

Here are a couple examples of the application of this theorem.

Let $n = 4$. Then $L_n + 1 + (-1)^n = 9$. Now we want the values for m such that $\frac{k(m)}{4}$ is even and $\gcd(m, 9) = 1$, the latter requirement being the same as $3 \not| m$. After some inspection we find $m = 7$ works since $k(m) = 16$. Thus $m = 7$, 14, 28, 35, 49, ... are all acceptable values. Also, $k(16) = 24$ so $m = 16$, 32, 64, 80, 112, ... work as well. For all these values of m, $S_4^{+/-} \equiv 0 \pmod{m}$.

When $m = 9$, $k(m) = 24$. We see that $\frac{k(m)}{n}$ is even for $n = 1$, 2, 3, 4, 6, 12. Of these values, $\gcd(9, L_n + 1 + (-1)^n) = 1$ for $n = 1$, 2, 3, 6. Hence $S_1^{+/-} \equiv S_2^{+/-} \equiv S_3^{+/-} \equiv S_6^{+/-} \equiv 0 \pmod{9}$.

When $m = 17$, $k(m) = 36$. Now $\frac{k(m)}{n}$ is even for $n = 1$, 2, 3, 6, 9, 18. Of these values, $\gcd(17, L_n + 1 + (-1)^n) = 1$ for $n = 1$, 2, 3, 6, 9. Hence $S_1^{+/-} \equiv S_2^{+/-} \equiv S_3^{+/-} \equiv S_6^{+/-} \equiv S_9^{+/-} \equiv 0 \pmod{17}$.

It is remarkable that in the example above where $m = 9$, the alternating sum of the residues themselves for $n = 1$, 2, 3, and 6 *actually equals* zero when $j \neq 0$. When $j = 0$, the alternating sum of the residues equals -9 for all four values of n.

Similarly, in the example when $m = 17$, the alternating sum of the residues themselves *actually equals* zero for all j. Clearly this is an area that is wide open for research and appears to have some fascinating results.

Though we have provided some sufficient conditions indicating when a sum will be congruent to zero, these conditions are nowhere close to necessary. There are many times when a sum will be congruent to zero for some j but not all. It appears that with some work, new and more general sufficient conditions may be found.

The notion of summing Fibonacci numbers over a single period is not new and has been examined previously by Aydin and Smith in [3]. Their approach, however, was to take the sum of powers of all the Fibonacci numbers in a period of $F(\text{mod } p)$ and observe its value

For all primes p	$\sum F_i \equiv 0$	$\sum(-1)^i F_i \equiv 0$
	$\sum F_i^2 \equiv 0$	
	$\sum F_i^3 \equiv 0$	$\sum(-1)^i F_i^3 \equiv 0$
For $p \neq 3$		$\sum(-1)^i F_i^4 \equiv 0$
For $p \neq 11$	$\sum F_i^5 \equiv 0$	$\sum(-1)^i F_i^5 \equiv 0$
For $p \neq 11, 29$	$\sum F_i^6 \equiv 0$	
	$\sum F_i^7 \equiv 0$	$\sum(-1)^i F_i^7 \equiv 0$

Table 4.1: Some sums of powers of Fibonacci numbers.

modulo p, where p is a prime. Table 4.1 displays a few of their results. All sums are taken over a single period and all congruences are $\pmod{p}$.

It seems that the next step is to look at summations of the form $\sum F_{ni+j}^e$ and $\sum(-1)^i F_{ni+j}^e$. While no known work has been done in this area, empirical evidence suggests that there are many interesting theorems waiting to be proven.

4.2 Fibonacci Subsequences

During my research I came across a paper [8] by Herta Freitag in which she describes a property of the unit digits of the Fibonacci numbers. In the paper she examines several subsequences of $F \pmod{10}$ where the terms of the subsequence actually follow the usual Fibonacci recurrence relation. First she conjectures and proves that $F_n + F_{n+5} \equiv F_{n+10} \pmod{10}$ for all n, then she shows that if $j \in \{1, 5, 13, 17, 25, 29, 37, 41, 49, 53\}$ the relation $F_n + F_{n+j} \equiv F_{n+2j} \pmod{10}$ still holds for all n.

Her paper leaves many questions open. Are there other subsequences of this type in $F \pmod{10}$ which *do* depend on the value of n as defined above? What can we say about the subsequences of $F \pmod{m}$ for arbitrary m? We can immediately answer the first question by noting that $F_0, F_9, F_{18}, \ldots \pmod{10}$ forms such a sequence, but $F_1, F_{10}, F_{19}, \ldots \pmod{10}$ does not. We will examine the second question closely.

First we need some notation. If a subsequence H of $F \pmod{m}$ exhibits the recurrence relation $H_{n+2} \equiv H_{n+1} + H_n \pmod{m}$, let us call H a "Fibonacci subsequence modulo m". We will drop the "modulo m" when the modulus is understood. We will only consider subsequences whose terms are evenly spaced throughout $F(\text{mod } m)$ and we will denote such subsequence by $\{F_n, F_{n+j}\}$ where F_n and F_{n+j} are successive term of the subsequence. We will often use the variables n and j like this where F_n is a term in the subsequence and j is the "spread" of the subsequence. Since $F(\text{mod } m)$ has period $k(m)$, we will always assume $0 \leq n < k(m)$ and $1 \leq j \leq k(m)$.

Let us examine some properties of these Fibonacci subsequences. Let $d =$ $\gcd(j, k(m))$. If $\{F_n, F_{n+j}\}$ is a Fibonacci subsequence then $\{F_{n+dx}, F_{n+dx+j}\}$ is also a Fibonacci subsequence for all x. To see this, consider a period of $F(\text{mod } m)$ where we start at F_n then take every j^{th} term. When we reach the end of the period, we "loop" back to the start and continue. After "wrapping" around once or several times we will eventually return to F_n. In the process, we will have taken every d^{th} number in the period. Thus not only is $\{F_{n+dx}, F_{n+dx+j}\}$ a Fibonacci subsequence, in a sense it is the same subsequence with a different starting point. We say that it is a "rotation" of the subsequence $\{F_n, F_{n+j}\}$.

In particular, notice that if $\{F_n, F_{n+j}\}$ is a Fibonacci subsequence and $\gcd(j, k(m)) = 1$, then $\{F_t, F_{t+j}\}$ is a rotation of $\{F_n, F_{n+j}\}$ for any t, and the subsequence has $k(m)$ terms.

So how do we find these Fibonacci subsequences? Given only a few successive terms of $\{F_n, F_{n+j}\}$, can we say whether or not it is a Fibonacci subsequence, without having to compute the entire subsequence? As a matter of fact, the main result of this section proves that in many cases we can do just that. Before we present the main result we provide the following two lemmas.

Lemma 4.9 $\{F_0, F_j\}$ *is a Fibonacci subsequence if and only if* $\{F_n, F_{n+j}\}$ *is a Fibonacci subsequence with* $F_n \equiv 0$.

