REFERENCES

1. Murray Edelberg, Solutions to Problems in 2, McGraw-Hill, 1968, p. 74.
2. C.L.Liu, *Introduction to Combinatorial Mathematics,* McGraw-Hill, 1968, Problem 4–4, p. 119.
3. N. J. A. Sloane, *A Handbook of Integer Sequences,* Academic Press, 1973, p. 59.

****

ON THE EQUALITY OF PERIODS OF DIFFERENT MODULI IN THE FIBONACCI 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 the Fibonacci sequence.

Let p be an arbitrary prime. Wall [2, p. 528] makes the following remark: "The most perplexing problem we have met in this study concerns the hypothesis $s(p^2) \neq s(p)$. We have run a test on a digital computer which shows that $s(p^2) \neq s(p)$ for all p up to 10,000; however, we cannot yet prove that $s(p^2) = s(p)$ is impossible. The question is closely related to another one, "can a number x have the same order mod p and mod p^2?," for which rare cases give an affirmative answer (e.g., $x = 3$, $p = 11$; $x = 2$, $p = 1093$); hence, one might conjecture that equality may hold for some exceptional p."

Based on Ward's Last Theorem [3, p. 205] we shall give necessary and sufficient conditions for $s(p^2) = s(p)$.

From Robinson [4, p. 30] we have for $m,n > 0$

(1) $$F_{n+r} \equiv F_r \pmod{m} \text{ for all integers } r \text{ if and only if } s(m) \mid n.$$

If $m,n > 0$ and $m \mid n$, then $F_{s(n)+r} \equiv F_r \pmod{m}$ for all r. Therefore by (1), $s(m) \mid s(n)$. So we have for $m,n > 0$

(2) $$m \mid n \text{ implies } s(m) \mid s(n).$$

It is easily verified that for all integers n

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

From Theorem 1 of [1, p. 39] we have that $s(m)$ is even if $m > 2$.

An equivalent form of the following theorem can be found in Vinson [1, p. 42].

Theorem 1. We have

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

To prove the above theorem it is sufficient, in view of Theorem 3 by Vinson [1, p. 42], to prove the following:

Lemma. $m = 1$ or 2 or $s(m)/2$ is odd if and only if $8 \nmid m$ and $2 \mid f(p)$ but $4 \nmid f(p)$ for every odd prime, p, which divides m.

Proof. Let $m = 1$ or 2 or $s(m)/2$ be odd. If $m = 1$ or 2, then the conclusion is clear. So we may assume that $m > 2$ and $s(m)/2$ is odd. Suppose $8 \mid m$. Then by (2), $12 = s(8) \mid s(m)$. Therefore $s(m)/2$ is even, a contradiction. Hence $8 \nmid m$.

Let p be any odd prime which divides m. From [1, p. 37] and (2), $f(p) \mid s(p) \mid s(m)$. Therefore $4 \nmid f(p)$. Suppose $2 \nmid f(p)$. Then by Theorem 1 of [1, p. 39] and (2), we have $4f(p) = s(p) \mid s(m)$, a contradiction. Thus $2 \mid f(p)$.

Conversely, let $8 \nmid m$ and $2 \mid f(p)$ but $4 \nmid f(p)$ for every odd prime, p, which divides m. Let p be any odd prime which divides m and let e be any positive integer. From [1, p. 40] we have that $f(p)$ and $f(p^e)$ are divisible by the same power of 2. Therefore $2 \mid f(p^e)$ and $4 \nmid f(p^e)$. Then since

$$p^e \mid F_{f(p^e)} = F_{f(p^e)/2} L_{f(p^e)/2}$$

and $p^e \nmid F_{f(p^e)/2}$ and $(F_n, L_n) = d \leqslant 2 < p$ for all integers n, we have $p^e \mid L_{f(p^e)/2}$. So by (3),

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

Therefore by definition, $f(p^e) = s(p^e)$.

