SOME PROPERTIES OF A GENERALIZED FIBONACCI SEQUENCE MODULO m

MARCELLUS E. WADDILL

Wake Forest University, Winston-Salem, NC 27109

The Fibonacci sequence reduced by the modulus *m* has been examined by Wall [1], Dynkin and Uspenskii [2], and others. In this paper we investigate the generalized Fibonacci sequence $\{K_n\}$, where $K_0 = 0$, $K_1 = K_2 = 1$, and

$$K_n = K_{n-1} + K_{n-2} + K_{n-3}, \ n > 2.$$
⁽¹⁾

We reduce $\{K_n\}$ modulo *m*, taking least nonnegative residues.

Definition: Let h = h(m), where h(m) denotes the number of terms in one period of the sequence $\{K_n\}$ modulo m before the terms start to repeat, be called the *length of the period* of $\{K_n\}$ (mod m).

Example: The values of $\{K_n\}$ (mod 7) are

0, 1, 1, 2, 4, 0, 6, 3, 2, 4, 2, 1, 0, 3, 4, 0, 0, 4, 4, 1, 2, 0, 3, 5, 1, 2, 1, 4, 0, 5, 2, 0, 0, 2, 2, 4, 1, 0, 5, 6, 4, 1, 4, 2, 0, 6, 1, 0.

and then repeat. Consequently, we conclude that h(7) = 48. Note that $K_{46} \equiv 1$, $K_{47} \equiv K_{48} \equiv 0$, $K_{49} \equiv 1 \pmod{7}$. Hence the sequence has started to repeat when we reach the triple 1, 0, 0. Note also that $K_{15} \equiv K_{16} \equiv 0$, $K_{31} \equiv K_{32} \equiv 0 \pmod{7}$, so that the 48 terms in one period are divided by adjacent double zeros into three sets of 16 terms each. This example illustrates a general principle contained in

Theorem 1: The sequence $\{K_n\} \pmod{m}$ forms a simply periodic sequence. That is, the sequence is periodic and repeats by returning to its starting values 0, 1, 1.

Proof: If we consider any three consecutive terms in the sequence reduced modulo m, there are only m^3 possible such distinct triples. Hence at some point in the sequence, we have a repeated triple. A repeated triple results in the recurrence of K_0 , K_1 , K_2 , for from the defining relation (1),

$$K_{n-2} = K_{n+1} - K_n - K_{n-1}.$$

Therefore, if

$$K_{t+1} \equiv K_{s+1}, K_t \equiv K_s$$
, and $K_{t-1} \equiv K_{s-1} \pmod{m}$,

then

$$K_{t-2} = K_{t+1} - K_t - K_{t-1} \equiv K_{s+1} - K_s - K_{s-1} \equiv K_{s-2} \pmod{m}$$

and, similarly (assuming that t > s),

Hence, any repeated triple implies a repeat of 0, 1, 1 and a return to the starting point of the sequence.

If h is the length of the period of $\{K_n\}$ (mod m), then clearly $K_h \equiv 0$, $K_{h+1} \equiv K_{h+2} \equiv 1 \pmod{m}$. From the defining relation (1), it also follows that $K_{h-1} \equiv 0$, $K_{h-2} \equiv 1$, $K_{h-3} \equiv m-1$, and $K_{h-4} \equiv 0 \pmod{m}$. We now list some identities for the sequence $\{K_n\}$ which will be useful in the sequel. These identities and their proofs may be found in [3].

$$K_{n+p} = K_n K_{p+1} + K_{n-1} (K_p + K_{p-1}) + K_{n-2} K_p, \ n \ge 2, \ p \ge 1;$$
(2)

$$K_{n+p} = K_{n-r}K_{p+r+1} + K_{n-r-1}(K_{p+r} + K_{p+r-1}) + K_{n-r-2}K_{p+r},$$
(3)
$$n > 2, p > 1, -p + 2 < r < n - 1;$$

$$L_n = K_{n-1} + K_{n-2}; (4)$$

$$\begin{vmatrix} 1 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{vmatrix}^{n} = \begin{vmatrix} K_{n+1} & L_{n+1} & K_{n} \\ K_{n} & L_{n} & K_{n-1} \\ K_{n-1} & L_{n-1} & K_{n-2} \end{vmatrix}, \ n \ge 2;$$
(5)

$$K_n^2 K_{n-3} + K_{n-1}^3 + K_{n-2}^2 K_{n+1} - K_{n+1} K_{n-1} K_{n-3} - 2K_n K_{n-1} K_{n-2} = 1, \ n \ge 3.$$
 (6)

The following theorem gives an unusual property about the terms which immediately precede and follow adjacent double zeros in the sequence $\{\mathcal{K}_n\}$ (mod m).

