ON THE EXISTENCE OF THE RANK OF APPARITION OF m IN THE LUCAS SEQUENCE

JAMES E. DESMOND
Pensacola Junior College, Pensacola, Florida 32504

Let m be an arbitrary positive integer. According to the notation of Vinson [1, p. 37] let $s(m)$ denote the period of F_n modulo m and let $f(m)$ denote the rank of apparition of m in F_n.

It is easily verified that

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

for all integers n.

In the sequel we shall use, without explicit reference, the well known facts that

$$F_{2n} = F_n L_n ,$$

and that F_n and L_n are both odd or both even and

$$(F_n, L_n) = d \leqslant 2, \quad \text{and} \quad F_m \mid F_{mn}$$

for all integers n and $m \neq 0$.

Lemma 1. $F_{2n} \equiv 0 \pmod m$ and $F_{2n+1} \equiv (-1)^n \pmod m$ if and only if $F_n \equiv 0 \pmod m$.

Proof. Let $F_{2n} \equiv 0 \pmod m$ and $F_{2n+1} \equiv (-1)^n \pmod m$. Then by (1), $F_n L_{n+1} \equiv 0 \pmod m$. Since $F_{2n} = F_n L_n \equiv 0 \pmod m$, we have

$$F_n L_{n+2} = F_n L_{n+1} + F_n L_n \equiv 0 \equiv F_n L_{n+1} - F_n L_n = F_n L_{n-1} \pmod m .$$

So whether n is negative or non-negative we obtain after finitely many steps that $F_n L_1 = F_n \equiv 0 \pmod m$.

Conversely, let $F_n \equiv 0 \pmod m$. Then $F_{2n} = F_n L_n \equiv 0 \pmod m$ and by (1), $F_{2n+1} \equiv (-1)^n \pmod m$.

Lemma 2. $F_{2n} \equiv 0 \pmod m$ and $F_{2n+1} \equiv (-1)^{n+1} \pmod m$ if and only if $L_n \equiv 0 \pmod m$.

Proof. Analogous to the proof of Lemma 1.

The following lemma can be found in Wall [2, p. 526]. We give an alternative proof.

Lemma 3. If $m > 2$, then $s(m)$ is even.

Proof. Suppose $s(m)$ is odd. We have by definition of $s(m)$ that

$$F_{2s(m)+1} = F_{s(m)+s(m)+1} \equiv F_{s(m)+1} \equiv 1 = (-1)^{s(m)+1} \pmod m .$$

Also

$$F_{2s(m)} = F_{s(m)} L_{s(m)} \equiv 0 \pmod m .$$

Therefore by Lemma 2, $L_{s(m)} \equiv 0 \pmod m$. But

$$(F_{s(m)}, L_{s(m)}) = d \leqslant 2$$

which contradicts the fact that $m > 2$.

An equivalent form of the following theorem, but with a different proof can be found in Vinson [1, p. 42].

Theorem 1. We have

i) $m > 2$ and $f(m)$ is odd if and only if $s(m) = 4f(m)$
ii) $m = 1$ or 2 or $s(m)/2$ is odd if and only if $s(m) = f(m)$
iii) $f(m)$ is even and $s(m)/2$ is even if and only if $s(m) = 2f(m)$.

Proof. We first prove the sufficiency in each case.

Case i): Let $m > 2$ and $f(m)$ be odd. From Vinson [1, p. 37] we have $f(m)|s(m)$. Since $s(m)$ is even for $m > 2$ we know that $s(m) \neq f(m)$ and $s(m) \neq 3f(m)$. We have $F_{2f(m)} \equiv 0 \pmod m$ and by (1),

$$F_{2f(m)+1} \equiv (-1)^{f(m)} = -1 \pmod m.$$

Therefore $s(m) \neq 2f(m)$ since $m > 2$. But $F_{4f(m)} \equiv 0 \pmod m$ and by (1),

$$F_{4f(m)+1} \equiv (-1)^{2f(m)} = 1 \pmod m.$$

Therefore $s(m) = 4f(m)$.