> **Proof:** The ideas in this proof are similar to those in the proof of theorem 3.25. Let s be the residue of $F_{n+1} \pmod{m}$. The pair $(F_n, F_{n+1}) \equiv s(F_0, F_1) \pmod{m}$, hence the sequence $F_n, F_{n+1}, F_{n+2}, \ldots \pmod{m}$ is the same as the sequence $sF_0, sF_1, sF_2, \ldots \pmod{m}$. Certainly, if $\{F_0, F_j\}$ is a Fibonacci subsequence then $\{sF_0, sF_j\}$ is a Fibonacci subsequence, and hence $\{F_n, F_{n+j}\}$ is a Fibonacci subsequence.

In the other direction, we know that $\gcd(s,m)=1$, (this is seen in the remark after identity 3.26) therefore there exists a t such that $t(F_n,F_{n+1})\equiv(F_0,F_1) \pmod{m}$, and the result follows as before.

Lemma 4.10 *For odd j, $F_{n-j}+F_n\equiv F_{n+j} \pmod{m}$ if and only if $(L_j-1)F_n\equiv 0 \pmod{m}$.*

Proof: We make use of identity 2.1, namely $F_{n+j}=L_jF_n+(-1)^{j+1}F_{n-j}$, in the first line below.

$$\begin{aligned} F_{n-j}+F_n\equiv F_{n+j} &\iff F_{n-j}+F_n\equiv L_jF_n+(-1)^{j+1}F_{n-j} \\ &\iff F_n\equiv L_jF_n \text{ (since } j \text{ is odd)} \\ &\iff (L_j-1)F_n\equiv 0 \pmod{m}. \end{aligned}$$

We are now ready to present the main theorem of this section.

Theorem 4.11 *If $F_j\equiv F_{2j} \pmod{m}$, then $\{F_n,F_{n+j}\}$ is a Fibonacci subsequence for all n such that $F_n\equiv 0 \pmod{m}$.*

Proof: We will look at two cases: j is odd and j is even. In each case we will show that $\{F_0,F_j\}$ must be a Fibonacci subsequence, then application of lemma 4.9 will imply the conclusion of the theorem.

Case 1: Suppose j is odd.

In lemma 4.10 we can view $(L_j-1)F_n\equiv 0 \pmod{m}$ as a linear congruence with F_n given and (L_j-1) the variable. The solution set of this linear congruence is $(L_j-1)\equiv\{0,\frac{m}{d_n},\frac{2m}{d_n},\frac{3m}{d_n},\ldots,\frac{(d_n-1)m}{d_n}\}$ where $d_n=\gcd(F_n,m)$. If (L_j-1) is congruent to any of the elements in the set, then the linear congruence will be satisfied. [4, p. 78].

Let n be given. Then

$$\begin{aligned} &\{\text{odd } j\ : F_{n-j}+F_n\equiv F_{n+j}\} \\ =\ &\left\{\text{odd } j\ : (L_j-1)\equiv 0,\frac{m}{d_n},\frac{2m}{d_n},\frac{3m}{d_n},\ldots,\text{ or }\frac{(d_n-1)m}{d_n}\right\}. \end{aligned}$$

We know that $F_n|F_{tn}$ so we must have $\gcd(F_n,m)|\gcd(F_{tn},m)$. Thus, using previous notation, $d_n|d_{tn}$. It follows that $\{0,\frac{m}{d_n},\frac{2m}{d_n},\ldots,\frac{(d_n-1)m}{d_n}\}\subseteq\{0,\frac{m}{d_{tn}},\frac{2m}{d_{tn}},\ldots,\frac{(d_{tn}-1)m}{d_{tn}}\}$.

Hence, if j is a solution given n, then j is a solution given any multiple of n. In other words, if $F_{n-j} + F_n \equiv F_{n+j} \pmod{m}$ then $F_{tn-j} + F_{tn} \equiv F_{tn+j} \pmod{m}$ for all t.

In particular, suppose that j is a solution given $n = j$ (this is exactly what the hypothesis of our theorem supposes). Then $F_0 + F_j \equiv F_{2j}$, $F_j + F_{2j} \equiv F_{3j}$, $F_{2j} + F_{3j} \equiv F_{4j}$, $\ldots \pmod{m}$. That is, $\{F_0, F_j\}$ is a Fibonacci subsequence.

Case 2: Suppose j is even.

First we look at a necessary condition. If we assume that $\{F_0, F_j\}$ is, in fact, a Fibonacci subsequence then we must have $F_j \equiv F_0 + F_{-j} \equiv F_{-j} \pmod{m}$. However, we know from identity 1.3 that for even j, $F_{-j} = -F_j$, and so we must conclude that $F_j \equiv -F_j \pmod{m}$. Thus if m is odd we must have $F_j \equiv 0 \pmod{m}$, and if m is even we have either $F_j \equiv 0$ or $\frac{m}{2} \pmod{m}$. Hence, the only nontrivial case occurs when m is even and $F_j \equiv \frac{m}{2} \pmod{m}$.

Once again, identity 2.1 states that $F_{n+j} = L_j F_n + (-1)^{j+1} F_{n-j}$. When we let $n = tj - j$ we get $F_{tj} = L_j F_{(t-1)j} + (-1)^{j+1} F_{(t-2)j}$. When $t = 2$ we get the familiar identity $F_{2j} = L_j F_j$, which implies here, $\frac{m}{2} \equiv L_j(\frac{m}{2}) \pmod{m}$. We use this relation to simplify the congruences (taken mod m) below.

$$\begin{aligned}
F_{3j} &\equiv L_j F_{2j} - F_j \\
&\equiv L_j(\frac{m}{2}) - (\frac{m}{2}) \equiv 0 \\
F_{4j} &\equiv L_j F_{3j} - F_{2j} \\
&\equiv L_j(0) - (\frac{m}{2}) \equiv \frac{m}{2} \\
F_{5j} &\equiv L_j F_{4j} - F_{3j} \\
&\equiv L_j(\frac{m}{2}) - (0) \equiv \frac{m}{2} \\
&\vdots
\end{aligned}$$

Hence our subsequence $\{F_0, F_j\} = 0, \frac{m}{2}, \frac{m}{2}, 0, \frac{m}{2}, \frac{m}{2}, \ldots$ will continue on in this manner and $\{F_0, F_j\}$ is a Fibonacci subsequence.

Now it is a simple matter to apply lemma 4.9 and see that if $F_n \equiv 0 \pmod{m}$ then $\{F_n, F_{n+j}\}$ must also be a Fibonacci subsequence.

This result gives us a fairly easy method for finding many of the Fibonacci subsequences of $F(\text{mod } m)$, if any exist. However, this method may actually give us more than that as the following conjecture asserts.

Conjecture 4.12 *If $5 \not| m$ then every Fibonacci subsequence contains a zero.*

If the above conjecture is true, then our method should give us *all* the Fibonacci subsequences of $F(\text{mod } m)$ when $5 \not| m$. It also appears that every time $5|m$ there must be at least one Fibonacci subsequence containing no zeros. This may have something to do with the fact that the period of the Lucas numbers $= k(m)$ when $5 \not| m$, and $\frac{1}{5}k(m)$ when $5|m$.

We also make the next conjecture, which tests for the existence of a Fibonacci subsequence when we are given four terms in a row and none of them are required to be congruent to zero modulo m.

