PRIMITIVE PERIODS OF GENERALIZED FIBONACCI SEQUENCES

CLAUDIA SMITH and VERNER E. HOGGATT, JR.
San Jose State University, San Jose, California 95192

1. INTRODUCTION

In this paper we are concerned with the primitive periodicity of Fibonacci-type sequences; where the Fibonacci sequence $\{F_n\}_{n=0}^{\infty}$ is defined with $F_0 = 0$, $F_1 = 1$, and $F_{n+2} = F_{n+1} + F_n$; and the generalized Fibonacci sequence $\{H_n\}_{n=0}^{\infty}$ has any two relatively prime starting values with the rule, $H_{n+2} = H_{n+1} + H_n$. The Lucas sequence $\{L_n\}_{n=0}^{\infty}$ is defined with $L_0 = 2$, $L_1 = 1$, and $L_{n+2} = L_{n+1} + L_n$; and the generalized Lucas sequence $\{G_n\}_{n=0}^{\infty}$ is defined recursively by $G_n = H_{n+1} + H_{n-1}$. We will see that in one case, that of modulo 3^n, all generalized Fibonacci sequences have the same primitive periodicity. Then we will observe that the primitive periods of $\{F_n\}$ and $\{L_n\}$ are the same, modulus p^m, where p is a prime, $p \neq 5$.

Prior to examination of the Fibonacci case mod 3^n we will prove the following theorem:

Theorem. If $n \mid F_m$, then $n^k \mid F_{mn^{k-1}}$. We use the fact that

$$\alpha^m = F_m\alpha + F_{m-1} \qquad \beta^m = F_m\beta + F_{m-1} \qquad (\alpha^{mn^{k-2}})^n = \alpha^{mn^{k-1}}$$

$$\alpha^{mn^{k-2}} = \alpha F_{mn^{k-2}} + F_{mn^{k-2}-1} \qquad \beta^{mn^{k-2}} = \beta F_{mn^{k-2}} + F_{mn^{k-2}-1} \quad .$$

By definition,

$$F_{mn^{k-1}} = \sum_{j=0}^{n} \binom{n}{j} (F_{mn^{k-2}})^j (F_{mn^{k-2}-1})^{n-j} F_j$$

$$F_{mn^{k-1}} = 0 + nF_{mn^{k-2}}(F_{mn^{k-2}-1})^{n-1}F_1 + \binom{n}{2}(F_{mn^{k-2}})^2 F_{mn^{k-2}-1}F_2 \cdot$$

By induction, $n^{k-1} \mid F_{mn^{k-2}}$. Clearly, n^{k-1} also divides all successive terms as j is increasing. Our proof is complete.

2. THE FIBONACCI CASE MOD 3^n

Theorem 1. The period (not necessarily primitive) of the Fibonacci sequence modulo 3^n is $2^3 \cdot 3^{n-1}$. We will prove that: (A) $F_{2^3\cdot 3^{n-1}} \equiv F_0 \pmod{3^n}$ and (B) $F_{2^3\cdot 3^{n-1}+1} \equiv F_1 \pmod{3^n}$.

A. The proof is direct.

$3 \mid F_{2^2}$, thus $3^k \mid F_{2^2\cdot 3^{k-1}}$, using the theorem; If $m \mid F_n$, then $m^k \mid F_{nm^{k-1}}$.

It follows that $3^k \mid F_{2^3\cdot 3^{k-1}}$, thus $F_{2^3\cdot 3^{k-1}} \equiv 0 \pmod{3^k}$.

Hence Part A is proved.

B. (1) First, $\quad F_{2^3\cdot 3^{n-1}+1} = (F_{2^2\cdot 3^{n-1}+1})^2 + (F_{2^2\cdot 3^{n-1}})^2$

using the identity

$$F_{m+n+1} = F_{m+1}F_{n+1} + F_mF_n \,.$$

Now, since $(F_{2^2\cdot 3^{n-1}})^2 \equiv 0 \pmod{3^n}$ From Part A, it follows that

(2) $(F_{2^3\cdot 3^{n-1}})^2 \equiv 1 \pmod{3^n}$ from the identity $F_{n+1}F_{n-1} - F_n^2 = (-1)^n$.

(3) Now, substituting into (1) we have $F_{2^3 \cdot 3^{n-1}+1} \equiv 1 + 0 \pmod{3^n}$. Hence Part B is proved.

Theorem 2. The primitive period of the Fibonacci sequence modulo 3^n is $2^3 \cdot 3^{n-1}$. Secondly, $2^2 \cdot 3^{n-1}$ is the entry point of 3^n. Let 3^k be the highest power of 3 dividing F_n; the notation is $3^k \| F_n$.

