# FIBONACCI NUMBERS: REDUCTION FORMULAS AND SHORT PERIODS


**Clifford A. Reiter**
Lafayette College, Easton, PA 18042


*(Submitted November 1991)*


Formulas for determining the Fibonacci numbers $F_{2n}$ and $F_{2n-1}$ in terms of $F_n$ and $F_{n-1}$ are well known as are some higher reduction formulas. For example, formulas for $F_{3n}$ and $F_{3n-1}$ are assigned as homework in Alfred [1], and in Chapter 17 of Dickson [3] there is a formula for $F_{pn}$ when $p$ is odd. This note describes a technique for constructing "simplified" formulas for $F_{in}$ and $F_{in-1}$ in terms of $F_n$ and $F_{n-1}$. Two families of recursively defined polynomials can be used to parametrize these formulas. This parametrization can be applied to the study of the period of the Fibonacci sequence modulo $m$. These periods have been the subject of considerable study; see [4], [6], and [7] as well as [2] which contains generalizations to continued fractions. The period of the Fibonacci sequence modulo $m$ is often close to the modulus in size, but Ehrlich [4] showed that the period of the Fibonacci sequence was surprisingly small for Fibonacci moduli and many other small periods do appear. His work utilized the reduction formulas for $F_{2n}$ and $F_{2n-1}$. We can generalize this result using the simplified reduction formulas for $F_{in}$ and $F_{in-1}$ for each even multiplier $i$.

## INTRODUCTION

It is well known that the Fibonacci numbers can be computed by taking powers of a matrix. Namely, if

$$T=\begin{pmatrix} F_0 & F_1 \\ F_1 & F_2 \end{pmatrix}=\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}, \text{ then } T^n=\begin{pmatrix} F_{n-1} & F_n \\ F_n & F_{n+1} \end{pmatrix}.$$

Consider the matrix $U$, given below, that captures the symmetry of $T^n$ and the fact that the (2, 2)-entry is sum of the entries in the first row. Its powers, $U^i$, can be used to get information about $T^{in}$. In particular, when $a=F_{n-1}$ and $b=F_n$, the first row gives reduction formulas for $F_{in-1}$ and $F_{in}$ in terms of $F_{n-1}$ and $F_n$.

$$U=\begin{pmatrix} a & b \\ b & a+b \end{pmatrix}, \quad U^2=\begin{pmatrix} a^2+b^2 & 2ab+b^2 \\ 2ab+b^2 & a^2+2ab+2b^2 \end{pmatrix}$$

$$U^3=\begin{pmatrix} a^3+3ab^2+b^3 & 3a^2b+3ab^2+2b^3 \\ 3a^2b+3ab^2+2b^3 & a^3+3a^2b+6ab^2+3b^3 \end{pmatrix}$$

The first row of $U^2$ gives the reduction formulas:

$$F_{2n-1}=F_{n-1}^2+F_n^2, \quad F_{2n}=2F_{n-1}F_n+F_n^2.$$

Those equations and simple variations are well known. The first row of $U^3$ gives additional, less well known reduction formulas:

$$F_{3n-1} = F_{n-1}^3 + 3F_{n-1}F_n^3, \quad F_{3n} = 3F_{n-1}^2F_n + 3F_{n-1}F_n^2 + 2F_n^3.$$

Higher reduction formulas can be produced by computing higher powers of $U$. It is easy to see that the entries in $U^i$ are homogeneous polynomials of degree $i$ in the variables $a$ and $b$. Many other formulas for $F_{in}$ and $F_{in-1}$ in terms of $F_n$ and $F_{n-1}$ are possible since