Theorem 2: If
$$K_n \equiv K_{n-1} \equiv 0 \pmod{m}$$
, then $K_{n-2}^3 \equiv K_{n+1}^3 \equiv 1 \pmod{m}$.

Proof: The fact that $K_{n-2}^3 \equiv K_{n+1}^3 \pmod{m}$ follows from the defining relation (1) and the fact that $K_n \equiv K_{n-1} \equiv 0 \pmod{m}$. To prove the other part, we observe by (6) that

$$K_{n-1}^{2}K_{n-4} + K_{n-2}^{3} + K_{n-3}^{2}K_{n} - K_{n}K_{n-2}K_{n-4} - 2K_{n-1}K_{n-2}K_{n-3} = 1.$$

All terms on the left side of this equation, except K_{n-2}^3 , are congruent to 0 modulo m. Hence we have

$$K_{n-2}^3 \equiv K_{n+1}^3 \equiv 1 \pmod{m}$$
.

346 SOME PROPERTIES OF A GENERALIZED FIBONACCI SEQUENCE MODULO m [Aug.

Theorem 3: If j is the least positive integer such that $K_{j-1} \equiv K_j \equiv 0$ (mod m), then

- (a) $K_{n,j-1} \equiv K_{n,j} \equiv 0 \pmod{m}$, for all positive integers n and
- (b) if $K_{t-1} \equiv K_t \equiv 0 \pmod{m}$, then t = nj for some positive integer n.

Proof of (a): The proof is by induction on n. For n = 1, the conclusion is immediate from the hypothesis. If we assume as induction hypothesis that $K_{n,j-1} \equiv K_{n,j} \equiv 0 \pmod{m}$, then by (2)

$$K_{(n+1)j} = K_{nj+j} = K_{nj}K_{j+1} + K_{nj-1}(K_j + K_{j-1}) + K_{nj-2}K_j \equiv 0 \pmod{m}.$$

A similar argument shows that $K_{n,i-1} \equiv 0 \pmod{m}$.

Proof of (b): Let t be such that $K_t \equiv K_{t-1} \equiv 0 \pmod{m}$. We have t > j since j was least such that $K_j \equiv K_{j-1} \equiv 0 \pmod{m}$. If j does not divide t, then by the division algorithm,

$$t = jq + r, 0 < r < j$$

We have by (2),

 $K_t = K_{jq+r} = K_{jq}K_{r+1} + K_{jq-1}(K_{r-1} + K_r) + K_{jq-2}K_r \equiv 0 \pmod{m}.$

But since $K_{jq} \equiv K_{jq-1} \equiv 0 \pmod{m}$, this equation implies that

 $K_{jq-2}K \equiv 0 \pmod{m}.$

By Theorem 2,

$$K_{ia}^3 = 2 \equiv 1 \pmod{m},$$

which implies that no divisors of m divide K_{jq-2} . Thus,

$$K_r \equiv 0 \pmod{m}$$
.

Similarly, we can show that

 $K_{r-1} \equiv 0 \pmod{m}.$

But r < j, and so these last two congruences contradict the choice of j as least such that

 $K_j \equiv K_{j-1} \equiv 0 \pmod{m}.$

The following theorem shows that in considering properties about the length of the period of $\{K_n\}$ (mod *m*) we can, without loss of generality, restrict the choice of *m* to p^t , where *p* is a prime and *t* a positive integer.