(4) We now prove that $3^n \| F_{2^2 \cdot 3^{n-1}}$. The proof is by induction. We will have to consider three cases,

CASE 1. $n = 1$. $3^1 \| F_{2^2 \cdot 3^{1-1}}$; $3 \| F_4 = 3$ and, $3^{1+1} \nmid F_{2^3 \cdot 3^{1-1}}$ $9 \nmid F_8 = 21$.

CASE 2. $n = 2$. $3^2 \| F_{2^2 \cdot 3^{2-1}}$; $9 \| F_{12} = 144$ and, $3^{2+1} \nmid F_{2^3 \cdot 3^{2-1}}$ $27 \nmid F_{24} = 46368$.

CASE 3. $n > 2$. Assume $3^k \| F_{2^2 \cdot 3^{k-1}}$; then we claim $3^{k+1} \nmid F_{2^3 \cdot 3^{k-1}}$.

$$F_{2^3 \cdot 3^{n-1}} = (F_{2^2 \cdot 3^{n-1}})(L_{2^2 \cdot 3^{n-1}})$$

using the identity $F_{2n} = F_n L_n$. Now, given that $3^n \| F_{2^2 \cdot 3^{n-1}}$ and since (F_n, L_n) is 1 or 2, then

$$3^{n+1} \nmid F_{2^3 \cdot 3^{n-1}}.$$

(5) If $3^{k+1} \nmid F_{2^2 \cdot 3^k}$ then 3^{k+1} divides a smaller F_m whose subscript **is a multiple of the first** F_m **that** is divisible by 3^k. It must be of the form, $p(2^2 \cdot 3^{k-1})$. Clearly, $p \neq 1$, for that contradicts our assumption that $3^k \| F_{2^2 \cdot 3^{k-1}}$. And $p \neq 2$, for $3^{k+1} \nmid F_{2^3 \cdot 3^{k-1}}$. We conclude that $p = 3$, hence the first F_m divisible by 3^{k+1} is $F_{2^2 \cdot 3^k}$. Furthermore,

$$F_{2^2 \cdot 3^k} = F_{2^2 \cdot 3^{k-1}}(5(F_{2^2 \cdot 3^{k-1}})^2 + 3)$$

implies $3^{k+1} \| F_{2^2 \cdot 3^k}$ as it clearly shows $3^{k+2} \nmid F_{2^2 \cdot 3^k}$. Our claim in (4) is true; our proof is complete by induction.

(6) Now that we have found the first F_m divisible by 3^k, we can write the primitive period modulo 3^k as a multiple of that subscript. The primitive period is of the form $s(2^2 \cdot 3^{k-1})$. We have shown that when $s = 2$ we have a period, not necessarily primitive. We must examine $s < 2$, that is, $s = 1$. If the primitive period were to be $1(2^2 \cdot 3^{k-1})$, then we would need

$$F_{2^2 \cdot 3^{k-1}} \equiv F_0 \quad \text{and} \quad F_{2^2 \cdot 3^{k-1}+1} \equiv F_1 \pmod{3^k}.$$

We claim that the latter is false.

(7) We assert that $F_{2^2 \cdot 3^{k-1}} \not\equiv F_1 \pmod{3^k}$, but that

$$F_{2^2 \cdot 3^{k-1}+1} \equiv (-F_1) \pmod{3^k}.$$

This follows by induction.

(8) Case 1. $k = 1$. $F_{2^2 \cdot 3^{1-1}+1} = F_5 = 2 \equiv -1 \pmod 3$.

Case 2. $k = 2$. $F_{2^2 \cdot 3^{2-1}+1} = F_{13} = 233 \equiv -1 \pmod{3^2}$.

Case 3. $k > 2$. Assume that $F_{2^2 \cdot 3^{k-1}+1} \equiv -1 \pmod{3^k}$.

(9) Recall from Theorem 1, that $F_{2^2 \cdot 3^{k-1}+1} \equiv 1 \pmod{3^k}$ and that $F_{2^2 \cdot 3^{k-1}} \equiv 0 \pmod{3^k}$.

(10) Observe that

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

using the identity $F_{m+n+1} = F_{m+1}F_{n+1} + F_m F_n$.

(11) Now **substituting** (9) into (10) and using our inductive assumption in (8) we have

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

That is, $F_{2^2 \cdot 3^k+1} \equiv (-F_1) \pmod{3^{k+1}}$ and our proof is complete.

(12) We conclude that $s \nless 2$, thus $s = 2$ provides the primitive period and Theorem 2 is proved.