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

In particular, consider simplifying the polynomials in $U^2$ and $U^3$ by the corresponding relation

$$a^2 = b^2 - ab + (-1)^n. \qquad (*)$$

(One can think of this as a simplification that introduces a new formal parameter $n$, or as two separate simplifications, depending on whether $n$ is even or odd.) The relation can be applied to $a^i$ for all $i \geq 2$. The result can be simplified again and the process repeated until the variable $a$ appears only linearly. We say that a polynomial that has been simplified in this way is *$a$-simplified*. For example, the $a$-simplified form of the first row of $U^2$ is

$$\left((-1)^n - ab + 2b^2,\ 2ab + b^2\right).$$

The $a$-simplified form of the first row of $U^3$ is

$$\left((-1)^n a - (-1)^n b + 5ab^2,\ 3(-1)^n b + 5b^3\right).$$

These give other reduction formulas for Fibonacci numbers:

$$F_{2n-1} = (-1)^n + F_n(2F_n - F_{n-1}), \quad F_{2n} = F_n(2F_{n-1} + F_n),$$
$$F_{3n-1} = (-1)^n(F_{n-1} - F_n) + 5F_{n-1}F_n^2, \quad F_{3n} = 3(-1)^n F_n + 5F_n^3.$$

These formulas are simpler because of the reduction that took place. In fact, since these $a$-simplified formulas have few multiplications, they are useful for very rapid computation of large Fibonacci numbers, see [5]. Consider one more example as a preview. The first row of $U^6$, $a$-simplified, then written in a special way, and with $n = 0$ is:

$$\left(1 + b(3+5b^2)\left(-(a(1+5b^2)) + b(7+10b^2)\right),\ b(2a+b)(1+5b^2)(3+5b^2)\right)$$

This is interesting because, when reduced modulo any factor of $b(3+5b^2)$, this is congruent to $(1, 0)$. This leads to repetition of the Fibonacci sequence at this stage modulo that factor.

These $a$-simplified formulas can be computed directly by raising $U$ to the appropriate power and applying identity $(*)$ repeatedly, but in the next section we see that they can be computed quickly using simple recursive formulas. Properties of these $a$-simplified polynomials are established. In the last section, we use the special form of these $a$-simplified reduction formulas to see that for many infinite families of moduli, the Fibonacci sequence reduced by that modulus has a short period.

## PARAMETRIZING THE $a$-SIMPLIFIED REDUCTION FORMULAS

We begin by defining the following intertwined polynomials in one variable $b$ and with the parameter $n$ giving a choice of sign. Only even indices are used for later convenience.

$$\begin{cases} R_0 = 0,\ R_2 = 1,\ R_{2j} = S_{2j-2} + (-1)^n R_{2j-4} & \text{for } j \geq 2, \\ S_0 = 2,\ S_2 = 1,\ S_{2j} = 5b^2 R_{2j-2} + (-1)^n S_{2j-4} & \text{for } j \geq 2. \end{cases} \tag{$**$}$$

Of course, this gives two sequences of polynomials, one sequence for odd $n$, the other for $n$ even. Let $R_{2j}^0$ designate the sequence when $n$ is even and $R_{2j}^1$ designate the sequence when $n$ is odd.

***Lemma 1:***

***(i)*** The polynomials $R_{2j}$ and $S_{2j}$ only include even degree terms.

***(ii)*** $\deg(R_{4j-2}) = 2j-2,\ \deg(S_{4j-2}) = 2j-2,$

***(iii)*** $\deg(R_{4j}) = 2j-2,\ \deg(S_{4j}) = 2j.$

***(iv)*** The polynomial $R_{2j}^0$ has positive coefficients and $R_{2j}^1$ is identical except that every other even degree coefficient, beginning with the second highest, is the opposite of the corresponding coefficient of $R_{2j}^0$

***(v)*** The polynomial $S_{2j}^0$ has positive coefficients and $S_{2j}^1$ is identical except that every other even degree coefficient, beginning with the second highest, is the opposite of the corresponding coefficient of $S_{2j}^0$ .

***Proof:*** (i) This is true for $j = 0$ and $j = 1$ and is preserved by the recursive definitions in $(**)$.

(ii) and (iii) These are true for $j = 0, 1$. [Notice that $\deg(R_0) = -2$ is an acceptable convention since $R_0 = 0 = 0b^{-2}$.] Checking the induction step for the four cases is direct:

$$\begin{aligned} \deg(R_{4j+2}) &= \deg(S_{4j} + (-1)^n R_{4j-2}) = \max(2j, 2j-2) = 2j, \\ \deg(S_{4j+2}) &= \deg(5b^2 R_{4j} + (-1)^n S_{4j-2}) = \max(2+2j-2, 2j-2) = 2j, \\ \deg(R_{4j+4}) &= \deg(S_{4j+2} + (-1)^n R_{4j}) = \max(2j, 2j-2) = 2j, \\ \deg(S_{4j+4}) &= \deg(5b^2 R_{4j+2} + (-1)^n S_{4j}) = \max(2+2j, 2j) = 2j+2. \end{aligned}$$

Notice that in each case the highest-order term does not involve $(-1)^n$ so that the highest coefficients are positive and there is no possibility of cancellation.