Case ii): The conclusion is clear for $m = 1$ or 2. Let $m > 2$ and $s(m)/2$ be odd. Then by Case i), $f(m)$ is even. So $F_{2f(m)} \equiv 0 \pmod m$ and by (1),

$$F_{2f(m)+1} \equiv (-1)^{f(m)} = 1 \pmod m$$

which implies that $s(m) \leqslant 2f(m)$. $s(m) \neq 2f(m)$ since $s(m)/2$ is odd and $f(m)$ is even. Therefore since $f(m)|s(m)$, we have $s(m) = f(m)$.

Case iii): Let $f(m)$ be even and $s(m)/2$ be even. Then $m > 2$. We have $F_{2f(m)} \equiv 0 \pmod m$ and by (1),

$$F_{2f(m)+1} \equiv (-1)^{f(m)} = 1 \pmod m.$$

Therefore $s(m) \leqslant 2f(m)$. Now, $F_{s(m)} \equiv 0 \pmod m$ and $F_{s(m)+1} \equiv 1 = (-1)^{s(m)/2} \pmod m$. So by Lemma 1, $F_{s(m)/2} \equiv 0 \pmod m$. Thus $s(m) \neq f(m)$ and therefore since $f(m)|s(m)$ we have $s(m) = 2f(m)$.

The necessity in each case follows directly from the implications already proved.

The following corollary is part of a theorem by Vinson [1, p. 39].

Corollary 1. Let p be any odd prime and e any positive integer. Then we have

i). $f(p^e)$ is odd if and only if $s(p^e) = 4f(p^e)$

ii). $f(p^e)$ is even and $f(p^e)/2$ is odd if and only if $s(p^e) = f(p^e)$

iii). $f(p^e)$ is even and $f(p^e)/2$ is even if and only if $s(p^e) = 2f(p^e)$.

Proof. By Theorem 1, we need only prove that $s(p^e)/2$ is odd if and only if $f(p^e)$ is even and $f(p^e)/2$ is odd. The sufficiency is clear by Theorem 1, ii).

Conversely, let $f(p^e)$ be even and $f(p^e)/2$ be odd. Then

$$F_{f(p^e)} = F_{f(p^e)/2} L_{f(p^e)/2} \equiv 0 \pmod{p^e}.$$

Since

$$(F_{f(p^e)/2}, L_{f(p^e)/2}) = d \leqslant 2 < p$$

we have $L_{f(p^e)/2} \equiv 0 \pmod{p^e}$. Therefore by (1),

$$F_{f(p^e)+1} \equiv (-1)^{(f(p^e)/2)+1} = 1 \pmod{p^e}.$$

Thus $s(p^e) = f(p^e)$ and so $s(p^e)/2$ is odd.

Definition. If m divides some member of the Lucas sequence, let $g(m)$ denote the smallest positive integer n such that $m|L_n$.

If m divides no member of the Lucas sequence, we shall say that $g(m)$ does not exist.

From Vinson [1, p. 37] we have

(2) $$F_n \equiv 0 \pmod m \text{ if and only if } f(m)|n.$$

It is interesting to note from the following proof that if $4|f(4n)$, then $g(4n)$ does not exist.

Lemma 4. If n is an odd integer and $g(4n)$ exists, then $4|L_{f(4n)/2}$.

Proof. By observing the residues of the Lucas sequence modulo 4 we find that $4|L_{g(4n)}$ implies $g(4n) = 3 + 6k$ for some integer k. Therefore $g(4n)$ is odd. We have $4n|L_{g(4n)}|F_{2g(4n)}$. So by (2), $f(4n)|2g(4n)$. Hence $4 \nmid f(4n)$. Since $4|F_{f(4n)}$ we have by (2) that $6 = f(4)|f(4n)$. Since $f(4n)/2$ is odd and $3|f(4n)/2$ we have from Carlitz [3, p. 15] that $4 = L_3|L_{f(4n)/2}$.

