ACTA ARITHMETICA
LXXXIII.2 (1998)

# The distribution of second order linear recurrence sequences mod $2^m$

by

Mark D. Morgan (College Park, Md.)

**1. Introduction.** Let $\{x_n\}$ be a sequence of residues modulo $2^m$ defined by the recursion relation

$$x_n = x_{n-1} + x_{n-2} \pmod{2^m}.$$

By choosing the pair $\{x_1, x_2\}$, called the *initial state vector*, the entire sequence is determined. A sequence generated by the recursion relation defined above is periodic. If at least one of the elements in the initial state vector is an odd number, then the sequence has period $3 \cdot 2^{m-1}$ and is called a *maximal period sequence* [1]. If $\{x_n\}$ is not a maximal period sequence, let $2^t$ be the highest power of 2 dividing both $x_1$ and $x_2$. Then it can easily be seen that the sequence has period $3 \cdot 2^{m-t-1}$.

By fixing $m$, an equivalence relation can be placed on the sequences. Let $X_i = \{x_i, x_{i+1}\}$. Then $X_1$ and $Y_1$ are *equivalent initial state vectors* if $Y_1 = X_j$ for some $j$. There are $2^{2m} - 2^{2(m-1)} = 3 \cdot 2^{2m-2}$ pairs of numbers modulo $2^m$ which contain at least one odd number. Each equivalence class contains $3 \cdot 2^{m-1}$ such pairs. Therefore the number of equivalence classes of maximal period sequences is $2^{m-1}$.

The main result of this paper is the complete determination of the distribution of any maximal period sequence satisfying the above recursion. In 1992, Jacobson determined the distribution of the Fibonacci numbers modulo $2^m$ (see [4]). The distribution of the Fibonacci numbers becomes stable for $m \geq 5$. In stark contrast, the distribution of the Lucas numbers does not possess the stability property. In this paper, their distribution is completely determined. By using these two distribution functions, the main result is obtained, which states that any maximal period sequence modulo $2^m$ is either equivalent to an odd multiple of the Fibonacci numbers or an

1991 *Mathematics Subject Classification*: Primary 11B39.
*Key words and phrases*: Fibonacci numbers, Lucas numbers, linear recurring sequences.

odd multiple of the Lucas numbers. Thus, the distribution of any maximal period sequence can be obtained by finding the odd number $k$ such that the sequence is equivalent to either $\{k, k\}$ or $\{k, 3k\}$.

The distribution of all of these sequences are highly non-uniform. Early work was done to find moduli for which the Fibonacci numbers are uniformly distributed. By the work of Niederreiter [6] and Kuipers and Shiue [5], the only moduli for which the Fibonacci numbers are uniformly distributed are $5^k$ for all $k$. In recent years, more general recursions of the form

$$x_n = ax_{n-1} + bx_{n-2} \pmod{2^m}, \qquad x_0 = 0,\ x_1 = 1,$$

have been studied to determine their distribution and stability properties.

Let $Z_{2^m}(a)$ be the number of occurrences of the residue $a$ in one period of the sequence $\{x_n\}$. This function will be called the *frequency distribution function*. A sequence is called *stable modulo* 2 if the range of the frequency distribution function remains constant for $m \geq m_0$ for some $m_0$. The Fibonacci numbers are stable modulo 2 with stability beginning at $m_0 = 5$ (see [4]). A criterion for stability was determined by Carlip and Jacobson [2]. In Section 3, $Z_{2^m}(a)$ is obtained for the Lucas numbers, and the range of the frequency distribution function is proved to become infinite as $m \to \infty$. This shows that stability of a sequence depends on the choice of initial state vector.

In [3], Carlip and Jacobson have determined the distribution for a number of sequences satisfying the more general recursion given above. Note that in the cases studied by Carlip and Jacobson the choice of initial state vector is restricted to $x_0 = 0$ and $x_1 = 1$. In addition, the distributions determined in [3] have also been stable sequences with stability beginning at arbitrary levels.

In Section 2, several standard facts are stated concerning the Fibonacci numbers and linear recurring sequences. A large part of Section 3 is devoted to proving several lemmas needed to find the distribution of the Lucas numbers modulo $2^m$. In Section 4, the distribution of any maximal period sequence is obtained by extending the results of Section 3. In addition, the proof of Theorem 3 produces a complete list of equivalence classes of maximal period sequences.

**2. Preliminary facts.** Let $F_n$ and $L_n$ denote the $n$th Fibonacci number and the $n$th Lucas number respectively. The following are standard facts concerning the Fibonacci numbers which will be used throughout the work.

FACT 1. $F_{m+n} = F_{m-1}F_n + F_mF_{n+1}$.

FACT 2. *If* $x_n = x_{n-1} + x_{n-2}$, *then for* $n \geq 3$, $x_n = x_1F_{n-2} + x_2F_{n-1}$.

FACT 3. *Suppose* $x_n = x_{n-1} + x_{n-2}$. *If* $y_1 = tx_1$ *and* $y_2 = tx_2$ *and* $y_n = y_{n-1} + y_{n-2}$, *then* $y_n = tx_n$.