Conjecture 4.13 *If $F_{n-j} + F_n \equiv F_{n+j}$ and $F_n + F_{n+j} \equiv F_{n+2j} \pmod{m}$ then $\{F_n, F_{n+j}\}$ is a Fibonacci subsequence.*

Finding just three consecutive terms of a subsequence which exhibit the Fibonacci recurrence relation is not sufficient to conclude that the subsequence is a Fibonacci subsequence. As a counter example we see that F_7, F_9, F_{11} are 1, 4, and 5 $\pmod{6}$ respectively, but $F_{13} \equiv 5 \pmod{6}$.

One thing that makes this area of research attractive is that these subsequences appear quite frequently. Suppose we don't count rotations as different subsequences, and we don't count trivial subsequences of all zeros or the Fibonacci sequence itself. Then for example we find that $F(\text{mod } 5)$ contains 8 Fibonacci subsequences, $F(\text{mod } 6)$ contains 11 Fibonacci subsequences, $F(\text{mod } 7)$ contains 1 Fibonacci subsequence, and $F(\text{mod } 10)$ contains 39 Fibonacci subsequences. Table 4.2 lists all the "smallest" pairs $(n, n+j)$ for which $\{F_n, F_{n+j}\}$ is a Fibonacci subsequence modulo 10. Note that $k(10) = 60$ and $\beta(10) = 4$.

Finally we mention that not only is the existence of these special subsequences interesting, but how they actually look has its intrigue. We have seen that if a Fibonacci subsequence exits with even spread, then it has the form $(\frac{m}{2})\cdot[F(\text{mod } 2)]$. Every third residue from $F(\text{mod } 6)$ forms a sequence like $2\cdot[F(\text{mod } 3)]$. Every seventh residue from $F(\text{mod } 91)$ forms a sequence like $F(\text{mod } 7)$ multiplied through by 13.

j	$\gcd(j, 60)$	$(n, n+j)$
1	1	(0,1)
5	5	(0,5) (1,6) (2,7) (3,8) (4,9)
9	3	(0,9)
10	10	(0,10) (5,15)
13	1	(0,13)
15	15	(0,15)*
17	1	(0,17)
20	20	(0,20) (5,25) (10,30) (15,45)
21	3	(0,21)
25	5	(0,25) (1,26) (2,27) (3,28) (4,29)
29	1	(0,29)
30	30	(0,30)* (15,45)*
33	3	(0,33)
35	5	(0,35)
37	1	(0,37)
40	20	(0,40) (5,45) (10,50) (15,55)
41	1	(0,41)
45	15	(0,45)* (3,48) (6,51) (9,54) (12,57)
49	1	(0,49)
50	10	(0,50) (5,55)
53	1	(0,53)
55	5	(0,55)
57	3	(0,57)
60	60	(0,60)* (15,75)* (30,90)* (45,105)*

Table 4.2: Subsequences of $F(\text{mod } 10)$. The subsequences with asterisks are trivial subsequences, containing only zeros.

Once again, it appears that for every new insight we gain into the Fibonacci sequence, a multitude of new relationships emerge to amaze and intrigue us.

Appendix A

The First 30 Fibonacci and Lucas Numbers

n	F_n			L_n		
1	1			1		
2	1			3		
3	2			4	$=$	2^2
4	3			7		
5	5			11		
6	8	$=$	2^3	18	$=$	$2 \cdot 3^2$
7	13			29		
8	21	$=$	$3 \cdot 7$	47		
9	34	$=$	$2 \cdot 17$	76	$=$	$2^2 \cdot 19$
10	55	$=$	$5 \cdot 11$	123	$=$	$3 \cdot 41$
11	89			199		
12	144	$=$	$2^4 \cdot 3^2$	322	$=$	$2 \cdot 7 \cdot 23$
13	233			521		
14	377	$=$	$13 \cdot 29$	843	$=$	$3 \cdot 281$
15	610	$=$	$2 \cdot 5 \cdot 61$	1364	$=$	$2^2 \cdot 11 \cdot 31$
16	987	$=$	$3 \cdot 7 \cdot 47$	2207		
17	1597			3571		
18	2584	$=$	$2^3 \cdot 17 \cdot 19$	5778	$=$	$2 \cdot 3^3 \cdot 107$
19	4181	$=$	$37 \cdot 113$	9349		
20	6765	$=$	$3 \cdot 5 \cdot 11 \cdot 41$	15127	$=$	$7 \cdot 2161$
21	10946	$=$	$2 \cdot 13 \cdot 421$	24476	$=$	$2^2 \cdot 29 \cdot 211$
22	17711	$=$	$89 \cdot 199$	39603	$=$	$3 \cdot 43 \cdot 307$
23	28657			64079	$=$	$139 \cdot 461$
24	46368	$=$	$2^5 \cdot 3^2 \cdot 7 \cdot 23$	103682	$=$	$2 \cdot 47 \cdot 1103$
25	75025	$=$	$5^2 \cdot 3001$	167761	$=$	$11 \cdot 101 \cdot 161$
26	121393	$=$	$233 \cdot 521$	271443	$=$	$3 \cdot 90481$
27	196418	$=$	$2 \cdot 17 \cdot 53 \cdot 109$	439204	$=$	$2^2 \cdot 19 \cdot 5779$
28	317811	$=$	$3 \cdot 13 \cdot 29 \cdot 281$	710647	$=$	$7^2 \cdot 14503$
29	514229			1149851	$=$	$59 \cdot 19489$
30	832040	$=$	$2^3 \cdot 5 \cdot 11 \cdot 31 \cdot 61$	1860498	$=$	$2 \cdot 3^2 \cdot 41 \cdot 2521$

Appendix B

$k(m)$, $\alpha(m)$, and $\beta(m)$ for 2 $\leq$ m $\leq$ 1000

m	$k(m)$	$\alpha(m)$	$\beta(m)$	m	$k(m)$	$\alpha(m)$	$\beta(m)$	m	$k(m)$	$\alpha(m)$	$\beta(m)$
2	3	3	1	37	76	19	4	72	24	12	2
3	8	4	2	38	18	18	1	73	148	37	4
4	6	6	1	39	56	28	2	74	228	57	4
5	20	5	4	40	60	30	2	75	200	100	2
6	24	12	2	41	40	20	2	76	18	18	1
7	16	8	2	42	48	24	2	77	80	40	2
8	12	6	2	43	88	44	2	78	168	84	2
9	24	12	2	44	30	30	1	79	78	78	1
10	60	15	4	45	120	60	2	80	120	60	2
11	10	10	1	46	48	24	2	81	216	108	2
12	24	12	2	47	32	16	2	82	120	60	2
13	28	7	4	48	24	12	2	83	168	84	2
14	48	24	2	49	112	56	2	84	48	24	2
15	40	20	2	50	300	75	4	85	180	45	4
16	24	12	2	51	72	36	2	86	264	132	2
17	36	9	4	52	84	42	2	87	56	28	2
18	24	12	2	53	108	27	4	88	60	30	2
19	18	18	1	54	72	36	2	89	44	11	4
20	60	30	2	55	20	10	2	90	120	60	2
21	16	8	2	56	48	24	2	91	112	56	2
22	30	30	1	57	72	36	2	92	48	24	2
23	48	24	2	58	42	42	1	93	120	60	2
24	24	12	2	59	58	58	1	94	96	48	2
25	100	25	4	60	120	60	2	95	180	90	2
26	84	21	4	61	60	15	4	96	48	24	2
27	72	36	2	62	30	30	1	97	196	49	4
28	48	24	2	63	48	24	2	98	336	168	2
29	14	14	1	64	96	48	2	99	120	60	2
30	120	60	2	65	140	35	4	100	300	150	2
31	30	30	1	66	120	60	2	101	50	50	1
32	48	24	2	67	136	68	2	102	72	36	2
33	40	20	2	68	36	18	2	103	208	104	2
34	36	9	4	69	48	24	2	104	84	42	2
35	80	40	2	70	240	120	2	105	80	40	2
36	24	12	2	71	70	70	1	106	108	27	4