3. THE GENERAL FIBONACCI CASE MOD 3^n

Theorem 3A. The period (not necessarily primitive) of any generalized Fibonacci sequence modulo 3^n is $2^3 \cdot 3^{n-1}$. We will prove that: (A) $H_{2^3 \cdot 3^{n-1}+1} \equiv H_1 \pmod{3^n}$ and (B) $H_{2^3 \cdot 3^{n+1}+2} \equiv H_2 \pmod{3^n}$.

A. We will have to consider three cases.

Case 1. $n = 1$. $\quad H_{2^3 \cdot 3^{1-1}+1} = H_9 = 21H_2 + 13H_1 \equiv H_1 \pmod{3^n}$.

Case 2. $n = 2$. $\quad H_{2^3 \cdot 3^{2-1}+1} = H_{25} = 46368H_2 + 28657H_1 \equiv H_1 \pmod{3^2}$.

Case 3. $n > 2$.

(13) First,
$$H_{2^3 \cdot 3^{n-1}+1} = H_1 F_{2^3 \cdot 3^{n-1}-1} + H_2 F_{2^3 \cdot 3^{n-1}}$$
from the identity
$$H_{n+1} = H_1 F_{n-1} + H_2 F_n .$$
(14) But since
$$F_{2^3 \cdot 3^{n-1}} \equiv 0 \pmod{3^n}, \quad \text{and} \quad F_{2^3 \cdot 3^{n-1}-1} = F_{2^3 \cdot 3^{n-1}+1} - F_{2^3 \cdot 3^{n-1}} = 1 - 0 = 1$$
from the recursion rule that $F_{m-1} = F_{m+1} - F_m$; we substitute (14) into (13) to obtain that

(15) $$H_{2^3 \cdot 3^{n-1}+1} \equiv H_1(1) + H_2(9) \pmod{3^n}$$

and Part A is proved.

B. First,
$$H_{2^3 \cdot 3^{n-1}+2} = H_1 F_{2^3 \cdot 3^{n-1}} + H_2 F_{2^3 \cdot 3^{n-1}+1}$$
from the identity
$$H_{n+2} = H_1 F_n + H_2 F_{n+1}.$$
Since $F_{2^3 \cdot 3^{n-1}} \equiv 0 \pmod{3^n}$ from 1-A, and
$$F_{2^3 \cdot 3^{n-1}+1} \equiv 1 \pmod{3^n}$$
from 1-B, Part B follows immediately.

Theorem 3B. The primitive period of any generalized Fibonacci sequence modulo 3^n is $2^3 \cdot 3^{n-1}$.

In Theorem 3A we proved that the period is at most $2^3 \cdot 3^{n-1}$. It remains to show that the primitive period is no smaller.

Consider the generalized Fibonacci sequence $\{H_n\}$, $(H_1, H_2) = 1$. Adding alternate terms we derive another generalized sequence $\{D_n\}$. We observe: $H_2 + H_0 = kD_1$ where k is an integer, $H_3 + H_1 = kD_2$, and so on.

We need to examine the possible values for k. We rewrite the equations above:
$$2H_2 - H_1 = kD_1 \qquad H_2 + 2H_1 = kD_2 .$$
We solve for H_1 and H_2:
$$H_2 = \frac{k}{5}(2D_1 + D_2) = \frac{k}{5}(D_3 + D_1) \qquad H_1 = \frac{k}{5}(2D_2 - D_1) = \frac{k}{5}(D_2 + D_0).$$

If $k = 5$, then $\{H_n\}$ is a generalized Lucas sequence. If $5 \nmid k$, then $k = 1$ because $(H_1, H_2) = 1$, and 5 must divide $(D_3 + D_1)$ and $(D_2 + D_0)$. Thus $k = 1$ implies that $\{D_n\}$ is a generalized Lucas sequence.

We conclude that modulo 5^n is the only prime modulus in which the primitive period of a generalized Fibonacci sequence will be smaller than in the Fibonacci case. We note that it will be smaller by a factor of five. Hence, our proof of Theorem 3B is complete.

Example. The period modulo 5^n of the Fibonacci sequence is $4 \cdot 5^n$ while the period mod 5^n of the Lucas sequence is $4 \cdot 5^{n-1}$.

4. THE FIBONACCI AND LUCAS CASES MOD p^m

Lemma 1. A prime p, does not divide $\{L_n\}$ if and only if the entry point of p in $\{F_n\}$, (EP_F), is odd.

We will examine two cases in the proof.

Case 1: Given $p \nmid \{L_n\}$.