FACT 4. *For* $n \geq 1$,

$$\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}^n = \begin{pmatrix} F_{n+1} & F_n \\ F_n & F_{n-1} \end{pmatrix}.$$

Jacobson has proved the following congruence relation concerning the Fibonacci numbers in Lemma 1 of [4].

LEMMA 1. *Let* $m \geq 5$. *Then*

$$F_{3\cdot 2^{m-2}} \equiv 2^m \pmod{2^{m+2}},$$
$$F_{3\cdot 2^{m-3}-1} \equiv 1 - 2^{m-2} \pmod{2^m}.$$

LEMMA 2. *Let* $x_n = x_{n-1} + x_{n-2} \pmod{2^m}$. *If* $m \geq 3$ *and* $n \geq 0$, *then*

$$x_{n+3\cdot 2^{m-2}} \equiv \begin{cases} x_n \pmod{2^m} & \text{if } x_n \text{ is even,} \\ x_n + 2^{m-1} \pmod{2^m} & \text{if } x_n \text{ is odd.} \end{cases}$$

Proof. Jacobson has proved this lemma for $x_n = F_n$ and $m \geq 5$ in Lemma 3 of [4]. Hence, Lemma 1 implies that

$$F_{3\cdot 2^{m-2}} \equiv 0 \pmod{2^m}, \quad F_{3\cdot 2^{m-2}-1} \equiv 1 + 2^{m-1} \pmod{2^m}.$$

These statements can also be verified for $m = 3$ and 4. Applying Fact 2 implies

$$\begin{aligned} x_{n+3\cdot 2^{m-2}} &= x_1 F_{n+3\cdot 2^{m-2}-2} + x_2 F_{n+3\cdot 2^{m-2}-1} \\ &= x_1(F_{n-3}F_{3\cdot 2^{m-2}} + F_{n-2}F_{3\cdot 2^{m-2}+1}) \\ &\quad + x_2(F_{n-2}F_{3\cdot 2^{m-2}} + F_{n-1}F_{3\cdot 2^{m-2}+1}) \\ &= F_{3\cdot 2^{m-2}}(x_1F_{n-3} + x_2F_{n-2}) + F_{3\cdot 2^{m-2}+1}(x_1F_{n-2} + x_2F_{n-1}) \\ &= F_{3\cdot 2^{m-2}}x_{n-1} + F_{3\cdot 2^{m-2}+1}x_n \\ &\equiv x_n(1 + 2^{m-1}) \pmod{2^m}. \end{aligned}$$

Therefore, the result follows by this computation. ∎

**3. Distribution of Fibonacci and Lucas numbers mod $2^m$.** The frequency distribution functions for the sequences formed by the Fibonacci numbers and the Lucas numbers are quite different. The frequency distribution function for $\{F_n\} \pmod{2^m}$ has the property that $Z_{2^m}(a) = Z_{2^{m+1}}(a)$ for $m \geq 5$. In stark contrast, the sequence formed by $\{L_n\} \pmod{2^m}$ does not possess this stability property for all values of $a$. Theorem 2 shows that when $a \equiv 2 \pmod{2^m}$, $Z_{2^m}(a) \to \infty$ as $m \to \infty$. However, for all other values of $a$, this stability property holds for $m \geq m_0$ for some $m_0$.

THEOREM 1 (Jacobson). *Let $Z_{2^m}(a)$ be the frequency distribution function for $\{F_n\} \pmod{2^m}$. Then*

$$Z_2(0) = Z_4(0) = Z_4(2) = 1,$$
$$Z_2(1) = Z_8(0) = Z_8(2) = Z_{16}(0) = Z_{16}(8) = 2,$$
$$Z_{16}(2) = 4,$$
$$Z_{2^m}(a) = \begin{cases} 1 & \text{if } a \equiv 3 \pmod 4 \text{ and } 2 \le m \le 4, \\ 3 & \text{if } a \equiv 1 \pmod 4 \text{ and } 2 \le m \le 4, \\ 0 & \text{in all other cases where } 2 \le m \le 4. \end{cases}$$

*For $m \ge 5$,*

$$Z_{2^m}(a) = \begin{cases} 1 & \text{if } a \equiv 3 \pmod 4, \\ 3 & \text{if } a \equiv 1 \pmod 4, \\ 2 & \text{if } a \equiv 0 \pmod 8, \\ 8 & \text{if } a \equiv 2 \pmod{32}, \\ 0 & \text{otherwise.} \end{cases}$$

THEOREM 2. *Let $Z_{2^m}(a)$ be the frequency distribution function for the sequence $\{L_n\} \pmod{2^m}$. Then*

$$Z_2(0) = Z_4(0) = 1, \qquad Z_2(1) = 2,$$
$$Z_4(0) = Z_4(2) = 1, \qquad Z_{32}(18) = 4,$$
$$Z_{64}(18) = Z_{128}(66) = 8, \qquad Z_{256}(66) = 16,$$
$$Z_{2^m}(a) = \begin{cases} 1 & \text{if } a \equiv 1 \pmod 4 \text{ and } 2 \le m \le 8, \\ 3 & \text{if } a \equiv 3 \pmod 4 \text{ and } 2 \le m \le 8, \\ 2 & \text{if } a \equiv 4 \pmod 8 \text{ and } 3 \le m \le 8, \\ 2^{\lfloor m/2 \rfloor} & \text{if } a \equiv 2 \pmod{2^m} \text{ and } 3 \le m \le 8, \\ 16 & \text{if } a \equiv 18 \pmod{128} \text{ and } m = 7 \text{ or } 8, \\ 0 & \text{in all other cases where } 2 \le m \le 8. \end{cases}$$