(iv) and (v) First we claim that $R_{2j}$ and $S_{2j}$ are homogeneous in the expressions $b^2$ and $(-1)^n$. The claim is true when $j = 0$ and $j = 1$. By parts (ii) and (iii) $\deg(R_{2j}) = \deg(S_{2j-2})$ and $\deg(S_{2j}) = 2 + \deg(R_{2j-2})$, thus, this homogeneity is preserved by the recursive definitions in $(**)$; hence, the claim is true. As noted above, the highest terms of $R_{2j}$ and $S_{2j}$ do not involve any powers of $(-1)^n$; by the claim, each term with lower powers of $b^2$ will have complementary powers of $(-1)^n$; hence, the alternation of signs when $n$ is odd. □

As an example, $S_{12} = 2(-1)^{3n} + 45(-1)^{2n}b^2 + 150(-1)^n b^4 + 125b^6$ has degree 6 and $S_{12}^0 = 2 + 45b^2 - 150b^4 + 125b^6$. Table 1 contains the first few $R_{2j}^0$ and $S_{2j}^0$ polynomials.

***Lemma 2:*** For $j \geq 1$,

***(i)*** $R_{2j+2}S_{2j-2} - R_{2j}S_{2j} = (-1)^{(j-1)n}$,

***(ii)*** $R_{2j-2}S_{2j+2} - R_{2j}S_{2j} = -(-1)^{(j-1)n}$.

***Proof:*** We prove (i) and (ii) simultaneously by induction. When $j = 1$, $R_4S_0 - R_2S_2 = 1\cdot 2 - 1\cdot 1 = (-1)^{0\cdot n}$ and $R_0S_4 - R_2S_2 = 0\cdot S_4 - 1\cdot 1 = -(-1)^{0\cdot n}$. Assuming (i) and (ii) hold for $j$, we see:

$$\begin{aligned} R_{2j+4}S_{2j} - R_{2j+2}S_{2j+2} &= (S_{2j+2} + (-1)^n R_{2j})S_{2j} - (S_{2j} + (-1)^n R_{2j-2})S_{2j+2}, \text{ by def.} \\ &= (-1)^n (R_{2j}S_{2j} - R_{2j-2}S_{2j+2}) = (-1)^{jn} \end{aligned}$$

using the induction hypothesis about part (ii). This completes the induction step of part (i). The induction step for part (ii) can be handled in a similar manner. □

**TABLE 1. The Polynomials $R_{2j}^0$ and $S_{2j}^0$ for Small $j$**

| | |
|---|---|
| $R_0^0 = 0 = 0b^{-2}$ | $S_0^0 = 2$ |
| $R_2^0 = 1$ | $S_2^0 = 1$ |
| $R_4^0 = 1$ | $S_4^0 = 2 + 5b^2$ |
| $R_6^0 = 3 + 5b^2$ | $S_6^0 = 1 + 5b^2$ |
| $R_8^0 = 2 + 5b^2 + 25b^4$ | $S_8^0 = 2 + 20b^2 + 25b^4$ |
| $R_{10}^0 = 5 + 25b^2 = 5(1 + 5b^2 + 5b^4)$ | $S_{10}^0 = 1 + 15b^2 + 25b^4$ |
| $R_{12}^0 = 3 + 20b^2 + 25b^4 = (1 + 5b^2)(3 + 5b^2)$ | $S_{12}^0 = 2 + 45b^2 + 150b^4 + 125b^6 = (2 + 5b^2)(1 + 20b^2 + 25b^4)$ |
| $R_{14}^0 = 7 + 70b^2 + 125b^4 + 125b^6$ | $S_{14}^0 = 1 + 30b^2 + 125b^4 + 125b^6$ |
| $R_{16}^0 = 4 + 50b^2 + 150b^4 + 125b^6 = (2 + 5b^2)(2 + 20b^2 + 25b^4)$ | $S_{16}^0 = 2 + 80b^2 + 500b^4 + 1000b^6 + 625b^8$ |
| $R_{18}^0 = 9 + 150b^2 + 675b^4 + 1125b^6 + 625b^8$ | $S_{18}^0 = 1 + 50b^2 + 375b^4 + 875b^6 + 625b^8$ |
| $= (3 + 5b^2)(3 + 45b^2 + 150b^4 + 125b^6)$ | $= (1 + 5b^2)(1 + 45b^2 + 150b^4 + 125b^6)$ |
| $R_{20}^0 = 5 + 100b^2 + 525b^4 + 1000b^6 + 625b^8$ | $S_{20}^0 = 2 + 125b^2 + 1250b^4 + 4375b^6 + 6250b^8 + 3125b^{10}$ |
| $= 5(1 + 5b^2 + 5b^4)(1 + 15b^2 + 25b^4)$ | $= (2 + 5b^2)(1 + 60b^2 + 475b^4 + 1000b^6 + 625b^8)$ |

