

LOWER BOUND FOR THE PERIOD OF THE FIBONACCI SERIES MODULO M

PAUL A. CATLIN
Ohio State University, Columbus, Ohio 43210

**A REPRINT
FROM**

THE FIBONACCI QUARTERLY

VOLUME 12

NUMBER 4

DECEMBER

1974

A LOWER BOUND FOR THE PERIOD OF THE FIBONACCI SERIES MODULO M

PAUL A. CATLIN
Ohio State University, Columbus, Ohio 43210

In this note we shall determine a nontrivial lower bound for the period of the Fibonacci series modulo m . This problem was posed by D. D. Wall [2], p. 529.

Let $a(m)$ denote the subscript of the first term of the Fibonacci series

$$(1) \quad F_{n+2} = F_{n+1} + F_n, \quad F_0 = 0, \quad F_1 = 1,$$

which is divisible by m . Let $k(m)$ denote the period of $\{F_n\}$ modulo m . Define the sequence $\{L_n\}$ so that

$$(2) \quad L_{n+2} = L_{n+1} + L_n, \quad L_0 = 2, \quad L_1 = 1.$$

Then our main result is the following theorem:

Theorem. Let t be any natural number such that $L_t \leq m$, where $m > 2$. Then $k(m) \geq 2t$, with equality if and only if $L_t = m$ and t is odd.

Wall posed the question for prime values of m . It is not known whether or not there are infinitely many prime m such that $L_t = m$ when t is odd.

For the proof of the theorem we need some preliminary results. The following theorem is proved in [1] (Th. 3).

Vinson's Theorem. Let m be any integer greater than 2. If $a(m)$ is odd, then $k(m) = 4a(m)$; if $a(m)$ is even and $a(p) \equiv 2 \pmod{4}$ for all odd prime divisors of m , then $k(m) = a(m)$; in any other case, $k(m) = 2a(m)$.

In addition to well known identities, the following is useful:

$$(3) \quad F_i \equiv -(-1)^i F_{k(m)-i} \pmod{m}.$$

Equation (3) follows by induction on i , using (1), $F_0 \equiv F_{k(m)} \equiv 0$, and $F_1 \equiv F_{k(m)+1} \equiv 1 \pmod{m}$.

Lemma. $k(L_n) = 4n$ when n is even; $k(L_n) = 2n$ when n is odd.

Proof: $a(L_n) = 2n$ is known, and may be proved using $F_{2n} = F_n L_n$, $F_t < L_n$ for $t \leq n+1$, and the fact that subscripts n for which $m \mid U_n$ form an ideal. The lemma follows by an application of Vinson's theorem.

Proof of Theorem: It is known [2] that $k(m)$ is even. Using the identities (3) and

$$(4) \quad L_n = F_{n-1} + F_{n+1},$$

we see that if $k(m) = 2t$ then $F_t \equiv -(-1)^t F_t \pmod{m}$, so t is odd or $F_t \equiv 0 \pmod{m}$. If t is odd then by (3) we have $F_{t+1} \equiv -F_{t-1} \pmod{m}$ implying (by (4)) that

$$(5) \quad L_t \equiv F_{t+1} + F_{t-1} \equiv 0 \pmod{m}.$$

Otherwise, if $F_t \equiv 0 \pmod{m}$ then by (1),

$$(6) \quad F_{t+1} - F_{t-1} \equiv 0 \pmod{m}.$$

Clearly, if $t \leq n$ then

$$(7) \quad 0 < F_{t+1} + F_{t-1} \leq F_{n+1} + F_{n-1} = L_n \leq m,$$

by the hypothesis of the theorem. By (4)

$$F_{t+1} - F_{t-1} = 2F_{t+1} - L_t,$$

and since $m \geq L_t > F_{t+1}$ when $t \leq n$, we have

$$(8) \quad F_{t+1} - F_{t-1} < m.$$

Now, (5) and (7) imply that $t = n$ and $L_t = m$, and (6) and (8) are never simultaneously true. Thus $t \geq n$, with equality only if $L_n = m$. By the lemma,

$$k(m) = 2t = 2n$$

if and only if n and t are odd and $L_n = m$. The conclusion of the theorem follows.

REFERENCES

1. John Vinson, "The Relation of the Period Modulo m to the Rank of Apparition of m in the Fibonacci Sequence," *The Fibonacci Quarterly*, Vol. 1, No. 2 (April, 1963), pp. 37-45.
2. D.D. Wall, "Fibonacci Series Modulo m ," *Amer. Math. Monthly*, 67 (1960), pp. 525-532.

★★★★★

[Continued from page 348.]

$$H_k(x) = \sum_{n=0}^{\infty} H_n^k x^n \quad (H_k(0) = (H_0)^k = r^k),$$

where

$$H_0(x) = f_0(x) = \sum_{n=0}^{\infty} x^n = (1-x)^{-1}$$

and

$$H_1(x) = (r+sx)(1-x-x^2)^{-1}$$

are

$$(2) \quad \left\{ \begin{array}{l} (1-3x+x^2)H_2(x) = r^2 - s^2x - 2exH_0(-x) \\ (1-4x-x^2)H_3(x) = r^3 + s^3x - 3exH_1(-x) \\ (1-7x+x^2)H_4(x) = r^4 - s^4x + 2e^2xH_0(x) - 8exH_2(-x) \\ (1-11x-x^2)H_5(x) = r^5 + s^5x + 5e^2xH_1(x) - 15exH_3(-x) \end{array} \right.$$

The general expression for the generating function is (see [3])

$$(3) \quad (1 - a_k x + (-1)^k x^2) H_k(x) = r^k - (-s)^k x + kx \sum_{j=1}^{[k/2]} \frac{(-1)^j}{j} e^j a_{kj} H_{k-2j}((-1)^j x),$$

where

$$(1-x-x^2)^{-j} = \sum_{k=2j}^{\infty} a_{kj} x^{k-2j},$$

that is, a_{kj} are generated by the j^{th} power of the generating function for Fibonacci numbers f_n . Note the occurrence in (3) of the Lucas numbers a_n .

FUNCTIONS ASSOCIATED WITH THE GENERATING FUNCTIONS

In the process of obtaining (3), we use

$$(4) \quad g_k(x) = \sqrt{5} H_k(x) = \sum_{j=0}^{[k/2]} \binom{k}{j} e^j F_{k-2j}((-1)^j x) \quad (F_0(x) = H_0(x)),$$

where

$$F_k(x) = [(r-sb)a]^k (1-a^k x)^{-1} + [(sa-r)b]^k (1-b^k x)^{-1} \quad (k = 1, 2, 3, \dots)$$

and

$$a = \frac{1+\sqrt{5}}{2}, \quad b = \frac{1-\sqrt{5}}{2} \quad (a, b \text{ roots of } x^2 - x - 1 = 0),$$

leading to the general inverse

[Continued on page 354.]