(16) Assume EP_F is even, that is, $EP_F = F_{2k}$, we write $p \,\|\, F_{2k}$.

(17) $p \,\|\, F_{2k}$ implies $p \nmid F_k$.

Recall the identity $F_{2k} = F_k L_k$. Therefore, $p \mid L_k$. This contradicts that $p \nmid \{L_n\}$.

(18) Hence our assumption in (16) is not true, so EP_F is odd. We conclude that $p \nmid \{L_n\}$ implies EP_F is odd.

Case 2: Given EP_F is odd.

(19) Assume $p \mid \{L_n\}$. Then there exists k such that $p \,\|\, L_k$.

(20) Recall that the greatest common divisor of (F_n, L_n) is 1 or 2. Hence $p \nmid F_k$.

(21) $p \| L_k$ implies $p \| F_{2k}$ from the identity $F_{2k} = F_k L_k$. This contradicts that EP_F is odd.

(22) Therefore $p \nmid \{L_n\}$. We conclude that EP_F is odd implies that $p \nmid \{L_n\}$ and our proof of Lemma 1 is complete.

Lemma 2. A prime p divides $\{L_n\}$ if and only if EP_F is either of the form 2 (odd) or 2^m (odd), $m \geq 2$. This follows immediately from Lemma 1 and the identity $F_{2^n k} = F_{2^{n-1}k} \cdot L_{2^{n-1}k}$.

Theorem 4. The primitive periods of $\{F_n\}$ and $\{L_n\}$ are of the same length, modulus p, for p a prime, $p \neq 5$.

Case 1. The primitive period for $\{L_n\}$ is no longer than for $\{F_n\}$.

(23) We have $L_{n+k} - L_{n-k} = L_n L_k$, k odd.

(24) $L_{n+k} - L_{n-k} = 5F_n F_k$, k even.

Now, let $2k$ denote the length of the period of $\{F_n\}$. Thus k denotes half the period of $\{F_n\}$. When EP_F of p is odd then the period, $2k$, is $4(EP_F)$. Thus $k = 2(EP_F)$ so k is even. Likewise, when EP_F of p is of the form 2^m (odd) for $m \geq 2$, then the period, $2k$, is $2(EP_F)$. Thus $k = EP_F = 2^m$ (odd) so k is even.

Note, above that either $k = 2EP_F$ or $k = EP_F$, thus $F_k \equiv 0$, mod p. Hence, $L_{n+k} - L_{n-k} \equiv 0$, mod p. It follows that the period of $\{L_n\}$ is $2k$ which is the period of $\{F_n\}$.

Now we consider the special case when EP_F is of the form 2 (odd). Then the period, $2k$, is EP_F, and $k = \frac{1}{2}2$ (odd) so k is odd. We will use Eq. (23). We recall that $F_{2k} F_k L_k$ implies $p | L_k$ since EP_F of p is F_{2k} implies $p \nmid F_k$. Hence $p | L_k$ means $L_k \equiv 0$, mod p. Therefore $L_{n+k} - L_{n-k} \equiv 0$, mod p. It follows that the period of $\{L_n\}$ is $2k$, again the same as the period of $\{F_n\}$.

Case 2. The primitive period for $\{L_n\}$ is no shorter than for $\{F_n\}$.

A. First we will consider the situation in which EP_F is odd. Then the period is $4(EP_F)$ and $k = 2(EP_F)$. By Lemma 1, $p \nmid \{L_n\}$.

(25) Assume the primitive period for $\{L_n\}$ is shorter than for $\{F_n\}$, that is, the primitive period for $\{L_n\}$ is half the period of $\{F_n\}$. Then the period for $\{L_n\}$ is $2(EP_F)$. We use Eq. (23) since

(26) EP_F is odd. We have $L_{n+EP_F} - L_{n-EP_F} = L_n L_{EP_F}$. But $p \nmid \{L_n\}$ thus $p \nmid L_{EP_F}$ so Eq. (26) is not con-

(27) gruent to zero. Therefore, the period cannot be $2(EP_F)$. Our assumption in (25) is false, so when EP_F is odd the period of $\{L_n\}$ is no shorter than for $\{F_n\}$.

B. Now we consider the situation in which EP_F is of the form $2d$, where d is odd. Then the period for $\{F_n\}$ is EP_F.

(28) Assume the primitive period for $\{L_n\}$ is shorter than for $\{F_n\}$. We note that $L_d \equiv 0$ since EP_F is F_{2d} and the fact that $F_{2d} = F_d L_d$. Now, assuming the primitive period for $\{L_n\}$ is smaller means that there exists c where $c < d$ such that $L_{n+c} - L_{n-c} = L_n L_c$. This would meet the requirement since the period $2c < 2d$. However, $L_c = 0$ implies that $F_{2c} \equiv 0$ mod p which contradicts that EP_F of p is F_{2d}.