We are now able to parametrize the $a$-simplified formulas for the powers of $U$ in terms of these polynomials.

***Theorem 3:*** For $j \geq 1$, define the following vector with entries that are polynomials in $a$ and $b$ (linear in $a$) and which includes the parity parameter $n$:

$$v(j) = \left((-1)^{jn} + bR_{2j}\left(-aS_{2j} + b(5(-1)^n R_{2j-2} + 2S_{2j})\right), b(2a+b)R_{2j}S_{2j}\right).$$

The first row of $U^{2j}$ after being $a$-simplified is given by $v(j)$.

***Proof:***

$$\begin{aligned} v(1) &= \left((-1)^n + bR_2\left(-aS_2 + b(5(-1)^n R_0 + 2S_2)\right), b(2a+b)R_2S_2\right) \\ &= \left((-1)^n - ab + 2b^2, 2ab + b^2\right) \end{aligned}$$

as required.

Assuming this is true for $j$, we want to show it for $j+1$; i.e., we need to show that the $a$-simplified form of $v(j)U^2$ is $v(j+1)$.

The second component of the $a$-simplified form of $v(j)U^2$ is obtained by multiplying $v(j)$ times the $a$-simplified form of the second column of $U^2$:

$$v(j)\cdot\left(b(2a+b),(-1)^n+ab+3b^2\right)=b(2a+b)\left((-1)^{jn}+5(-1)^n b^2 R_{2j}R_{2j-2}+(-1)^n R_{2j}S_{2j}+5b^2R_{2j}S_{2j}\right)$$
$$=b(2a+b)\left(5b^2R_{2j}\left((-1)^n R_{2j-2}+S_{2j}\right)+(-1)^n R_{2j+2}S_{2j-2}\right)$$

using $(-1)^{(j-1)n}+R_{2j}S_{2j}=R_{2j+2}S_{2j-2}$ from Lemma 2(i). Then using the recursive definitions of $R_{2j+2}$ and then $S_{2j+2}$, we see the above is $b(2a+b)R_{2j+2}S_{2j+2}$ as required.

The first component of the $a$-simplified form of $v(j)U^2$ can be shown to be the first component of $v(j+1)$ in a straightforward, but more tedious, manner. However, it is convenient to first simplify the identity required for the first component using the identity obtained above for the second component. We leave the details for the reader. □

As an example, consider $j=4$. By Theorem 3 we see the first row of $U^8$ after being $a$-simplified is:

$$\left((-1)^{4n}+bR_8\left((2b-a)S_8+5b(-1)^n R_6\right),b(2a+b)R_8S_8\right)$$

where $R_6=3(-1)^n+5b^2$, $R_8=2(-1)^n+5b^2$, and $S_8=2(-1)^{2n}+20(-1)^n b^2+25b^4$ as can be seen from Table 1 and Lemma 1. Now letting $a=F_{n-1}$ and $b=F_n$, we get

$$F_{8n-1}=1+F_n\left(2(-1)^n+5F_n^2\right)\left((2F_n-F_{n-1})\left(2+20(-1)^nF_n^2+25F_n^4\right)+5F_n(-1)^n\left(3(-1)^n+5F_n^2\right)\right)$$

and

$$F_{8n}=F_n(2F_{n-1}+F_n)\left(2(-1)^n+5F_n^2\right)\left(2+20(-1)^nF_n^2+25F_n^4\right).$$