Theorem 4: If *m* has prime factorization

$$m = p_1^{t_1} p_2^{t_2} \cdots p_s^{t_s},$$

and if h_i denotes the length of the period of $\{K_n\}$ (mod $p_i^{t_i}$), then the length of the period of $\{K_n\}$ (mod *m*) is equal to l.c.m. $[h_i]$, the least common multiple of the h_i .

Proof: For all *i*, if h_i denotes the length of the period of $\{K_n\}$ (mod $p_i^{t_i}$),

$$\begin{split} & K_{h_i-1} \equiv K_{h_i} \equiv 0 \pmod{p_i^{t_i}} \\ & K_{h_i-2} \equiv K_{h_i+1} \equiv 1 \pmod{p_i^{t_i}}, \end{split}$$

and also

$$K_{rh_i-1} \equiv K_{rh_i} \equiv 0 \pmod{p_i^{t_i}},$$

$$K_{rh_i-2} \equiv K_{rh_i+1} \equiv 1 \pmod{p_i^{t_i}},$$

for all positive integers r. If $j = 1.c.m. [h_i]$, it follows then that

$$K_j \equiv K_{j-1} \equiv 0 \pmod{m},$$

$$K_{j-2} \equiv K_{j+1} \equiv 1 \pmod{m}.$$

Conversely, if h is the length of the period of $\{K_n\}$ (mod m), then

$$K_h \equiv K_{h-1} \equiv 0 \pmod{m},$$

$$K_{h-2} \equiv K_{h+1} \equiv 1 \pmod{m},$$

which implies that for all i,

$$K_{h} \equiv K_{h-1} \equiv 0 \pmod{p_{i}^{t_{i}}},$$

$$K_{h-2} \equiv K_{h+1} \equiv 1 \pmod{p_{i}^{t_{i}}}.$$

By Theorem 3, $h = h_i r_i$ for all h_i and an appropriate r_i . That is, h is a common multiple of the h_i . By definition of h then, h = j, the l.c.m. $[h_i]$.

Theorem 5: If $K_t \equiv K_{t-1} \equiv 0 \pmod{m}$, then $K_{t-4} \equiv 0 \pmod{m}$.

Proof: By the defining relation (1) and the hypothesis, we have

$$K_t = K_{t-1} + K_{t-2} + K_{t-3} \equiv 0 \pmod{m}, \tag{7}$$

$$K_{t-1} = K_{t-2} + K_{t-3} + K_{t-4} \equiv 0 \pmod{m}.$$
(8)

Now subtracting (8) from (7), we have

$$K_{t-1} - K_{t-4} \equiv 0 \pmod{m},$$

or

348

$$K_{t-1} \equiv K_{t-4} \pmod{m}.$$

The next theorem gives an interesting transformation of a certain factor from the subscript to a power in moving from the modulus m to m^2 when the subscript is a specified function of the length of the period of $\{K_n\}$ (mod m). This theorem is useful in establishing the length of the period of $\{K_n\}$ (mod p^n) relative to the length of the period of $\{K_n\}$ (mod p), p a prime.

Theorem 6: If h is the length of the period of $\{K_n\} \pmod{m}$, then the following identities hold in terms of the modulus m^2 .

$$K_{sh+1} \equiv K_{h+1}^{s} \pmod{m^2}, \qquad (9)$$

$$K_{sh-1} \equiv sK_{h-2}^{s-1}K_{h-1} \pmod{m^2}, \tag{10}$$

$$K_{sh-2} \equiv K_{h-2}^{s} \pmod{m^2}, \tag{11}$$

$$K_{sh} \equiv (K_{h+1}^{s} - sK_{h-2}^{s-1}K_{h-1} - K_{h-2}^{s}) \pmod{m^{2}}.$$
 (12)

Proof of (9): The proof is by induction on s. For s = 1, the conclusion is immediate. If we assume that

$$K_{sh+1} \equiv K_{h+1}^{s} \pmod{m^2},$$

then, by (2),

$$K_{(s+1)h+1} = K_{(sh+1)+h} = K_{sh+1}K_{h+1} + K_{sh}(K_h + K_{h-1}) + K_{sh-1}K_h.$$

Since h is the length of the period of $\{K_n\} \pmod{m}$, and also using Theorem 3, we have

$$K_h \equiv K_{h-1} \equiv K_{sh} \equiv K_{sh-1} \equiv 0 \pmod{m}.$$

But these congruences imply that

$$K_{sh}(K_h + K_{h-1}) \equiv K_{sh-1}K_h \equiv 0 \pmod{m^2},$$

which together with the induction hypothesis implies that

$$K_{(s+1)h+1} \equiv K_{sh+1}K_{h+1} \equiv K_{h+1}^{s}K_{h+1} \equiv K_{h+1}^{s+1} \pmod{m^2},$$

and the result is proved.