(29) Our assumption in (28) is false, so when EP_F is of the form $2d$ where d is odd, then the period for $\{L_n\}$ is no shorter than for $\{F_n\}$.

C. Lastly, we consider the situation in which EP_F is of the form $2^m d$, where d is odd and $m \geq 2$. Then the

(30) period for F_n, is $2EP_F$. Assuming the primitive period for $\{L_n\}$ is smaller, then it too must be even since the period for $\{F_n\}$ is even. There exists b where $b < EP_F$ such that $L_{n+b} - L_{n-b} = 5F_n F_b$.

But if $2b$ is to be the period for $\{L_n\}$ then $5F_nF_b \equiv 0 \bmod p$. But $F_b \not\equiv 0 \bmod p$ since $b < EP_F$. Our
(31) assumption in (30) must be false. We conclude that if EP_F is of the form $2^m d$, where d is odd, $m \geq 2$, then the primitive period for $\{L_n\}$ is no shorter than for $\{F_n\}$.

Our conclusions in (27), (29), and (31) prove that Case 2 is true. Thus our proof of Theorem 4 is complete.

Examples of Theorem 4

Example 1. EP_F of p is odd.

Take $p = 13$. The $EP_F = 7$. We see the length of the primitive period of $\{F_n\}$ is 28.

Period of $\{F_n\}$ mod 13 = 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, 0.

Period of $\{L_n\}$ mod 13 = 1, 3, 4, 7, 11, 5, 3, 8, 11, 6, 4, 10, 1, 11, 12, 10, 9, 6, 2, 8, 10, 5, 2, 7, 9, 3, 12, 2.

We see that the primitive period of $\{F_n\}$ is exactly the same length as the primitive period of $\{L_n\}$.

We also observe that Lemma 1 is demonstrated as $p \nmid \{L_n\}$.

Example 2. EP_F of p is of the form 2 (odd).

Take $p = 29$. The EP_F = 14 = 2(7). The length of the primitive period of $\{F_n\}$ is 14.

Period of $\{F_n\}$ mod 29 = 1, 1, 2, 3, 5, 8, 13, 21, 5, 26, 2, 28, 1, 0.

Period of $\{L_n\}$ mod 29 = 1, 3, 4, 7, 11, 18, 0, 18, 18, 7, 25, 3, 28, 2.

We see that the primitive period of $\{F_n\}$ is exactly the same length as of $\{L_n\}$.

Also note that the $EP_F = 2EP_L$. We see Lemma 2 demonstrated.

Example 3. EP_F of p is of the form 2^m (odd), $m \geq 2$.

Take p = 47. The EP_F = 16 = $2^4(1)$. The length of the primitive period of $\{F_n\}$ is 32.

Period of $\{F_n\}$ mod 47 = 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, 0.

Period of $\{L_n\}$ mod 47 = 1, 3, 4, 7, 11, 18, 29, 0, 29, 29, 11, 40, 36, 29, 18, 0, 18, 18, 36, 7, 43, 3, 46, 2.

Again we see that the primitive period of $\{F_n\}$ is exactly the same as for $\{L_n\}$.

We notice that the $EP_F = 2EP_L$, and we see Lemma 2 demonstrated.

Comment. In this study we came across an unanswered problem that was discovered by D. D. Wall in 1960. It concerns the hypothesis that "Period mod $p^2 \neq$ Period mod p." He ran a test on a digital computer that verified the hypothesis was true for all p less than 10,000. Until this day no one as yet has proven that the Period mod p^2 = Period mod p is impossible.

We give an example to show that the above hypothesis does not hold for composite numbers. Period mod 12^2 = Period mod 12 = 24.

Period mod 12 of $\{F_n\}$ = 1, 1, 2, 3, 5, 8, 1, 9, 10, 7, 5, 0, 5, 5, 10, 3, 1, 4, 5, 9, 2, 11, 1, 0.

Period mod 12^2 of $\{F_n\}$ = 1, 1, 2, 3, 5, 8, 13, 21, 55, 89, 0, 89, 89, 34, 123, 13, 136, 5, 141, 2, 143, 1, 0.

We note that EP_F of 12 = EP_F of 12^2.

REFERENCE

D. D. Wall, "Fibonacci Series Modulo *m*," *The Amer. Math. Monthly,* Vol. 67, No. 6 (June-July 1960), pp. 525–532.

****