*For $m \ge 9$,*

$$Z_{2^m}(a) = \begin{cases} 1 & \text{if } a \equiv 1 \pmod 4, \\ 3 & \text{if } a \equiv 3 \pmod 4, \\ 2 & \text{if } a \equiv 4 \pmod 8, \\ 16 & \text{if } a \equiv 18 \pmod{128}, \\ 2^{t+2} & \text{if } a \equiv 2+5 \cdot 2^{2t} \pmod{2^{2t+3}} \text{ for } 3 \le t \le \lfloor (m-3)/2 \rfloor, \\ 2^{\lfloor m/2 \rfloor} & \text{if } a \equiv 2 \pmod{2^m}, \\ 2^{\lfloor m/2 \rfloor} & \text{if } a \equiv 2 + 2^{m-1} \pmod{2^m} \text{ and } m \text{ is odd,} \\ & \text{or } a \equiv 2 + 2^{m-2} \pmod{2^m} \text{ and } m \text{ is even,} \\ 0 & \text{otherwise.} \end{cases}$$

The proof of Theorem 2 depends on the following series of lemmas. For $m \le 8$, the values of the frequency distribution function can be verified by

computation. So the induction arguments that follow will start with a base case $m$ where $m \le 9$.

In order to obtain the desired result, it is convenient to investigate certain subsequences of $\{L_n\}$. Define $W_n = L_{6n}$ and $T_n = W_{2^{n-1}}$. The Lucas numbers that have indices which are multiples of six are all congruent to 2 (mod 8). These prove to be the most challenging and interesting aspect of the frequency distribution function, and so special attention should be given to the sequence $\{W_n\}$. A basic fact about the Lucas numbers is $L_n = F_{n-1} + F_{n+1}$ for all $n$. So let

$$B = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}^6 = \begin{pmatrix} 13 & 8 \\ 8 & 5 \end{pmatrix}.$$

Hence Fact 4 implies

$$L_n = \operatorname{tr} \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}^n \quad \text{and} \quad W_n = \operatorname{tr} \begin{pmatrix} 13 & 8 \\ 8 & 5 \end{pmatrix}^n.$$

Let $\lambda_1$ and $\lambda_2$ be the eigenvalues for the matrix $B$. Then $\lambda_1 = 9 + 4\sqrt{5}$ and $\lambda_2 = 9 - 4\sqrt{5}$. From the above facts, $W_n = \lambda_1^n + \lambda_2^n$ for all positive integers $n$. Note that

$$\lambda_1^{n+1} + \lambda_2^{n+1} = (\lambda_1^n + \lambda_2^n)(\lambda_1 + \lambda_2) - \lambda_1\lambda_2(\lambda_1^{n-1} + \lambda_2^{n-1}).$$

Translating this into a statement concerning the sequence $\{W_n\}$ gives

$$W_{n+1} = W_n W_1 - \lambda_1\lambda_2 W_{n-1} = 18W_n - W_{n-1}. \tag{1}$$

Hence the sequence $\{W_n\}$ obeys a different recursion with $W_0 = 2$ and $W_1 = 18$.

There is a basic fact concerning $2 \times 2$ matrices which relates the trace of a matrix with the trace of the square of the matrix.

Fact 5. *Let $A$ be a $2 \times 2$ matrix. Then* $\operatorname{tr}(A^2) = (\operatorname{tr} A)^2 - 2 \det A$.

Applying this fact yields

$$W_{2n} = (W_n)^2 - 2. \tag{2}$$

Hence the sequence $\{T_n\}$ can be defined by

$$T_{n+1} = T_n^2 - 2 \quad \text{where } T_1 = 18. \tag{3}$$

Lemma 3. *$T_n \equiv 2 \pmod{2^m}$ if and only if $m \le 2n + 2$.*

Proof. The first step is to prove that if $m = 2n + 2$, then $T_n \equiv 2 \pmod{2^m}$. If this is true, then the statement holds for all $m < 2n + 2$. Clearly the result holds for $n = 1$ since $T_1 = 18 \equiv 2 \pmod{16}$. So suppose $T_n \equiv 2 \pmod{2^m}$, where $m = 2n + 2$. Then $T_n = 2 + 2^m z$ for some integer $z$. Then

$$T_{n+1} = T_n^2 - 2 = 2 + 2^{m+2}z + 2^{2m}z^2 \equiv 2 \pmod{2^{m+2}},$$

which completes the induction. It is sufficient to show that if $m = 2n + 3$, then $T_n \equiv 2 + 2^{m-1} \pmod{2^m}$. Clearly the result is true for $n = 1$, since $T_1 \equiv 18 \pmod{32}$. So assume $T_n \equiv 2 + 2^{m-1} \pmod{2^m}$ for $m = 2n + 3$. Then $T_n = 2 + 2^{m-1} + 2^m z$ for some integer $z$. So

$$T_{n+1} = (2 + 2^{m-1} + 2^m z)^2 - 2 \equiv 2 + 2^{m+1} \pmod{2^{m+2}},$$

which will complete the proof. ∎

Note that the condition in the previous lemma, $m \le 2n + 2$, can be rewritten as $n \ge \lceil m/2 \rceil - 1$. The relationship between the sequences $\{T_n\}$ and $\{W_n\}$ implies that $W_r \equiv 2 \pmod{2^m}$ where $r = 2^{\lceil m/2 \rceil - 2}$. Now that one occurrence of the residue 2 has been located in the sequence $\{W_n\}$, the next step is to locate the remainder of them.