m	$k(m)$	$\alpha(m)$	$\beta(m)$	m	$k(m)$	$\alpha(m)$	$\beta(m)$	m	$k(m)$	$\alpha(m)$	$\beta(m)$
107	72	36	2	146	444	111	4	185	380	95	4
108	72	36	2	147	112	56	2	186	120	60	2
109	108	27	4	148	228	114	2	187	180	90	2
110	60	30	2	149	148	37	4	188	96	48	2
111	152	76	2	150	600	300	2	189	144	72	2
112	48	24	2	151	50	50	1	190	180	90	2
113	76	19	4	152	36	18	2	191	190	190	1
114	72	36	2	153	72	36	2	192	96	48	2
115	240	120	2	154	240	120	2	193	388	97	4
116	42	42	1	155	60	30	2	194	588	147	4
117	168	84	2	156	168	84	2	195	280	140	2
118	174	174	1	157	316	79	4	196	336	168	2
119	144	72	2	158	78	78	1	197	396	99	4
120	120	60	2	159	216	108	2	198	120	60	2
121	110	110	1	160	240	120	2	199	22	22	1
122	60	15	4	161	48	24	2	200	300	150	2
123	40	20	2	162	216	108	2	201	136	68	2
124	30	30	1	163	328	164	2	202	150	150	1
125	500	125	4	164	120	60	2	203	112	56	2
126	48	24	2	165	40	20	2	204	72	36	2
127	256	128	2	166	168	84	2	205	40	20	2
128	192	96	2	167	336	168	2	206	624	312	2
129	88	44	2	168	48	24	2	207	48	24	2
130	420	105	4	169	364	91	4	208	168	84	2
131	130	130	1	170	180	45	4	209	90	90	1
132	120	60	2	171	72	36	2	210	240	120	2
133	144	72	2	172	264	132	2	211	42	42	1
134	408	204	2	173	348	87	4	212	108	54	2
135	360	180	2	174	168	84	2	213	280	140	2
136	36	18	2	175	400	200	2	214	72	36	2
137	276	69	4	176	120	60	2	215	440	220	2
138	48	24	2	177	232	116	2	216	72	36	2
139	46	46	1	178	132	33	4	217	240	120	2
140	240	120	2	179	178	178	1	218	108	27	4
141	32	16	2	180	120	60	2	219	296	148	2
142	210	210	1	181	90	90	1	220	60	30	2
143	140	70	2	182	336	168	2	221	252	63	4
144	24	12	2	183	120	60	2	222	456	228	2
145	140	70	2	184	48	24	2	223	448	224	2

m	$k(m)$	$\alpha(m)$	$\beta(m)$
224	48	24	2
225	600	300	2
226	228	57	4
227	456	228	2
228	72	36	2
229	114	114	1
230	240	120	2
231	80	40	2
232	84	42	2
233	52	13	4
234	168	84	2
235	160	80	2
236	174	174	1
237	312	156	2
238	144	72	2
239	238	238	1
240	120	60	2
241	240	120	2
242	330	330	1
243	648	324	2
244	60	30	2
245	560	280	2
246	120	60	2
247	252	126	2
248	60	30	2
249	168	84	2
250	1500	375	4
251	250	250	1
252	48	24	2
253	240	120	2
254	768	384	2
255	360	180	2
256	384	192	2
257	516	129	4
258	264	132	2
259	304	152	2
260	420	210	2
261	168	84	2
262	390	390	1
263	176	88	2
264	120	60	2
265	540	135	4
266	144	72	2
267	88	44	2
268	408	204	2
269	268	67	4
270	360	180	2
271	270	270	1
272	72	36	2
273	112	56	2
274	276	69	4
275	100	50	2
276	48	24	2
277	556	139	4
278	138	138	1
279	120	60	2
280	240	120	2
281	56	28	2
282	96	48	2
283	568	284	2
284	210	210	1
285	360	180	2
286	420	210	2
287	80	40	2
288	48	24	2
289	612	153	4
290	420	210	2
291	392	196	2
292	444	222	2
293	588	147	4
294	336	168	2
295	580	290	2
296	228	114	2
297	360	180	2
298	444	111	4
299	336	168	2
300	600	300	2
301	176	88	2
302	150	150	1
303	200	100	2
304	72	36	2
305	60	15	4
306	72	36	2
307	88	44	2
308	240	120	2
309	208	104	2
310	60	30	2
311	310	310	1
312	168	84	2
313	628	157	4
314	948	237	4
315	240	120	2
316	78	78	1
317	636	159	4
318	216	108	2
319	70	70	1
320	480	240	2
321	72	36	2
322	48	24	2
323	36	18	2
324	216	108	2
325	700	175	4
326	984	492	2
327	216	108	2
328	120	60	2
329	32	16	2
330	120	60	2
331	110	110	1
332	168	84	2
333	456	228	2
334	336	168	2
335	680	340	2
336	48	24	2
337	676	169	4
338	1092	273	4
339	152	76	2
340	180	90	2

m	$k(m)$	$\alpha(m)$	$\beta(m)$	m	$k(m)$	$\alpha(m)$	$\beta(m)$	m	$k(m)$	$\alpha(m)$	$\beta(m)$
341	30	30	1	380	180	90	2	419	418	418	1
342	72	36	2	381	256	128	2	420	240	120	2
343	784	392	2	382	570	570	1	421	84	21	4
344	264	132	2	383	768	384	2	422	42	42	1
345	240	120	2	384	192	96	2	423	96	48	2
346	348	87	4	385	80	40	2	424	108	54	2
347	232	116	2	386	1164	291	4	425	900	225	4
348	168	84	2	387	264	132	2	426	840	420	2
349	174	174	1	388	588	294	2	427	240	120	2
350	1200	600	2	389	388	97	4	428	72	36	2
351	504	252	2	390	840	420	2	429	280	140	2
352	240	120	2	391	144	72	2	430	1320	660	2
353	236	59	4	392	336	168	2	431	430	430	1
354	696	348	2	393	520	260	2	432	72	36	2
355	140	70	2	394	396	99	4	433	868	217	4
356	132	66	2	395	780	390	2	434	240	120	2
357	144	72	2	396	120	60	2	435	280	140	2
358	534	534	1	397	796	199	4	436	108	54	2
359	358	358	1	398	66	66	1	437	144	72	2
360	120	60	2	399	144	72	2	438	888	444	2
361	342	342	1	400	600	300	2	439	438	438	1
362	90	90	1	401	200	100	2	440	60	30	2
363	440	220	2	402	408	204	2	441	336	168	2
364	336	168	2	403	420	210	2	442	252	63	4
365	740	185	4	404	150	150	1	443	888	444	2
366	120	60	2	405	1080	540	2	444	456	228	2
367	736	368	2	406	336	168	2	445	220	55	4
368	48	24	2	407	380	190	2	446	1344	672	2
369	120	60	2	408	72	36	2	447	296	148	2
370	1140	285	4	409	408	204	2	448	96	48	2
371	432	216	2	410	120	60	2	449	448	224	2
372	120	60	2	411	552	276	2	450	600	300	2
373	748	187	4	412	624	312	2	451	40	20	2
374	180	90	2	413	464	232	2	452	228	114	2
375	1000	500	2	414	48	24	2	453	200	100	2
376	96	48	2	415	840	420	2	454	456	228	2
377	28	14	2	416	336	168	2	455	560	280	2
378	144	72	2	417	184	92	2	456	72	36	2
379	378	378	1	418	90	90	1	457	916	229	4