Theorem 2. If $m > 2$ and $g(m)$ exists, then $2g(m) = f(m)$.

Proof. We have $m \mid L_{g(m)} \mid F_{2g(m)}$. So by (2), $f(m) \mid 2g(m)$. Suppose $f(m)$ is odd. Then $f(m) \mid g(m)$ and therefore by (2), $m \mid F_{g(m)}$. Thus $m \mid (L_{g(m)}, F_{g(m)}) = d \leqslant 2$, a contradiction since $m > 2$. Hence $f(m)$ is even.

To complete the proof it suffices to show that $m \mid L_{f(m)/2}$ which implies $g(m) = f(m)/2$. We have

$$m \mid F_{f(m)} = F_{f(m)/2} L_{f(m)/2} .$$

Let $m = m_1 m_2$ where $m_1 \mid F_{f(m)/2}$ and $m_2 \mid L_{f(m)/2}$. Since $f(m)/2 \mid g(m)$ we have $m_1 \mid F_{f(m)/2} \mid F_{g(m)}$. Therefore $m_1 \mid (F_{g(m)}, L_{g(m)}) = d \leqslant 2$. So $m_1 = 1$ or 2. If $m_1 = 1$, then $m_2 = m \mid L_{f(m)/2}$, the desired conclusion. Assume $m_1 = 2$. Then m is even. Since $2 \mid F_{f(m)/2}$ we have $2 \mid L_{f(m)/2}$. If $m_2 = m/2$ is odd, then $2m_2 = m \mid L_{f(m)/2}$, the desired conclusion. Assume $m_2 = m/2$ is even. Since $g(8)$ does not exist we know that $8 \nmid m$. Therefore $m_2/2 = m/4$ is odd. Since $g(4(m_2/2)) = g(m)$ exists we have by Lemma 4 that $4 \mid L_{f(m)/2}$. Thus $m = 4(m_2/2) \mid L_{f(m)/2}$. The proof is complete.

Corollary 2. For any odd prime p and any positive integer e, $g(p^e)$ exists if and only if $f(p^e)$ is even.

Proof. The sufficiency follows from Theorem 2 and the necessity follows from the facts $F_{2n} = F_n L_n$ and $(F_n, L_n) = d \leqslant 2 < p$ for all integers n.

Theorem 3. We have

i) $g(m)$ exists and is odd if and only if $s(m) = f(m)$
ii) $g(m)$ exists and is even if and only if $s(m) = 2f(m)$ and $F_{f(m)+1} \equiv -1 \pmod m$
iii) $g(m)$ does not exist if and only if either $s(m) = 2f(m)$ and $F_{f(m)+1} \not\equiv -1 \pmod m$ or $s(m) = 4f(m)$.

Proof. Case i): Let $g(m)$ exist and be odd. The case $m = 1$ or 2 is clear. Assume $m > 2$. By Theorem 2, $f(m) = 2g(m)$. Therefore by (1),

$$F_{f(m)+1} \equiv (-1)^{g(m)+1} = 1 \pmod m .$$

Hence $s(m) = f(m)$.

Conversely, let $s(m) = f(m)$. The case $m = 1$ or 2 is clear. Assume $m > 2$. By Theorem 1, $s(m)/2$ is odd. Therefore

$$F_{s(m)} \equiv 0 \pmod m \quad \text{and} \quad F_{s(m)+1} \equiv 1 = (-1)^{(s(m)/2)+1} \pmod m .$$

Hence by Lemma 2, $L_{s(m)/2} \equiv 0 \pmod m$ and thus $g(m)$ exists. By Theorem 2, $s(m) = f(m) = 2g(m)$. Therefore $g(m)$ is odd.

Case ii): Let $g(m)$ exist and be even. Then $m > 2$ and by Theorem 2, $f(m) = 2g(m)$. Thus $4 \mid f(m)$ and so by Theorem 1, $s(m) = 2f(m)$. By (1), $F_{f(m)+1} \equiv (-1)^{g(m)+1} = -1 \pmod m$.