In particular, when $n=3$, we have $F_3=2$, $F_2=1$, so

$$F_{23}=1+2(-2+20)\left((4-1)(2-80+400)-10(-3+20)\right)=28657$$

and

$$F_{24}=2(4)(-2+20)(2-80+400)=46368,$$

which are correct.

***Corollary 4:*** Let $j\geq 1$. The first row of $U^{2j+1}$ after being $a$-simplified is given by

$$\left((-1)^{jn}a-(-1)^n bR_{2j}S_{2j}+5ab^2R_{2j}R_{2j+2},\right.$$
$$\left.(-1)^{jn}b+2(-1)^n bR_{2j}S_{2j}+5b^3R_{2j}R_{2j+2}\right).$$

***Proof:*** Multiplying out $v(j)U$ and reducing $a^2$ by $(*)$ gives

$$\Big((-1)^{jn}a-(-1)^n bR_{2j}S_{2j}+5(-1)^n ab^2R_{2j}R_{2j-2}+5ab^2R_{2j}S_{2j},$$
$$(-1)^{jn}b+2(-1)^n bR_{2j}S_{2j}+5(-1)^n b^3R_{2j}R_{2j-2}+5b^3R_{2j}S_{2j}\Big).$$

The recursive definition for $R_{2j+2}$ simplifies that into the desired result. □

Notice in particular that the second component depends on $b$ but not on $a$. Thus, we get a formula for $F_{(2j+1)n}$ in terms of $F_n$ alone. As an example, consider $j = 3$. Corollary 4 gives the $a$-simplified form of the first row of $U^7$ as:

$$\Big(-(-1)^n bR_6S_6+a\big((-1)^{3n}+5b^2R_6R_8\big),\ (-1)^{3n}b+bR_6\big(2(-1)^n S_6+5b^2R_8\big)\Big)$$
$$=\Big(-3(-1)^{3n}b-20(-1)^{2n}b^3-25(-1)^n b^5+a\big((-1)^{3n}+30(-1)^{2n}b^2+125(-1)^n b^4+125b^6\big),$$
$$7(-1)^{3n}b+70(-1)^{2n}b^3+175(-1)^n b^5+125b^7\Big).$$

So, if $n$ is even, $a = F_{n-1}$, and $b = F_n$, we see:

$$F_{7n-1} = -3F_n-20F_n^3-25F_n^5+F_{n-1}(1+30F_n^2+125F_n^4+125F_n^6),$$
$$F_{7n} = 7F_n+70F_n^3+175F_n^5+125F_n^7.$$

In particular, if $n = 2$, $F_{n-1} = F_1 = 1$ and $F_n = F_2 = 1$, so

$$F_{13} = -3-20-25+1+30+125+125 = 233$$

and

$$F_{14} = 7+70+175+125 = 377$$

as is easy to check. Of course, there are similar formulas when $n$ is odd.

## SHORT PERIODS MODULO $M$

As noted earlier, it is well known that the Fibonacci sequence is purely periodic when reduced modulo an integer $m$. We write $k = k(m)$ to designate the period of the Fibonacci sequence modulo $m$. For example, consider the Fibonacci sequence and its residues modulo eight:

| | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 1 | 1 | 2 | 3 | 5 | 8 | 13 | 21 | 34 | 55 | 89 | 144 | 233 | 377 | 610 | 987 |
| 0 | 1 | 1 | 2 | 3 | 5 | 0 | 5 | 5 | 2 | 7 | 1 | 0 | 1 | 1 | 2 | 3 |

The repetition of the 0–1 pair at $F_{12}$–$F_{13}$ guarantees that the sequence modulo eight will repeat. Therefore, $k(8) = 12$. In general, we have

***Lemma 5:*** The period $k = k(m)$ is the smallest positive number such that $F_k \equiv 0 \pmod{m}$ and $F_{k+1} \equiv 1 \pmod{m}$.