m	$k(m)$	$\alpha(m)$	$\beta(m)$
458	114	114	1
459	72	36	2
460	240	120	2
461	46	46	1
462	240	120	2
463	928	464	2
464	168	84	2
465	120	60	2
466	156	39	4
467	936	468	2
468	168	84	2
469	272	136	2
470	480	240	2
471	632	316	2
472	348	174	2
473	440	220	2
474	312	156	2
475	900	450	2
476	144	72	2
477	216	108	2
478	714	714	1
479	478	478	1
480	240	120	2
481	532	133	4
482	240	120	2
483	48	24	2
484	330	330	1
485	980	245	4
486	648	324	2
487	976	488	2
488	60	30	2
489	328	164	2
490	1680	840	2
491	490	490	1
492	120	60	2
493	252	126	2
494	252	126	2
495	120	60	2
496	120	60	2
497	560	280	2
498	168	84	2
499	498	498	1
500	1500	750	2
501	336	168	2
502	750	750	1
503	1008	504	2
504	48	24	2
505	100	50	2
506	240	120	2
507	728	364	2
508	768	384	2
509	254	254	1
510	360	180	2
511	592	296	2
512	768	384	2
513	72	36	2
514	516	129	4
515	1040	520	2
516	264	132	2
517	160	80	2
518	912	456	2
519	696	348	2
520	420	210	2
521	26	26	1
522	168	84	2
523	1048	524	2
524	390	390	1
525	400	200	2
526	528	264	2
527	180	90	2
528	120	60	2
529	1104	552	2
530	540	135	4
531	696	348	2
532	144	72	2
533	280	140	2
534	264	132	2
535	360	180	2
536	408	204	2
537	712	356	2
538	804	201	4
539	560	280	2
540	360	180	2
541	90	90	1
542	270	270	1
543	360	180	2
544	144	72	2
545	540	135	4
546	336	168	2
547	1096	548	2
548	276	138	2
549	120	60	2
550	300	150	2
551	126	126	1
552	48	24	2
553	624	312	2
554	1668	417	4
555	760	380	2
556	138	138	1
557	124	31	4
558	120	60	2
559	616	308	2
560	240	120	2
561	360	180	2
562	168	84	2
563	376	188	2
564	96	48	2
565	380	95	4
566	1704	852	2
567	432	216	2
568	420	210	2
569	568	284	2
570	360	180	2
571	570	570	1
572	420	210	2
573	760	380	2
574	240	120	2

m	$k(m)$	$\alpha(m)$	$\beta(m)$	m	$k(m)$	$\alpha(m)$	$\beta(m)$	m	$k(m)$	$\alpha(m)$	$\beta(m)$
575	1200	600	2	614	264	132	2	653	1308	327	4
576	96	48	2	615	40	20	2	654	216	108	2
577	1156	289	4	616	240	120	2	655	260	130	2
578	612	153	4	617	1236	309	4	656	120	60	2
579	776	388	2	618	624	312	2	657	888	444	2
580	420	210	2	619	206	206	1	658	96	48	2
581	336	168	2	620	60	30	2	659	658	658	1
582	1176	588	2	621	144	72	2	660	120	60	2
583	540	270	2	622	930	930	1	661	220	55	4
584	444	222	2	623	176	88	2	662	330	330	1
585	840	420	2	624	168	84	2	663	504	252	2
586	588	147	4	625	2500	625	4	664	168	84	2
587	1176	588	2	626	1884	471	4	665	720	360	2
588	336	168	2	627	360	180	2	666	456	228	2
589	90	90	1	628	948	474	2	667	336	168	2
590	1740	870	2	629	684	171	4	668	336	168	2
591	792	396	2	630	240	120	2	669	448	224	2
592	456	228	2	631	630	630	1	670	2040	1020	2
593	1188	297	4	632	156	78	2	671	60	30	2
594	360	180	2	633	168	84	2	672	48	24	2
595	720	360	2	634	636	159	4	673	1348	337	4
596	444	222	2	635	1280	640	2	674	2028	507	4
597	88	44	2	636	216	108	2	675	1800	900	2
598	336	168	2	637	112	56	2	676	1092	546	2
599	598	598	1	638	210	210	1	677	452	113	4
600	600	300	2	639	840	420	2	678	456	228	2
601	600	300	2	640	960	480	2	679	784	392	2
602	528	264	2	641	640	320	2	680	180	90	2
603	408	204	2	642	72	36	2	681	456	228	2
604	150	150	1	643	1288	644	2	682	30	30	1
605	220	110	2	644	48	24	2	683	1368	684	2
606	600	300	2	645	440	220	2	684	72	36	2
607	1216	608	2	646	36	18	2	685	1380	345	4
608	144	72	2	647	1296	648	2	686	2352	1176	2
609	112	56	2	648	216	108	2	687	456	228	2
610	60	15	4	649	290	290	1	688	264	132	2
611	224	112	2	650	2100	525	4	689	756	189	4
612	72	36	2	651	240	120	2	690	240	120	2
613	1228	307	4	652	984	492	2	691	138	138	1