Conversely, let $s(m) = 2f(m)$ and $F_{f(m)+1} \equiv -1 \pmod m$. We have $F_{f(m)} \equiv 0 \pmod m$. By Theorem 1, $m > 2$ and $f(m)$ is even. If $f(m)/2$ is odd, then $F_{f(m)+1} \equiv (-1)^{f(m)/2} \pmod m$ which implies by Lemma 1 that $F_{f(m)/2} \equiv 0 \pmod m$, a contradiction. Hence $f(m)/2$ is even. Therefore $F_{f(m)+1} \equiv (-1)^{(f(m)/2)+1} \pmod m$ which implies by Lemma 2 that $L_{f(m)/2} \equiv 0 \pmod m$. Thus $g(m)$ exists and by Theorem 2, $f(m)/2 = g(m)$ is even.

Case iii): Follows from Cases i) and ii) and from Theorem 1.

Corollary 3. For any odd prime p and any positive integer e we have

i) $g(p^e)$ exists and is odd if and only if $s(p^e) = f(p^e)$
ii) $g(p^e)$ exists and is even if and only if $s(p^e) = 2f(p^e)$
iii) $g(p^e)$ does not exist if and only if $s(p^e) = 4f(p^e)$.

Proof. In view of Theorem 3 we need only prove that $s(p^e) = 2f(p^e)$ implies $F_{f(p^e)+1} \equiv -1 \pmod{p^e}$. By Corollary 1, if $s(p^e) = 2f(p^e)$, then $f(p^e)$ is even and $f(p^e)/2$ is even. We have

$$F_{f(p^e)} = F_{f(p^e)/2} L_{f(p^e)/2} \equiv 0 \pmod{p^e} \quad \text{and} \quad (F_{f(p^e)/2}, L_{f(p^e)/2}) = d \leqslant 2 < p .$$

Therefore $L_{f(p^e)/2} \equiv 0 \pmod{p^e}$. So by (1),

$$F_{f(p^e)+1} \equiv (-1)^{(f(p^e)/2)+1} = -1 \pmod{p^e} .$$

Theorem 4. Let p be an odd prime and e be any positive integer. Then

i) $g(p^e)$ exists and is odd if $p \equiv 11$ or $19 \pmod{20}$
ii) $g(p^e)$ exists and is even if $p \equiv 3$ or $7 \pmod{20}$
iii) $g(p^e)$ does not exist if $p \equiv 13$ or $17 \pmod{20}$
iv) $g(p^e)$ is odd or does not exist if $p \equiv 21$ or $29 \pmod{40}$.

Proof. Follows from Vinson [1, p. 43] and Corollary 3.

Wall [2, p. 525] has shown that the period of L_n modulo m exists for all positive integers m.

Let $h(m)$ denote the period of L_n modulo m.

Corollary 4. Let $g(m)$ exist. Then

i) $m = 1$ or 2 if and only if $h(m) = g(m)$
ii) $m > 2$ and $g(m)$ is odd if and only if $h(m) = 2g(m)$
iii) $g(m)$ is even if and only if $h(m) = 4g(m)$.

Proof. Since $g(m)$ exists and $g(5)$ does not exist we have $(m, 5) = 1$. So from the corollary to Theorem 8 of Wall [2, p. 529] we have $s(m) = h(m)$. We first prove the sufficiency in each case.

Case i) is clear.

Case ii): By Theorems 2 and 3, $2g(m) = f(m) = s(m) = h(m)$.

Case iii): By Theorems 2 and 3, $4g(m) = 2f(m) = s(m) = h(m)$.

The necessity in each case follows directly from the implications already proved.

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.
3. L. Carlitz, "A Note on Fibonacci Numbers" *The Fibonacci Quarterly*, Vol. 2, No. 1 (Feb. 1964), pp. 15–28.

****