***Proof:*** By definition, $k$ is the smallest positive integer such that $F_{k+n} \equiv F_n$ for all $n \geq 0$. It is clear that this implies $F_k \equiv F_0 = 0$ and $F_{k+1} \equiv F_1 = 1$. If there is any other occurrence of these congruences, namely, $F_j \equiv 0 = F_0$ and $F_{j+1} \equiv 1 = F_1$, then by adding those equation we see $F_{j+2} \equiv F_2$ and by induction $F_{j+n} \equiv F_n$ for all $n \geq 0$. Thus, $j \geq k$ by the definition of $k$, and we see that $k$ is the smallest positive number satisfying the desired congruences. □

***Lemma 6:*** If $F_c \equiv 0$ and $F_{c+1} \equiv 1$ modulo $m$, then $k(m)|c$.

***Proof:*** We can write $c = qk(m) + r$ where $0 \leq r < k(m)$. Now $F_{k+n} \equiv F_n$ modulo $m$ implies that we can add multiples of $k(m)$ to the index and get a congruent number: $0 = F_c \equiv F_{c-qk(m)} = F_r$ and $1 = F_{c+1} \equiv F_{c+1-qk(m)} = F_{r+1}$. Since $r < k(m)$, we know by the previous lemma that $r = 0$. Hence, $c = qk(m)$ and so $k(m)$ divides $c$. □

The next theorems give techniques for generating many infinite families of moduli $m$ with very small periods modulo $m$. The examples all have period bounded by a constant times the logarithm of the modulus. Ehrlich [4] showed that to be the case for the Fibonacci moduli; these would be given by the families below with trivial choice of $g(b) = b$.

***Theorem 7:*** Let $n$ be even and $g(b)$ be any polynomial that divides $bR^0_{2j}(b)$ and let $m = g(F_n)$ and $k = k(m)$. Then $k$ divides $2jn$.

***Proof:*** If we let $a = F_{n-1}$ and $b = F_n$ in Theorem 3, we see that since all the terms of $v(j)$ are divisible by $bR^0_{2j}(b)$ except the term $(-1)^{jn}$, we get

$$\begin{aligned}(F_{2jn-1}, F_{2jn}) = v(j) &\equiv \left((-1)^{jn}, 0\right) \mod m \\ &= (1, 0) \text{ since } n \text{ is even.}\end{aligned}$$

Thus, $F_{2jn} \equiv 0$ and $F_{2jn+1} \equiv 1$; thus, $k$ divides $2jn$ by Lemma 6. □

***Theorem 8:*** Let $n$ be odd and $g(b)$ be any polynomial that divides $bR^1_{2j}(b)$ and let $m = g(F_n)$ and $k = k(m)$. Then

***(i)*** if $j$ is even, $k$ divides $2jn$;

***(ii)*** if $j$ is odd, then $k$ divides $4jn$.

***Proof:*** Again we let $a = F_{n-1}$ and $b = F_n$ in Theorem 3 to get

$$(F_{2jn-1}, F_{2jn}) = v(j) \equiv \left((-1)^{jn}, 0\right) \mod m.$$

***(i)*** If $j$ is even, then this is (1, 0); thus, $F_{2jn} \equiv 0$ and $F_{2jn-1} \equiv F_{2jn+1} \equiv 1$; hence, $k$ divides $2jn$ by Lemma 6.

***(ii)*** If $j$ is odd, then this is (-1, 0); thus, $F_{2jn} \equiv 0$ and $F_{2jn-1} \equiv 1$. In the first section we saw identities $F_{2s-1} = F^2_{s-1} + F^2_s$ and $F_{2s} = 2F_{s-1}F_s + F^2_s$, with $s = 2jn$ we see $F_{4jn-1} \equiv (-1)^2 + 0^2 = 1$ and $F_{4jn} \equiv 0$. So $F_{4jn+1} \equiv 1$ and $k$ divides $4jn$ by Lemma 6. □

Since $m$ is exponential in $n$ (becasue the Fibonacci numbers are), these theorems give examples where the periods are bounded above by a constant times the logarithm of the modulus. Lower bounds will be considered after considering some examples.