LEMMA 4. *Suppose $m \ge 3$ and let $r = 2^{\lceil m/2 \rceil - 2}$. Then for all integers $k$ and $\mu$,*

$$W_{k+\mu r} \equiv 2W_k - W_{k-\mu r} \pmod{2^{m+1}}.$$

*In addition, $W_{kr} \equiv 2 \pmod{2^m}$.*

Proof. First assume $\mu = 1$. Let $\lambda_1$ and $\lambda_2$ be the eigenvalues of the matrix $B$ as defined previously. Without loss of generality, assume $k \ge r$ since the sequence $\{W_n\} \pmod{2^m}$ is periodic. Then

$$\begin{aligned} W_{k+r} &= \lambda_1^{k+r} + \lambda_2^{k+r} = (\lambda_1^k + \lambda_2^k)(\lambda_1^r + \lambda_2^r) - \lambda_1^r \lambda_2^r (\lambda_1^{k-r} + \lambda_2^{k-r}) \\ &= W_k W_r - W_{k-r}. \end{aligned}$$

By the previous lemma, $W_r \equiv 2 \pmod{2^m}$. So $W_r = 2 + 2^m z$ for some integer $z$. Hence

$$W_{r+k} = 2W_k + 2^m z W_k - W_{k-r} \equiv 2W_k - W_{k-r} \pmod{2^{m+1}},$$

since every term in the sequence $\{W_n\}$ is even. Noting that $W_0 \equiv W_r \equiv 2 \pmod{2^m}$ and using the above recursion, we obtain $W_{kr} \equiv 2 \pmod{2^m}$ for all integers $k$. To complete the proof, it is necessary to consider $\mu > 1$. By the same argument as above, replace $r$ by $\mu r$. But since $W_{\mu r} \equiv 2 \pmod{2^m}$ for all $\mu$, the result is obtained. ∎

LEMMA 5. *For $m \ge 6$, the period of the sequence $\{W_n\} \pmod{2^m}$ is $2^{m-5}$.*

Proof. The result can be showed by direct computation for $m = 6, 7$, and 8. So assume that the sequence $\{W_n\}$ reduced modulo $2^m$ has period $p = 2^{m-5}$ where $m \ge 8$. Then by reducing $\{W_n\}$ modulo $2^{m+1}$, the period must be a multiple of $p$. Note that for $m \ge 8$, $2^{m-5} > 2^{\lceil m/2 \rceil - 2}$. Thus for $m \ge 8$, $p/2$ is a multiple of $2^{\lceil m/2 \rceil - 2}$. Hence by Lemma 4, $W_{p/2} \equiv 2 \pmod{2^m}$. Since $p$ is the period, this forces $W_{p/2+1} \equiv 18 + 2^{m-1} \pmod{2^m}$.

Hence $W_{p/2+1} \equiv 18 + 2^{m-1} + 2^m z \pmod{2^{m+1}}$ for some integer $z$. Then using Lemma 4 with $k = p/2 + 1$ and $\mu r = p/2$,

$$W_{p+1} \equiv 2(18 + 2^{m-1} + 2^m z) - 18 \equiv 18 + 2^m \pmod{2^{m+1}}.$$

Now, applying the lemma again with $k = p + 1$ and $\mu r = p$ yields

$$W_{2p+1} \equiv 2(18 - 2^m) - 18 \equiv 18 \pmod{2^{m+1}}.$$

Since $W_{2p} \equiv 2 \pmod{2^{m+1}}$, the period modulo $2^{m+1}$ must be $2p$. Hence, induction completes the proof. ∎

Lemma 2 shows how the second half of the period of the sequence $\{L_n\}$ depends on the first half of the period. Now, the same can be done for the sequence $\{W_n\}$.