The proofs of (10) and (11) follow in a similar manner.

Proof of (12): Using the defining relation (1) and (9), (10), and (11), we have

$$K_{sh} = K_{sh+1} - K_{sh-1} - K_{sh-2} \equiv (K_{h+1}^s - sK_{h-2}^{s-1}K_{h-1} - K_{h-2}^s) \pmod{m^2}.$$

We return now to the question of the relation between the length of the period of $\{K_n\}$ (mod p) and the length of the period of $\{K_n\}$ (mod p^r) where r is an arbitrary positive integer. First, a preliminary theorem:

Theorem 7: If p is a prime and h = h(p) is the length of the period of $\{K_n\} \pmod{p}$, then $K_{h+1}^p \equiv 1 \pmod{p^2}$.

Proof: If $K_{h+1} \equiv 1 \pmod{p^2}$, then $K_{h+1}^p \equiv 1 \pmod{p^2}$ trivially. If $K_{h+1} \not\equiv 1 \pmod{p^2}$, then

$$K_{h+1}^{p} - 1 = (K_{h+1} - 1)(K_{h+1}^{p-1} + K_{h+1}^{p-2} + \cdots + K_{h+1}^{p} + 1).$$

Now

$$K_{h+1} - 1 \equiv 0 \pmod{p} \tag{13}$$

349

and

$$K_{h+1}^{s} \equiv 1 \pmod{p}$$

for any s. Therefore,

 $K_{h+1}^{p-1} + K_{h+1}^{p-2} + \dots + K_{h+1} + 1 \equiv 1 + 1 + \dots + 1 \equiv 0 \pmod{p}.$ (14)

Using (13) and (14), we see that

$$K_{h+1}^p - 1 \equiv 0 \pmod{p^2}$$
.

We now state the main theorem.

Theorem 8: If p is a prime and $h(p^2) \neq h(p)$, then $h(p^r) = p^{r-1}h(p)$ for any positive integer r > 1.

Proof: We prove the case when p = 2. The general case follows in a similar manner by means of induction. Since h = h(p) is the length of the period of $\{K_h\}$ (mod p), then using (5), we have

1	1	1	h	K +1	L_{h+1}	K _h		1	0	0	(mod <i>p</i>),
1	0	0	=	K _h	L_{h+1}	K _{h-1}	Ξ	0	1	0	(mod p),
0	1	0		K _{h-1}	L_{h-1}	K _{h-2}		0	0	1	

where h is the smallest sech power for which this property holds. [The sequence $\{L_n\}$ is defined by (4).] Now also by (5),

1	1	$1^{h_{p}}$		K_{hp+1}	L_{hp+1}	K_{hp}	
1	0	0	=	K _{hp}	L_{hp}	K_{hp-1}	•
0	1	0		K_{hp-1}	L_{hp}	K _{hp-2}	

If $h(p) \neq h(p^2)$, then using (9), (10), and (12), the first column of the matrix on the right has values as follows:

 $K_{hp+1} \equiv K_{h+1}^p \pmod{p^2},$ (15)

$$K_{hp} \equiv (K_{h+1}^p - pK_{h-2}^{p-1}K_{h-1} - K_{h-2}^p) \pmod{p^2},$$
(16)

$$K_{hp-1} \equiv p K_{h-2}^{p-1} K_{h-1} \pmod{p^2}.$$
 (17)

By Theorem 7 and (15), it follows that

$$K_{hp+1} \equiv 1 \pmod{p^2}$$
. (18)