Table 2 shows the periods for moduli generated by taking $g(b) = bR_6^1(b)$ with $n$ odd. Table 3 gives periods for even $n$ for the corresponding polynomial.

Table 4 gives the periods for moduli near 196400. This gives some idea of how small the period $k(196418) = 108$ that also appears in Table 2 is relative to "typical" values.

**TABLE 2. Periods for Moduli Generated with $g(b) = bR_6^1(b)$**

| $n$ | $F_n$ | $m = g(F_n)$ | $k(m)$ |
|---|---|---|---|
| 1 | 1 | 2 | 3* |
| 3 | 2 | 34 | 36 |
| 5 | 5 | 610 | 60 |
| 7 | 13 | 10946 | 84 |
| 9 | 34 | 196418 | 108 |
| 11 | 89 | 3524578 | 132 |
| 13 | 233 | 63245986 | 156 |
| 15 | 610 | 1134903170 | 180 |
| 17 | 1597 | 20365011074 | 204 |
| 19 | 4181 | 365435296162 | 228 |

* Period is less than the maximum allowed by the theorems.

**TABLE 3. Periods for Moduli Generated with $g(b) = bR_6^0(b)$**

| $n$ | $F_n$ | $m = g(F_n)$ | $k(m)$ |
|---|---|---|---|
| 2 | 1 | 8 | 12 |
| 4 | 3 | 144 | 24 |
| 6 | 8 | 2584 | 36 |
| 8 | 21 | 46368 | 48 |
| 10 | 55 | 832040 | 60 |
| 12 | 144 | 14930352 | 72 |
| 14 | 377 | 267914296 | 84 |
| 16 | 987 | 4807526976 | 96 |
| 18 | 2584 | 86267571272 | 108 |
| 20 | 6765 | 1548008755920 | 120 |

**TABLE 4. Some Periods Near 196400**

| $m$ | $k(m)$ | $m$ | $k(m)$ |
|---|---|---|---|
| 196400 | 29400 | 196413 | 352 |
| 196401 | 27720 | 196414 | 196416 |
| 196402 | 49416 | 196415 | 9840 |
| 196403 | 62028 | 196416 | 480 |
| 196404 | 105672 | 196417 | 364 |
| 196405 | 340 | 196418 | 108 |
| 196406 | 56112 | 196419 | 728 |
| 196407 | 43608 | 196420 | 240 |
| 196408 | 147300 | 196421 | 99216 |
| 196409 | 197604 | 196422 | 31032 |
| 196410 | 196440 | 196423 | 704 |
| 196411 | 12064 | 196424 | 25080 |
| 196412 | 98208 | 196425 | 264600 |

Table 5 gives periods for $g(b) = R_{10}^0(b)$ with $n$ even. These moduli get large quickly while the periods stay small. Table 6 gives values for a nontrivial divisor of $bR_{12}$.

**TABLE 5. Periods for Moduli Generated with $g(b) = R_{10}^0(b)$**

| $n$ | $F_n$ | $m = g(F_n)$ | $k(m)$ |
|---|---|---|---|
| 2 | 1 | 55 | 20 |
| 4 | 3 | 2255 | 40 |
| 6 | 8 | 104005 | 60 |
| 8 | 21 | 4873055 | 80 |
| 10 | 55 | 228841255 | 100 |
| 12 | 89 | 10750060805 | 120 |
| 14 | 377 | 505019869255 | 140 |
| 16 | 987 | 23725155368255 | 160 |

**TABLE 6. Periods for Moduli Generated with a Factor of $bR_{12}^1(b)$: $g(b) = -b + 5b^3$**

| $n$ | $F_n$ | $m = g(F_n)$ | $k(m)$ |
|---|---|---|---|
| 1 | 1 | 4 | 6* |
| 3 | 2 | 38 | 18* |
| 5 | 5 | 620 | 60 |
| 7 | 13 | 10972 | 84 |
| 9 | 34 | 196486 | 108 |
| 11 | 89 | 3524756 | 132 |
| 13 | 233 | 63246452 | 156 |
| 15 | 610 | 1134904390 | 180 |

Notice that in these examples the periods $k(m)$ were exactly the quantity that Theorems 7 and 8 give as a multiple of the period except for a few small moduli in Table 2 and Table 6. In general, it appears that the bounds given in the theorems are met for sufficiently large $n$. While we cannot prove such a theorem, we can show that the periods cannot be much smaller than the given period for sufficiently large $n$ for the full polynomial factors.