LEMMA 6. *For $m \geq 8$ and all integers $k$,*

$$W_{k+2^{m-6}} \equiv \begin{cases} W_k \pmod{2^m} & \text{if } k \text{ is even,} \\ W_k + 2^{m-1} \pmod{2^m} & \text{if } k \text{ is odd.} \end{cases}$$

Proof. The proof will follow by induction on $k$. In the proof of the previous lemma, it is apparent that

$$W_0 \equiv W_{2^{m-6}} \equiv 2 \pmod{2^m}, \quad W_1 \equiv 18 \pmod{2^m},$$
$$W_{1+2^{m-6}} \equiv 18 + 2^{m-1} \pmod{2^m}.$$

Hence the lemma holds for $k = 0$ and $k = 1$. Assume the lemma holds for all integers less than or equal to $k$. First suppose $k$ is even. Then

$$\begin{aligned} W_{k+1+2^{m-6}} &= 18W_{k+2^{m-6}} - W_{k-1+2^{m-6}} \\ &\equiv 18W_k - W_{k-1} - 2^{m-1} \equiv W_{k+1} + 2^{m-1} \pmod{2^m}. \end{aligned}$$

Now assume $k$ is odd. Then

$$W_{k+1+2^{m-6}} \equiv 18(W_k + 2^{m-1}) - W_{k-1} \equiv W_{k+1} \pmod{2^m}.$$

Hence the result holds for all $k \geq 0$. By periodicity of the sequence, the result also holds for negative values of $k$. ∎

LEMMA 7. *Let $m \geq 6$. Then for all integers $k$,*

$$W_k \equiv W_{-k} \pmod{2^m}.$$

Proof. Define the $\{W_n\}$ sequence also for negative values of $n$. Then since $W_0 = 2$, $W_1 = 18$, we have $W_{-1} = 18$. Hence $W_t = W_{-t}$ for $t = 0$ and $t = 1$. Assume that this holds for $t = 0, 1, \ldots, k$. Then

$$W_{k+1} = 18W_k - W_{k-1} = 18W_{-k} - W_{1-k} = W_{-k-1},$$

which completes the proof. ∎

LEMMA 8. *Let $m \geq 6$ and $r = r(m) = 2^{\lceil m/2 \rceil - 2}$. Then for all integers $k$,*

$$W_{r(m)(2k+1)/2} \equiv \begin{cases} 2 + 2^{m-2} \pmod{2^m} & \text{if } m \text{ is even,} \\ 2 + 2^{m-1} \pmod{2^m} & \text{if } m \text{ is odd.} \end{cases}$$

Proof. First assume $k = 0$ and $m$ is even. Then when $m = 6$, $r(m)/2 = 1$, and since $W_1 \equiv 18 \pmod{2^6}$, the result holds. So assume that the result holds for all even $j$ with $6 \leq j \leq m$. Then

$$W_{r(m)/2} = 2 + 2^{m-2} + 2^m z$$

for some integer $z$. Then by (2),

$$\begin{aligned} W_{r(m)} &= (2 + 2^{m-2} + 2^m z)^2 - 2 \\ &= 2 + 2^m + 2^{2m-4} + 2^{2m} z^2 + 2^{2m-1} z + 2^{m+2} z \\ &\equiv 2 + 2^m \pmod{2^{m+2}}. \end{aligned}$$

Since $r(m) = r(m+2)/2$, we obtain $W_{r(m)/2} \equiv 2 + 2^{m-2} \pmod{2^m}$ when $m$ is even.

Now assume $m$ is odd. Then $r(7)/2 = 2$ and since $W_2 \equiv 66 \pmod{2^7}$, the result holds for $m = 7$. Now by a similar inductive argument as above, assume $W_{r(m)/2} = 2 + 2^{m-1} + 2^m z$ for some integer $z$. Then

$$\begin{aligned} W_{r(m)} &= (2 + 2^{m-1} + 2^m z)^2 - 2 \\ &= 2 + 2^{m+1} + 2^{2m-2} + 2^{2m} z^2 + 2^{2m} z + 2^{m+2} z \\ &\equiv 2 + 2^{m+1} \pmod{2^{m+2}}. \end{aligned}$$

Therefore, $W_{r(m)/2} \equiv 2 + 2^{m-1} \pmod{2^m}$ where $m$ is odd and $m \geq 7$.

Next assume $k = 1$. Then Lemmas 4 and 7 imply that

$$W_{3r(m)/2} \equiv 2W_{r(m)/2} - W_{-r(m)/2} \pmod{2^m} \equiv W_{r(m)/2} \pmod{2^m}.$$

Assume $k > 1$ and that the statement holds for all values less than $k$. Then

$$\begin{aligned} W_{r(m)(2k+1)/2} &\equiv 2W_{r(m)(2k-1)/2} - W_{r(m)(2k-3)/2} \pmod{2^m} \\ &\equiv W_{r(m)/2} \pmod{2^m} \end{aligned}$$

by the induction hypothesis. Therefore the statement holds for all positive integers $k$ and must also hold for all negative values of $k$. ∎

LEMMA 9. *Suppose $m \geq 3$ and $k \equiv 3 \pmod 6$. Then*

$$L_{k+3\cdot 2^{m-2}} \equiv L_k + 2^m \pmod{2^{m+1}}.$$

Proof. The lemma can be shown for $m = 3$ and 4 by direct computation. So assume $m \geq 5$. Using the fact that $L_n = F_{n-1} + F_{n+1}$ shows

$$L_{k+3\cdot 2^{m-2}} - L_k = F_{k+3\cdot 2^{m-2}-1} + F_{k+3\cdot 2^{m-2}+1} - F_{k-1} - F_{k+1}.$$

Since $k \equiv 3 \pmod 6$, $F_k$ is even and $F_{k-1}$ and $F_{k-2}$ are odd. Lemma 1 implies that