m	$k(m)$	$\alpha(m)$	$\beta(m)$
692	348	174	2
693	240	120	2
694	696	348	2
695	460	230	2
696	168	84	2
697	360	180	2
698	174	174	1
699	104	52	2
700	1200	600	2
701	700	175	4
702	504	252	2
703	684	342	2
704	480	240	2
705	160	80	2
706	708	177	4
707	400	200	2
708	696	348	2
709	118	118	1
710	420	210	2
711	312	156	2
712	132	66	2
713	240	120	2
714	144	72	2
715	140	70	2
716	534	534	1
717	952	476	2
718	1074	1074	1
719	718	718	1
720	120	60	2
721	208	104	2
722	342	342	1
723	240	120	2
724	90	90	1
725	700	350	2
726	1320	660	2
727	1456	728	2
728	336	168	2
729	1944	972	2
730	2220	555	4
731	792	396	2
732	120	60	2
733	1468	367	4
734	2208	1104	2
735	560	280	2
736	48	24	2
737	680	340	2
738	120	60	2
739	738	738	1
740	1140	570	2
741	504	252	2
742	432	216	2
743	496	248	2
744	120	60	2
745	740	185	4
746	2244	561	4
747	168	84	2
748	180	90	2
749	144	72	2
750	3000	1500	2
751	750	750	1
752	96	48	2
753	1000	500	2
754	84	42	2
755	100	50	2
756	144	72	2
757	1516	379	4
758	378	378	1
759	240	120	2
760	180	90	2
761	380	95	4
762	768	384	2
763	432	216	2
764	570	570	1
765	360	180	2
766	768	384	2
767	812	406	2
768	384	192	2
769	192	96	2
770	240	120	2
771	1032	516	2
772	1164	582	2
773	1548	387	4
774	264	132	2
775	300	150	2
776	588	294	2
777	304	152	2
778	1164	291	4
779	360	180	2
780	840	420	2
781	70	70	1
782	144	72	2
783	504	252	2
784	336	168	2
785	1580	395	4
786	1560	780	2
787	1576	788	2
788	396	198	2
789	176	88	2
790	780	390	2
791	304	152	2
792	120	60	2
793	420	105	4
794	2388	597	4
795	1080	540	2
796	66	66	1
797	228	57	4
798	144	72	2
799	288	144	2
800	1200	600	2
801	264	132	2
802	600	300	2
803	740	370	2
804	408	204	2
805	240	120	2
806	420	210	2
807	536	268	2
808	300	150	2

m	$k(m)$	$\alpha(m)$	$\beta(m)$	m	$k(m)$	$\alpha(m)$	$\beta(m)$	m	$k(m)$	$\alpha(m)$	$\beta(m)$
809	202	202	1	848	216	108	2	887	1776	888	2
810	1080	540	2	849	568	284	2	888	456	228	2
811	270	270	1	850	900	225	4	889	256	128	2
812	336	168	2	851	912	456	2	890	660	165	4
813	1080	540	2	852	840	420	2	891	1080	540	2
814	1140	570	2	853	1708	427	4	892	1344	672	2
815	1640	820	2	854	240	120	2	893	288	144	2
816	72	36	2	855	360	180	2	894	888	444	2
817	792	396	2	856	72	36	2	895	1780	890	2
818	408	204	2	857	1716	429	4	896	192	96	2
819	336	168	2	858	840	420	2	897	336	168	2
820	120	60	2	859	78	78	1	898	1344	672	2
821	820	205	4	860	1320	660	2	899	210	210	1
822	552	276	2	861	80	40	2	900	600	300	2
823	1648	824	2	862	1290	1290	1	901	108	27	4
824	624	312	2	863	1728	864	2	902	120	60	2
825	200	100	2	864	144	72	2	903	176	88	2
826	1392	696	2	865	1740	435	4	904	228	114	2
827	1656	828	2	866	2604	651	4	905	180	90	2
828	48	24	2	867	1224	612	2	906	600	300	2
829	276	69	4	868	240	120	2	907	1816	908	2
830	840	420	2	869	390	390	1	908	456	228	2
831	1112	556	2	870	840	420	2	909	600	300	2
832	672	336	2	871	952	476	2	910	1680	840	2
833	1008	504	2	872	108	54	2	911	70	70	1
834	552	276	2	873	1176	588	2	912	72	36	2
835	1680	840	2	874	144	72	2	913	840	420	2
836	90	90	1	875	2000	1000	2	914	2748	687	4
837	360	180	2	876	888	444	2	915	120	60	2
838	1254	1254	1	877	1756	439	4	916	114	114	1
839	838	838	1	878	438	438	1	917	1040	520	2
840	240	120	2	879	1176	588	2	918	72	36	2
841	406	406	1	880	120	60	2	919	102	102	1
842	84	21	4	881	176	88	2	920	240	120	2
843	56	28	2	882	336	168	2	921	88	44	2
844	42	42	1	883	1768	884	2	922	138	138	1
845	1820	455	4	884	252	126	2	923	140	70	2
846	96	48	2	885	1160	580	2	924	240	120	2
847	880	440	2	886	888	444	2	925	1900	475	4

m	$k(m)$	$\alpha(m)$	$\beta(m)$	m	$k(m)$	$\alpha(m)$	$\beta(m)$	m	$k(m)$	$\alpha(m)$	$\beta(m)$
926	2784	1392	2	951	1272	636	2	976	120	60	2
927	624	312	2	952	144	72	2	977	652	163	4
928	336	168	2	953	212	53	4	978	984	492	2
929	928	464	2	954	216	108	2	979	220	110	2
930	120	60	2	955	380	190	2	980	1680	840	2
931	1008	504	2	956	714	714	1	981	216	108	2
932	156	78	2	957	280	140	2	982	1470	1470	1
933	1240	620	2	958	1434	1434	1	983	1968	984	2
934	936	468	2	959	1104	552	2	984	120	60	2
935	180	90	2	960	480	240	2	985	1980	495	4
936	168	84	2	961	930	930	1	986	252	126	2
937	1876	469	4	962	1596	399	4	987	32	16	2
938	816	408	2	963	72	36	2	988	252	126	2
939	1256	628	2	964	240	120	2	989	528	264	2
940	480	240	2	965	1940	485	4	990	120	60	2
941	470	470	1	966	48	24	2	991	198	198	1
942	1896	948	2	967	176	88	2	992	240	120	2
943	240	120	2	968	660	330	2	993	440	220	2
944	696	348	2	969	72	36	2	994	1680	840	2
945	720	360	2	970	2940	735	4	995	220	110	2
946	1320	660	2	971	970	970	1	996	168	84	2
947	1896	948	2	972	648	324	2	997	1996	499	4
948	312	156	2	973	368	184	2	998	498	498	1
949	1036	259	4	974	2928	1464	2	999	1368	684	2
950	900	450	2	975	1400	700	2	1000	1500	750	2