***Lemma 9:*** Let $\tau$ be the golden ratio, then for $n \geq 1$ we have: $\tau^{n-2} \leq F_n \leq \tau^{n-1}$.

***Proof:*** The theorem is true for $n = 1$ and $n = 2$ by direct computation: $\tau^{-1} < F_1 = 1 = \tau^0$, $\tau^0 = F_2 = 1 < \tau$. If it is true for $n$ and $n-1$, we can add inequalities to get:

$$\tau^{n-3} + \tau^{n-2} \leq F_{n-1} + F_n \leq \tau^{n-2} + \tau^{n-1}.$$

This simplifies to $\tau^{n-1} \leq F_{n+1} \leq \tau^n$, using $\tau^2 = \tau + 1$, completing the induction. □

In Lemma 9, notice that strict inequality must hold for $n \geq 3$ since $F_n$ is an integer.

***Lemma 10:*** Let $m \geq 2$ be a modulus and $\tau$ the golden ratio, then $k(m) > \frac{\log(m)}{\log(\tau)}$.

***Proof:*** We can pick $n$ so that $\tau^{n-1} < m < \tau^n$. Since $F_n < \tau^{n-1}$ it is not possible for $F_j$ to be reduced to zero modulo $m$ for any $j \leq n$. Therefore, $k(m) > n$. However, $m < \tau^n$ implies $n > \log(m)/\log(\tau)$ and, hence, the conclusion. □

While the upper bounds on $k(m)$ given in Theorems 7 and 8 are $2jn$ or $4jn$, we can show that for sufficiently large $n$ that $k(m)$ is not many factors smaller than those bounds. However, we conjecture that equality holds for sufficiently large $n$.

***Theorem 11:*** Suppose $g(b)$ is $R_{2j}^e(b)$ or $bR_{2j}^e(b)$ with $j \geq 3$ where $e$ is 0 or 1. Also let $m = g(F_n)$ where $n$ has the same parity as $e$ and let $k = k(m)$. Then $k(m) > 0.3jn$ for sufficiently large $n$.

***Proof:*** In Lemma 1 and Table 1 we see the highest-order term of $R_{2j}^e(b)$ is at least five times $b^{j-1}$ or $b^{j-2}$. Therefore, for sufficiently large $n$, $m > F_n^{j-2}$. From that inequality and Lemmas 9 and 10, we see that, for sufficiently large $n$,

$$k(m) > \frac{\log(m)}{\log(\tau)} > \frac{(j-2)\log(F_n)}{\log(\tau)} > (j-2)(n-2) \geq \frac{3}{10} jn,$$

since $(j-2)/j \geq 1/3$ and $(n-2)/n \geq 18/20$ for $n \geq 20$. □

## REFERENCES


1. Brother U. Alfred. *An Introduction to Fibonacci Discovery.* Santa Clara, Calif: The Fibonacci Association, 1965.
2. R. A. Bateman, E. A. Clark, M. L. Hancock, & C. A. Reiter. "The Period of Convergents Modulo *M* of Reduced Quadratic Irrationals." *Fibonacci Quarterly* **29.3** (1991):220-29.
3. Leonard Eugene Dickson. *History of the Theory of Numbers.* 1919; rpt. Chelsea, 1971.
4. Amos Ehrlich. "On the Periods of the Fibonacci Sequence Modulo *M*." *Fibonacci Quarterly* **27.1** (1989):11-13.
5. Roman E. Maeder. "Fibonacci on the Fast Track." *Math. J.* **1.3** (1991):42-46.
6. John Vinson. "The Relation of the Period Modulo to the Rank of Apparition of *m* in the Fibonacci Sequence." *Fibonacci Quarterly* **1.1** (1963):37-46.
7. D. D. Wall. "Fibonacci Series Modulo *m*." *Amer. Math. Monthly* **67** (1960):525-32.


AMS number: 11B39

❖❖❖