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

Hence $F_{3\cdot 2^{m-2}+1} \equiv 1 + 2^m - 2^{m-1} \pmod{2^{m+1}}$. Then by Fact 1,

$$\begin{aligned} F_{k+3\cdot 2^{m-2}-1} &= F_{k-2}F_{3\cdot 2^{m-2}} + F_{k-1}F_{3\cdot 2^{m-2}+1} \\ &\equiv 2^m + F_{k-1}(1 + 2^m - 2^{m-1}) \pmod{2^{m+1}} \\ &\equiv F_{k-1}(1 - 2^{m-1}) \pmod{2^{m+1}}. \end{aligned}$$

Similarly,

$$\begin{aligned} F_{k+3\cdot 2^{m-2}+1} &= F_kF_{3\cdot 2^{m-2}} + F_{k+1}F_{3\cdot 2^{m-2}+1} \\ &\equiv 2^mF_k + F_{k+1}(1 + 2^m - 2^{m-1}) \pmod{2^{m+1}} \\ &\equiv F_{k+1}(1 + 2^m - 2^{m-1}) \pmod{2^{m+1}}. \end{aligned}$$

Then

$$\begin{aligned} L_{k+3\cdot 2^{m-2}} - L_k &\equiv F_{k-1}(1 - 2^{m-1}) + F_{k+1}(1 + 2^m - 2^{m-1}) \\ &\quad -F_{k-1} - F_{k+1} \pmod{2^{m+1}} \\ &\equiv -2^{m-1}F_{k-1} - 2^{m-1}F_{k+1} + 2^mF_{k+1} \pmod{2^{m+1}} \\ &\equiv -2^{m-1}L_k + 2^mF_{k+1} \pmod{2^{m+1}}. \end{aligned}$$

Since $k \equiv 3 \pmod 6$, $L_k \equiv 0 \pmod 4$. Also, $F_{k+1}$ is odd. Thus

$$-2^{m-1}L_k + 2^mF_{k+1} \equiv 2^m \pmod{2^{m+1}},$$

which completes the proof. ∎

It is now possible to proceed with the proof of Theorem 2. The proofs of the cases $a \equiv 1 \pmod 2$ and $a \equiv 4 \pmod 8$ contain ideas which are similar to Jacobson's proof of Theorem 1. The remainder of the cases contain ideas which are not found in Jacobson's proof.

*Proof of Theorem 2*

Case 1: $a \equiv 1 \pmod 2$. Suppose $L_k \equiv a \pmod{2^m}$. Either $L_k \equiv a \pmod{2^{m+1}}$ or $L_k \equiv a + 2^m \pmod{2^{m+1}}$. Then Lemma 2 implies that $L_{k+3\cdot 2^{m-1}} \equiv L_k + 2^m \pmod{2^{m+1}}$ for $m \geq 2$. Hence by lifting the sequence $\{L_n\}$ modulo $2^{m+1}$, either $L_k$ or $L_{k+3\cdot 2^{m-1}} \equiv a \pmod{2^{m+1}}$, but not both. So $Z_{2^m}(a) = Z_{2^{m+1}}(a)$ for $m \geq 2$. Therefore, $Z_{2^m}(a) = 1$ if $a \equiv 1 \pmod 4$, and $Z_{2^m}(a) = 3$ if $a \equiv 3 \pmod 4$ for $m \geq 2$.

Case 2: $a \equiv 4 \pmod 8$. First note that $Z_8(a) = 2$. So suppose $Z_{2^m}(a) = 2$. If $L_k \equiv a \pmod{2^m}$, then $k \equiv 3 \pmod 6$. When looking at the sequence modulo $2^{m+1}$, it is necessary to examine the sequential elements with indices

$k, k+3\cdot 2^{m-2}, k+3\cdot 2^{m-1}$, and $k+3\cdot 2^{m-2}+3\cdot 2^{m-1}$. It is apparent from Lemma 2 that

$$L_k \equiv L_{k+3\cdot 2^{m-1}} \pmod{2^{m+1}}$$

and

$$L_{k+3\cdot 2^{m-2}} \equiv L_{k+3\cdot 2^{m-2}+3\cdot 2^{m-1}} \pmod{2^{m+1}}.$$

However, Lemma 9 implies that $L_k$ and $L_{k+3\cdot 2^{m-2}}$ are different modulo $2^{m+1}$. Hence, $Z_{2^{m+1}}(a) = 2$. Therefore, $Z_{2^m}(a) = 2$ for $m \geq 3$.

Case 3: $a \equiv 2 \pmod{2^m}$. By Lemma 4, $W_{kr} \equiv 2 \pmod{2^m}$ for all integers $k$ where $r = 2^{\lceil m/2\rceil - 2}$ and $m \geq 3$. The subsequence $\{W_n\}$ of $\{L_n\}$ contains $2^{m-2}$ elements and every $r$th element is a 2. So

$$Z_{2^m}(a) \geq \frac{2^{m-2}}{2^{\lceil m/2\rceil - 2}} = 2^{\lfloor m/2\rfloor}$$

for $m \geq 3$. Equality is shown later.