Appendix C

One Period Of $F(\text{mod } m)$ for 2 ≤ m ≤ 50

m																				
2	0	1	1																	
3	0	1	1	2	0	2	2	1												
4	0	1	1	2	3	1														
5	0	1	1	2	3	0	3	3	1	4	0	4	4	3	2	0	2	2	4	1
6	0	1	1	2	3	5	2	1	3	4	1	5	0	5	5	4	3	1	4	5
	3	2	5	1																
7	0	1	1	2	3	5	1	6	0	6	6	5	4	2	6	1				
8	0	1	1	2	3	5	0	5	5	2	7	1								
9	0	1	1	2	3	5	8	4	3	7	1	8	0	8	8	7	6	4	1	5
	6	2	8	1																
10	0	1	1	2	3	5	8	3	1	4	5	9	4	3	7	0	7	7	4	1
	5	6	1	7	8	5	3	8	1	9	0	9	9	8	7	5	2	7	9	6
	5	1	6	7	3	0	3	3	6	9	5	4	9	3	2	5	7	2	9	1
11	0	1	1	2	3	5	8	2	10	1										
12	0	1	1	2	3	5	8	1	9	10	7	5	0	5	5	10	3	1	4	5
	9	2	11	1																
13	0	1	1	2	3	5	8	0	8	8	3	11	1	12	0	12	12	11	10	8
	5	0	5	5	10	2	12	1												
14	0	1	1	2	3	5	8	13	7	6	13	5	4	9	13	8	7	1	8	9
	3	12	1	13	0	13	13	12	11	9	6	1	7	8	1	9	10	5	1	6
	7	13	6	5	11	2	13	1												
15	0	1	1	2	3	5	8	13	6	4	10	14	9	8	2	10	12	7	4	11
	0	11	11	7	3	10	13	8	6	14	5	4	9	13	7	5	12	2	14	1
16	0	1	1	2	3	5	8	13	5	2	7	9	0	9	9	2	11	13	8	5
	13	2	15	1																
17	0	1	1	2	3	5	8	13	4	0	4	4	8	12	3	15	1	16	0	16
	16	15	14	12	9	4	13	0	13	13	9	5	14	2	16	1				
18	0	1	1	2	3	5	8	13	3	16	1	17	0	17	17	16	15	13	10	5
	15	2	17	1																
19	0	1	1	2	3	5	8	13	2	15	17	13	11	5	16	2	18	1		
20	0	1	1	2	3	5	8	13	1	14	15	9	4	13	17	10	7	17	4	1
	5	6	11	17	8	5	13	18	11	9	0	9	9	18	7	5	12	17	9	6
	15	1	16	17	13	10	3	13	16	9	5	14	19	13	12	5	17	2	19	1
21	0	1	1	2	3	5	8	13	0	13	13	5	18	2	20	1				
22	0	1	1	2	3	5	8	13	21	12	11	1	12	13	3	16	19	13	10	1
	11	12	1	13	14	5	19	2	21	1										
23	0	1	1	2	3	5	8	13	21	11	9	20	6	3	9	12	21	10	8	18
	3	21	1	22	0	22	22	21	20	18	15	10	2	12	14	3	17	20	14	11
	2	13	15	5	20	2	22	1												
24	0	1	1	2	3	5	8	13	21	10	7	17	0	17	17	10	3	13	16	5
	21	2	23	1																

m																				
25	0	1	1	2	3	5	8	13	21	9	5	14	19	8	2	10	12	22	9	6
	15	21	11	7	18	0	18	18	11	4	15	19	9	3	12	15	2	17	19	11
	5	16	21	12	8	20	3	23	1	24	0	24	24	23	22	20	17	12	4	16
	20	11	6	17	23	15	13	3	16	19	10	4	14	18	7	0	7	7	14	21
	10	6	16	22	13	10	23	8	6	14	20	9	4	13	17	5	22	2	24	1
26	0	1	1	2	3	5	8	13	21	8	3	11	14	25	13	12	25	11	10	21
	5	0	5	5	10	15	25	14	13	1	14	15	3	18	21	13	8	21	3	24
	1	25	0	25	25	24	23	21	18	13	5	18	23	15	12	1	13	14	1	15
	16	5	21	0	21	21	16	11	1	12	13	25	12	11	23	8	5	13	18	5
	23	2	25	1																
27	0	1	1	2	3	5	8	13	21	7	1	8	9	17	26	16	15	4	19	23
	15	11	26	10	9	19	1	20	21	14	8	22	3	25	1	26	0	26	26	25
	24	22	19	14	6	20	26	19	18	10	1	11	12	23	8	4	12	16	1	17
	18	8	26	7	6	13	19	5	24	2	26	1								
28	0	1	1	2	3	5	8	13	21	6	27	5	4	9	13	22	7	1	8	9
	17	26	15	13	0	13	13	26	11	9	20	1	21	22	15	9	24	5	1	6
	7	13	20	5	25	2	27	1												
29	0	1	1	2	3	5	8	13	21	5	26	2	28	1						
30	0	1	1	2	3	5	8	13	21	4	25	29	24	23	17	10	27	7	4	11
	15	26	11	7	18	25	13	8	21	29	20	19	9	28	7	5	12	17	29	16
	15	1	16	17	3	20	23	13	6	19	25	14	9	23	2	25	27	22	19	11
	0	11	11	22	3	25	28	23	21	14	5	19	24	13	7	20	27	17	14	1
	15	16	1	17	18	5	23	28	21	19	10	29	9	8	17	25	12	7	19	26
	15	11	26	7	3	10	13	23	6	29	5	4	9	13	22	5	27	2	29	1
31	0	1	1	2	3	5	8	13	21	3	24	27	20	16	5	21	26	16	11	27
	7	3	10	13	23	5	28	2	30	1										
32	0	1	1	2	3	5	8	13	21	2	23	25	16	9	25	2	27	29	24	21
	13	2	15	17	0	17	17	2	19	21	8	29	5	2	7	9	16	25	9	2
	11	13	24	5	29	2	31	1												
33	0	1	1	2	3	5	8	13	21	1	22	23	12	2	14	16	30	13	10	23
	0	23	23	13	3	16	19	2	21	23	11	1	12	13	25	5	30	2	32	1
34	0	1	1	2	3	5	8	13	21	0	21	21	8	29	3	32	1	33	0	33
	33	32	31	29	26	21	13	0	13	13	26	5	31	2	33	1				
35	0	1	1	2	3	5	8	13	21	34	20	19	4	23	27	15	7	22	29	16
	10	26	1	27	28	20	13	33	11	9	20	29	14	8	22	30	17	12	29	6
	0	6	6	12	18	30	13	8	21	29	15	9	24	33	22	20	7	27	34	26
	25	16	6	22	28	15	8	23	31	19	15	34	14	13	27	5	32	2	34	1
36	0	1	1	2	3	5	8	13	21	34	19	17	0	17	17	34	15	13	28	5
	33	2	35	1																
37	0	1	1	2	3	5	8	13	21	34	18	15	33	11	7	18	25	6	31	0
	31	31	25	19	7	26	33	22	18	3	21	24	8	32	3	35	1	36	0	36
	36	35	34	32	29	24	16	3	19	22	4	26	30	19	12	31	6	0	6	6
	12	18	30	11	4	15	19	34	16	13	29	5	34	2	36	1				
38	0	1	1	2	3	5	8	13	21	34	17	13	30	5	35	2	37	1		
39	0	1	1	2	3	5	8	13	21	34	16	11	27	38	26	25	12	37	10	8
	18	26	5	31	36	28	25	14	0	14	14	28	3	31	34	26	21	8	29	37
	27	25	13	38	12	11	23	34	18	13	31	5	36	2	38	1				
40	0	1	1	2	3	5	8	13	21	34	15	9	24	33	17	10	27	37	24	21
	5	26	31	17	8	25	33	18	11	29	0	29	29	18	7	25	32	17	9	26
	35	21	16	37	13	10	23	33	16	9	25	34	19	13	32	5	37	2	39	1