Now, suppose that $m > 2$ and $s(m)/2$ is even. Let m have the prime factorization $m = 2^a p_1^{a_1} \cdots p_r^{a_r}$ with $a \geqslant 0$. Then by [1, p. 41]

$$s(m) = \underset{1 \leqslant i \leqslant r}{\text{l.c.m.}} \{s(2^a), s(p_i^{a_i})\} .$$

Then $4 \mid s(m)$ implies $4 \mid s(2^a)$ or $4 \mid s(p_j^{a_j})$ for some j such that $1 \leqslant j \leqslant r$. If $4 \mid s(2^a)$, then $a \geqslant 3$. Thus $8 \mid m$, a contradiction. If $4 \mid s(p_j^{a_j}) = f(p_j^{a_j})$, then we have another contradiction. Therefore $s(m)/2$ is odd or $m = 1$ or 2.

Various relationships of equality between integral multiples of $s(m)$, $f(m)$, $s(t)$ and $f(t)$ for arbitrary positive integers m and t can be obtained as corollaries to Theorem 1. We mention only the following:

Corollary 1. If $m > 2$ and $t > 2$ and

i) $s(m)/2$ and $s(t)/2$ are both odd, or
ii) $f(m)$ and $f(t)$ are both odd, or
iii) $s(m)/2$, $s(t)/2$, $f(m)$ and $f(t)$ are all even,

then $s(m) = s(t)$ if and only if $f(m) = f(t)$.

Theorem 2. Let m and t be positive integers such that $m \mid L_{f(m)/2}$ if $f(m)$ is even and $t \mid L_{f(t)/2}$ if $f(t)$ is even. Then $s(m) = s(t)$ if and only if $f(m) = f(t)$.

Proof. Let $s(m) = s(t)$. We have $m = 1$ iff $t = 1$ and $m = 2$ iff $t = 2$, so we may assume that $m > 2$ and $t > 2$. By Corollary 1, we need only consider the case; $s(m)/2 = s(t)/2$ is even and $f(m)$ and $f(t)$ have different parity, say $f(m)$ is odd and $f(t)$ is even. Then by Theorem 1, $4f(m) = s(m) = s(t) = 2f(t)$. Therefore $f(t)/2 = f(m)$ is odd. Since $f(t)$ is even we have by hypothesis that $t \mid L_{f(t)/2}$. Thus by (3),

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

But $t \mid F_{f(t)}$ and $f(t) < s(t)$. This contradicts the definition of $s(t)$. Therefore the case under consideration cannot occur.

Conversely, let $f(m) = f(t)$. As before we may assume that $m > 2$ and $t > 2$. By Corollary 1, we need only consider the case; $f(m) = f(t)$ is even and $s(m)/2$ and $s(t)/2$ have different parity, say $s(m)/2$ is odd and $s(t)/2$ is even. Then by Theorem 1,

$$2s(m) = 2f(m) = 2f(t) = s(t).$$

Therefore $f(t)/2$ is odd. Since $f(t)$ is even we have $t \mid L_{f(t)/2}$. Thus by (3), $F_{f(t)+1} \equiv 1 \pmod{t}$. But $t \mid F_{f(t)}$ and $f(t) < s(t)$. This is a contradiction and therefore the case under consideration cannot occur.

Corollary 2. Let p and q be arbitrary odd primes and e and a be arbitrary positive integers. Then $s(p^e) = s(q^a)$ if and only if $f(p^e) = f(q^a)$.

Proof. By Theorem 2 we need only show that if $f(p^e)$ is even then $p^e \mid L_{f(p^e)/2}$. We have

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

Thus $p^e \mid L_{f(p^e)/2}$.

Corollary 3. Let $\phi_n(x) = x + x^2/2 + \cdots + x^n/n$, and let $k(x) = k_p(x) = (x^{p-1} - 1)/p$, where p is an odd prime greater than 5. Then $s(p^2) = s(p)$ if and only if $\phi_{(p-1)/2}(5/9) \equiv 2k(3/2) \pmod{p}$.

[Continued on page 96.]