Case 4: $a \equiv 2 + 2^{m-2} \pmod{2^m}$, $m$ even. By Lemma 8, $W_{r(2k+1)/2} \equiv 2 + 2^{m-2} \pmod{2^m}$ for all integers $k$ where $r$ is defined as before and $m \geq 6$. So there is at least one occurrence of $2 + 2^{m-2}$ in any $r$ consecutive sequence members of $\{W_n\}$. So by the same argument as in the previous case, $Z_{2^m}(a) \geq 2^{\lfloor m/2\rfloor}$ for $m \geq 6$.

Case 5: $a \equiv 2 + 2^{m-1} \pmod{2^m}$, $m$ odd. The argument is analogous to the previous case. However, the odd case of Lemma 8 is used to get $Z_{2^m}(a) \geq 2^{\lfloor m/2\rfloor}$ for $m \geq 7$.

Case 6: $a \equiv 18 \pmod{128}$. First note that $Z_{128}(a) = 16$ by computation. Define $\overline{Z}_{2^m}(a)$ to be the number of occurrences of the residue $a$ in one period of the sequence $\{W_n\} \pmod{2^m}$. Then for $m \geq 6$ and any residue $b$ in $\{W_n\}$,

$$Z_{2^m}(b) = 8\overline{Z}_{2^m}(b).$$

So $\overline{Z}_{128}(a) = 2$. Note that if $W_k \equiv a \pmod{2^m}$, then $k$ is odd, since one period of $\{W_n\} \pmod{128}$ is $\{2, 18, 66, 18\}$. By Lemma 7, $W_{2^{m-5}-k}$ is the only other occurrence of $a$ for all positive indices less than $2^{m-5}$. So assume $\overline{Z}_{2^m}(a) = 2$. To count the number of occurrences of $a$ modulo $2^{m+1}$, it is necessary to examine the sequential elements with indices $k, 2^{m-5} - k, k + 2^{m-5}$, and $2^{m-4} - k$. Lemma 6 implies that $W_{k+2^{m-5}} \equiv W_k + 2^m \pmod{2^{m+1}}$. As in a previous argument, exactly two of these four elements must be $a$. Hence, $\overline{Z}_{2^{m+1}}(a) = \overline{Z}_{2^m}(a)$ for $m \geq 8$. Therefore, $Z_{2^m}(a) = 16$ for $m \geq 7$.

Case 7: $a \equiv 2+5(2^6) \pmod{512}$. Note that this case applies only when $m \geq 9$. Let

$$A_0 = \{18 + 2^7 z \mid 0 \leq z < 2^{m-7}\}.$$

Note that $A_0$ is the set of residues modulo $2^m$ which are congruent to 18 modulo 128. Also let

$$A_1 = \{322 + 2^9 z \mid 0 \le z < 2^{m-9}\}.$$

Similarly $A_1$ is the set of all residues modulo $2^m$ which are congruent to 322 modulo 512. Let $f$ be a function mapping $A_0$ into $\mathbb{Z}/2^m\mathbb{Z}$ defined by $f(x) = x^2 - 2$. Then

$$\begin{aligned} f(18 + 2^7 z) &\equiv 322 + 2^9(9z) + 2^{14} z^2 \pmod{2^m} \\ &\equiv 322 + 2^9(9z + 2^5 z^2) \pmod{2^m} \equiv 322 + 2^9 \widetilde{z} \pmod{2^m}, \end{aligned}$$

where $\widetilde{z}$ is an integer such that $0 \le \widetilde{z} < 2^{m-9}$. This implies that $f(A_0) \subset A_1$. Now suppose $18 + 2^7 z_1$ and $18 + 2^7 z_2$ are elements of $A_0$ such that

$$f(18 + 2^7 z_1) \equiv f(18 + 2^7 z_2) \pmod{2^m}.$$

Then

$$\begin{aligned} 322 + 2^9(9z_1 + 32z_1^2) &\equiv 322 + 2^9(9z_2 + 32z_2^2) \pmod{2^m}, \\ 9(z_1 - z_2) - 32(z_2^2 - z_1^2) &\equiv 0 \pmod{2^{m-9}}, \\ (z_1 - z_2)(9 + 32(z_1 + z_2)) &\equiv 0 \pmod{2^{m-9}}, \\ z_1 - z_2 &\equiv 0 \pmod{2^{m-9}}. \end{aligned}$$

Therefore, $z_1 \equiv z_2 \pmod{2^{m-9}}$, which implies that $f(A_0)$ has at least $2^{m-9}$ elements, and so $f(A_0) = A_1$. Also, the function $f$ which maps $A_0$ to $f(A_0)$ is a 4-to-1 function. Let $b \in A_1$. Then there are exactly 4 distinct values in $A_0$, say $a_1, a_2, a_3$, and $a_4$, such that $f(a_i) = b$ for each $i$. Then by a previous case, $\overline{Z}_{2^m}(a_i) = 2$ for each $i$, where $\overline{Z}_{2^m}(a_i)$ is as defined before. By looking at the sequence $\{W_n\}$, recall by (2) that $W_{2k} \equiv b \pmod{2^m}$ if and only if $W_k \equiv a_i \pmod{2^m}$ for some $i = 1, 2, 3$, or 4. By Lemma 7, one occurrence of $a_i$ in the sequence $\{W_n\}$ lies in the first half of the period, and the other in the second half. By doubling the indices to find the locations of $b$, half of the occurrences will fall within the first period and half in the second period of $\{W_n\}$. Therefore $\overline{Z}_{2^m}(b) = 4$, which implies that $Z_{2^m}(b) = 32$.