m																				
41	0	1	1	2	3	5	8	13	21	34	14	7	21	28	8	36	3	39	1	40
	0	40	40	39	38	36	33	28	20	7	27	34	20	13	33	5	38	2	40	1
42	0	1	1	2	3	5	8	13	21	34	13	5	18	23	41	22	21	1	22	23
	3	26	29	13	0	13	13	26	39	23	20	1	21	22	1	23	24	5	29	34
	21	13	34	5	39	2	41	1												
43	0	1	1	2	3	5	8	13	21	34	12	3	15	18	33	8	41	6	4	10
	14	24	38	19	14	33	4	37	41	35	33	25	15	40	12	9	21	30	8	38
	3	41	1	42	0	42	42	41	40	38	35	30	22	9	31	40	28	25	10	35
	2	37	39	33	29	19	5	24	29	10	39	6	2	8	10	18	28	3	31	34
	22	13	35	5	40	2	42	1												
44	0	1	1	2	3	5	8	13	21	34	11	1	12	13	25	38	19	13	32	1
	33	34	23	13	36	5	41	2	43	1										
45	0	1	1	2	3	5	8	13	21	34	10	44	9	8	17	25	42	22	19	41
	15	11	26	37	18	10	28	38	21	14	35	4	39	43	37	35	27	17	44	16
	15	31	1	32	33	20	8	28	36	19	10	29	39	23	17	40	12	7	19	26
	0	26	26	7	33	40	28	23	6	29	35	19	9	28	37	20	12	32	44	31
	30	16	1	17	18	35	8	43	6	4	10	14	24	38	17	10	27	37	19	11
	30	41	26	22	3	25	28	8	36	44	35	34	24	13	37	5	42	2	44	1
46	0	1	1	2	3	5	8	13	21	34	9	43	6	3	9	12	21	33	8	41
	3	44	1	45	0	45	45	44	43	41	38	33	25	12	37	3	40	43	37	34
	25	13	38	5	43	2	45	1												
47	0	1	1	2	3	5	8	13	21	34	8	42	3	45	1	46	0	46	46	45
	44	42	39	34	26	13	39	5	44	2	46	1								
48	0	1	1	2	3	5	8	13	21	34	7	41	0	41	41	34	27	13	40	5
	45	2	47	1																
49	0	1	1	2	3	5	8	13	21	34	6	40	46	37	34	22	7	29	36	16
	3	19	22	41	14	6	20	26	46	23	20	43	14	8	22	30	3	33	36	20
	7	27	34	12	46	9	6	15	21	36	8	44	3	47	1	48	0	48	48	47
	46	44	41	36	28	15	43	9	3	12	15	27	42	20	13	33	46	30	27	8
	35	43	29	23	3	26	29	6	35	41	27	19	46	16	13	29	42	22	15	37
	3	40	43	34	28	13	41	5	46	2	48	1								
50	0	1	1	2	3	5	8	13	21	34	5	39	44	33	27	10	37	47	34	31
	15	46	11	7	18	25	43	18	11	29	40	19	9	28	37	15	2	17	19	36
	5	41	46	37	33	20	3	23	26	49	25	24	49	23	22	45	17	12	29	41
	20	11	31	42	23	15	38	3	41	44	35	29	14	43	7	0	7	7	14	21
	35	6	41	47	38	35	23	8	31	39	20	9	29	38	17	5	22	27	49	26
	25	1	26	27	3	30	33	13	46	9	5	14	19	33	2	35	37	22	9	31
	40	21	11	32	43	25	18	43	11	4	15	19	34	3	37	40	27	17	44	11
	5	16	21	37	8	45	3	48	1	49	0	49	49	48	47	45	42	37	29	16
	45	11	6	17	23	40	13	3	16	19	35	4	39	43	32	25	7	32	39	21
	10	31	41	22	13	35	48	33	31	14	45	9	4	13	17	30	47	27	24	1
	25	26	1	27	28	5	33	38	21	9	30	39	19	8	27	35	12	47	9	6
	15	21	36	7	43	0	43	43	36	29	15	44	9	3	12	15	27	42	19	11
	30	41	21	12	33	45	28	23	1	24	25	49	24	23	47	20	17	37	4	41
	45	36	31	17	48	15	13	28	41	19	10	29	39	18	7	25	32	7	39	46
	35	31	16	47	13	10	23	33	6	39	45	34	29	13	42	5	47	2	49	1

Bibliography

[1] Brother U. Alfred, "Primes which are Factors of All Fibonacci Sequences," Fibonacci Quarterly, 2 (1964), pp. 33-38.

[2] Agnes Andreassian, "Fibonacci Sequences Modulo M," Fibonacci Quarterly, 12 (1974), pp. 51-64.

[3] Huseyin Aydin and Geoff C. Smith, "Fourier Analysis in Finite Nilpotent Groups," Applications of Fibonacci Numbers, vol. 5 (1993), pp. 49-59.

[4] David M. Burton, Elementary Number Theory, Third Edition, Wm. C. Brown Publishers, Dubuque, Iowa, 1994.

[5] Paul A. Catlin, "A Lower Bound for the Period of the Fibonacci Series Modulo M," Fibonacci Quarterly, 12 (1974), pp. 349-350.

[6] Stuart Clary and Paul Hemenway, "On Sums of Cubes of Fibonacci Numbers," Applications of Fibonacci Numbers, vol. 5 (1993), pp. 123-136.

[7] Amos Ehrlich, "On the Periods of the Fibonacci Sequence Modulo M," Fibonacci Quarterly, 27 (1989), pp. 11-13.

[8] Herta T. Freitag, "A Property of Unit Digits of Fibonacci Numbers," Fibonacci Numbers and Their Applications, 1984, pp. 39-41.

[9] John H. Halton, "On the Divisibility Properties of Fibonacci Numbers," Fibonacci Quarterly, 4 (1966), pp. 217-240.

[10] E. T. Jacobson, "Distribution of the Fibonacci Numbers Mod 2^k," Fibonacci Quarterly, 30 (1992), pp. 211-215.

[11] Judy Kramer and Verner E. Hoggatt, Jr., "Special Cases of Fibonacci Periodicity," Fibonacci Quarterly, 10 (1972), pp. 519-522.

[12] Lawrence Kuipers and Jau-Shyong Shiue, "A Distribution Property of the Sequence of Fibonacci Numbers," Fibonacci Quarterly, 10 (1972), pp. 375-376, 392.

[13] S. E. Mamangakis, "Remarks on the Fibonacci Series Modulo m," American Mathematical Monthly, 68 (1961), pp. 648-649.

[14] Harald Niederreiter, "Distribution fo the Fibonacci Numbers Mod 5^k," Fibonacci Quarterly, 10 (1972), pp. 373-374.

[15] D. W. Robinson, "The Fibonacci Matrix Modulo m," Fibonacci Quarterly, 1 (1963), pp. 29-36.

[16] Ken Siler "Fibonacci Summations," Fibonacci Quarterly, 1 (1963), pp. 67-70.

[17] T. E. Stanley, "Some Remarks on the Periodicity of the Sequence of Fibonacci Numbers," Fibonacci Quarterly, 14 (1976), pp. 52-54.

[18] T. E. Stanley, "Powers of the Period Function for the Sequence of Fibonacci Numbers," Fibonacci Quarterly, 18 (1980), pp. 44-45.

[19] T. E. Stanley, "Some Remarks on the Periodicity of the Sequence of Fibonacci Numbers - II," Fibonacci Quarterly, 18 (1980), pp. 45-47.

[20] Steven Vajda, Fibonacci & Lucas Numbers, and the Golden Section. Ellis Horwood Limited, Chichester, England, 1989.

[21] John Vinson, "The Relation of the Period Modulo m to the Rand of Apparition of m in the Fibonacci Sequence," Fibonacci Quarterly, 1 (1963), pp. 37-45.

[22] D. D. Wall, "Fibonacci Series Modulo m," American Mathematical Monthly, 67 (1960), pp. 525-532.