Using Theorem 7, (16), and (17), it follows that

$$K_{hp} \equiv K_{hp-1} \equiv 0 \pmod{p^2}, \tag{19}$$

From (18) and (19) we conclude that the length of the period of $\{K_n\}$ (mod p^2) is hp if

$$K_{t+1} \equiv 1 \pmod{p^2},$$
 (20)

$$K_t \equiv K_{t-1} \equiv 0 \pmod{p^2}, \tag{21}$$

for no t < hp. To see that this is indeed the case, we observe that since 20) and (21) also imply that

> $K_{t+1} \equiv 1 \pmod{p},$ (22)

$$K_t \equiv K_{t-1} \equiv 0 \pmod{p}, \tag{23}$$

then by Theorem 3, t = hq for some q. Now assuming that (22) and (23) hold,

			t.			$\neg ha$		—		79					
1	1	1	0	1	1	1		K_{h+1}	L_{h+1}	K _h		1	0	0	
1	0	0	=	1	0	0	=	K _h	L_h	K_{h-1}	Ξ	0	1	0	(mod p^2)
0	1	0		0	1	0		K_{h-1}	L_{h-1}	K_{h-2}		0	0	1	(mod p^2)
Since $h(p) \neq h(p^2)$,															

$$A = \begin{vmatrix} K_{h+1} & L_{h+1} & K_{h} \\ K_{h} & L_{h} & K_{h-1} \\ K_{h-1} & L_{h-1} & K_{h-2} \end{vmatrix} \not\equiv \begin{vmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{vmatrix} \pmod{p^{2}},$$

350

[Aug.

but by (18) and (19),

$$A^{\mathcal{P}} \equiv A^{\mathcal{Q}} \equiv I \pmod{p^2}$$
.

Since $A \not\equiv I \pmod{p^2}$ and p is prime, this implies that p divides q or $p \leq q$ and $t = hq \geq hp$. Thus hp is the length of the period of $\{K_n\} \pmod{p^2}$. Whether the hypothesis $h(p) \neq h(p^2)$ is necessary or whether $h(p^2)$ can ne-ver equal h(p) is an open question. No example of $h(p) = h(p^2)$ was found, yet a proof that none exists was not found either. In the event that k is largest such that $h(p^k) = h(p)$, it can be shown that $h(p^r) = p^{r-k}h(p)$.

Theorem 9: If $K_t \equiv K_{t-1} \equiv 0 \pmod{m}$, then $K_{st+1} \equiv K_{t+1}^s \pmod{m}$ for all positive integers s.

Proof: The proof is similar to the proof of (9).

The example illustrates that at the end of a period, the triple 1, 0, 0 occurs in the sequence $\{K_n\}$ (mod m). In the example, we also saw that adjacent double zeros (not necessarily preceded by 1) occur at equally spaced intervals throughout the period and that adjacent double zeros occur three times within the period. For one period of $\{K_n\}$ (mod 3), we have

in which the adjacent double zeros occur once (at the beginning or end) of a period cycle. A general principle is given by

Theorem 10: If t is the least positive integer such that $K_t \equiv K_{t-1} \equiv 0 \pmod{m}$, then either $K_{t+1} \equiv 1 \pmod{m}$ or $K_{3t+1} \equiv 1 \pmod{m}$ and the length of the period is t or 3t.

Proof: Suppose $K_{t+1} \equiv 1 \pmod{m}$. Then using (6) and $K_t \equiv K_{t-1} \equiv 0 \pmod{m}$ m), we have

$$1 = K_t^2 K_{t-3} + K_{t-1}^3 + K_{t-2}^2 K_{t+1} - K_{t+1} K_{t-1} K_{t-3} - 2K_t K_{t-1} K_{t-3}$$
$$\equiv K_{t-2}^2 K_{t+1} \equiv K_{t+1}^3 \pmod{m},$$

since $K_{t-2} \equiv K_{t+1} \pmod{m}$. By Theorem 9,

$$K_{3t+1} \equiv K_{t+1}^3 \pmod{m}$$

and so we have

 $K_{3t+1} \equiv 1 \pmod{m}$

as required.

To show that $K_{2t+1} \not\equiv 1 \pmod{m}$ if $K_{t+1} \not\equiv 1 \pmod{m}$ we assume the contrary and observe that

$$K_{3t+1} \equiv K_{t+1}^3 \equiv 1 \equiv K_{2t+1} \equiv K_{t+1}^2 \pmod{m}$$
.

SOME PROPERTIES OF A GENERALIZED FIBONACCI SEQUENCE MODULO m [Aug.

Hence,

352

$$K_{t+1}^3 \equiv K_{t+1}^2 \pmod{m}$$
,

which implies that $K_{t+1} \equiv 1 \pmod{m}$ since the g.c.d. $(K_{t+1}^2, m) = 1$. This is a contradiction of our assumption that $K_{t+1} \not\equiv 1 \pmod{m}$.

Remark: If $K_{t-1} \equiv K_t \equiv 0 \pmod{m}$ and $K_{t+1} \not\equiv 1 \pmod{m}$, then we showed in the proof of Theorem 10 that

$$K_{t+1}^3 \equiv 1 \pmod{m}$$
.

It also follows that

$$K_{2++1}^3 \equiv 1 \pmod{m}$$
,

since

$$K_{2t+1}^3 \equiv (K_{t+1}^2)^3 \equiv (K_{t+1}^3)^2 \equiv 1^2 \equiv 1 \pmod{m}.$$

Theorem 10 and the Remark would imply that only integers n which can occur in the sequence $\{K_n\}$ (mod m) immediately preceding and following adjacent double zeros are such that

$$n \equiv 1 \pmod{m}$$
.

or

 $n^3 \equiv 1 \pmod{m}$.

The Remark would also imply that if $n \not\equiv 1 \pmod{m}$, then there exist at least two distinct values n_1 , n_2 such that

$$n_1^3 \equiv n_2^3 \equiv 1 \pmod{m},$$

where n_1 , n_2 are the immediate predecessors and successors of adjacent double zeros in the sequence $\{K_n\} \pmod{m}$.

Theorem 11: If p is prime, h = h(p), and $K_t \equiv K_{t-1} \equiv 0 \pmod{p}$ where t < h, then h = 3t and

$$K_{r} + K_{r+t} + K_{r+2t} \equiv 0 \pmod{p}$$
.

Proof: That h = 3t is an immediate consequence of Theorem 9 since t < h. To prove the second statement, we have by (2),

$$K_{r+t} = K_{r+1}K_t + (K_r + K_{r-1})K_{t-1} + K_rK_{t-2} \equiv K_rK_{t-2} \pmod{p}$$
(24)

since $K_t \equiv K_{t-1} \equiv 0 \pmod{p}$.

$$K_{r+2t} = K_{r+t+1}K_t + (K_{r+t} + K_{r+t-1})K_{t-1} + K_{r+t}K_{t-2} \equiv K_{r+t}K_{t-2} \pmod{p}$$
(25)

$$K_{r+3t} = K_{r+2t+1}K_t + (K_{r+2t} + K_{r+2t-1})K_{t-1} + K_{r+2t}K_{t-2}$$
(26)
$$\equiv K_{r+2t}K_{t-2} \pmod{p}.$$

Now adding the left and right sides of (24), (25), and (26) and using the fact that $K_{r+3t} \equiv K_r \pmod{p}$, we get

$$K_{r+t} + K_{r+2t} + K_r \equiv (K_r + K_{r+t} + K_{r+2t})K_{t-2} \pmod{p}.$$
(27)

Since $K_{t-2} \not\equiv 1 \pmod{p}$ and p is prime, (20) implies that

$$K_r + K_{r+t} + K_{r+2t} \equiv 0 \pmod{p}$$

as required.

REFERENCES

- D. D. Wall, "Fibonacci Series Modulo m," American Math. Monthly, Vol. 67 (1960), pp. 525-532.
- E. B. Dynkin & V. A. Uspenskii, Problems in the Theory of Numbers (Boston: D. C. Heath and Company, 1963), pp. 28-32.
- 3. Marcellus E. Waddill & Louis Sacks, "Another Generalized Fibonacci Sequence," *The Fibonacci Quarterly*, Vol. 5, No. 3 (October 1967), pp. 209-222.