Case 8: $a \equiv 2 + 5(2^{2t}) \pmod{2^{2t+3}}$ for $3 \le t \le \lfloor (m-3)/2 \rfloor$. This was proved in the previous case for $t = 3$. Let

$$A_n = \{2 + 5 \cdot 2^{2(n+2)} + 2^{7+2n} z \mid 0 \le z < 2^{m-7-2n}\}$$

for $1 \le n \le \lfloor (m-7)/2 \rfloor$. Note that $A_1$ is consistent with its previous definition, and let $f$ and $A_0$ be as before. The claim is that $f^n(A_0) = A_n$ for $1 \le n \le \lfloor (m-7)/2 \rfloor$. The case $n = 1$ was shown previously. Let $t_j = 2 + 5 \cdot 2^{2(n+1)} + 2^{5+2n} z_j \in A_{n-1}$ for $2 \le n < \lfloor (m-7)/2 \rfloor$. Then

$$\begin{aligned} f(t_j) &= 2 + 5 \cdot 2^{2(n+2)} + 25 \cdot 2^{4(n+1)} + 2^{10+4n} z_j^2 + 2^{7+2n} z_j + 5 \cdot 2^{4n+8} z_j \\ &= 2 + 5 \cdot 2^{2(n+2)} + 2^{7+2n}(z_j + 2^{3+2n} z_j^2 + 25 \cdot 2^{2n-3} + 5 z_j \cdot 2^{2n+1}) \\ &\equiv 2 + 5 \cdot 2^{2(n+2)} + 2^{7+2n} y \pmod{2^m} \end{aligned}$$

for some integer $y$ where $0 \le y < 2^{m-7-2n}$. Thus $f(t_j) \in A_n$, and $f(A_{n-1}) \subset A_n$. Suppose $t_1$ and $t_2$ are in $A_{n-1}$ such that $f(t_1) \equiv f(t_2) \pmod{2^m}$. Then

$$\begin{aligned} &2^{7+2n}(2^{3+2n} z_1^2 + (1 + 5 \cdot 2^{2n+1}) z_1 + 25 \cdot 2^{2n-3}) \\ &\qquad \equiv 2^{7+2n}(2^{3+2n} z_2^2 + (1 + 5 \cdot 2^{2n+1}) z_2 + 25 \cdot 2^{2n-3}) \pmod{2^m}, \\ &2^{3+2n} z_1^2 + (1 + 5 \cdot 2^{2n+1}) z_1 + 25 \cdot 2^{2n-3} \\ &\qquad \equiv 2^{3+2n} z_2^2 + (1 + 5 \cdot 2^{2n+1}) z_2 + 25 \cdot 2^{2n-3} \pmod{2^{m-7-2n}}, \\ &\quad 2^{3+2n}(z_1^2 - z_2^2) + (1 + 5 \cdot 2^{2n+1})(z_1 - z_2) \equiv 0 \pmod{2^{m-7-2n}}, \\ &\quad (z_1 - z_2)(2^{3+2n}(z_1 + z_2) + 1 + 5 \cdot 2^{2n+1}) \equiv 0 \pmod{2^{m-7-2n}}, \\ &\qquad z_1 - z_2 \equiv 0 \pmod{2^{m-7-2n}}. \end{aligned}$$

Therefore $|f(A_{n-1})| \ge 2^{m-7-2n}$. However, $|A_n| = 2^{m-7-2n}$, and so $f(A_{n-1}) = A_n$, which proves the claim. In addition, $f$ is a 4-to-1 function mapping $A_{n-1}$ onto $A_n$. Note that since $a \equiv 2 + 5 \cdot 2^{2t} \pmod{2^{2t+3}}$ for $3 \le t \le \lfloor (m-3)/2 \rfloor$, $a \in A_{t-2}$. Let $r = t - 2$. Then the case $t = 3$ showed that $Z_{2^m}(a) = 2^5$ if $a \in A_1$. So suppose $Z_{2^m}(a) = 2^{r+4}$ for all $a \in A_r$ where $r < \lfloor (m-7)/2 \rfloor$. Now suppose $b \in A_{r+1}$. Then there are 4 distinct values in $A_r$, say $a_1, a_2, a_3$, and $a_4$, such that $f(a_i) = b$ for each $i$. So in order to look for occurrences of $b$ in the sequence $\{W_n\}$, it suffices to double the indices where each $a_i$ occurs. So by the same argument as in the $t = 3$ case, $Z_{2^m}(b) = 2 Z_{2^m}(a_i)$. Hence, $Z_{2^m}(b) = 2^{r+5}$ if $b \in A_{r+1}$. Therefore, since $a \in A_r$, $Z_{2^m}(a) = 2^{r+4} = 2^{t+2}$.

Finally, to verify that the entire frequency distribution function has been determined, it is sufficient to check that

$$\sum_{j=0}^{2^m - 1} Z_{2^m}(j) = 3 \cdot 2^{m-1}.$$

This will force the inequalities found before to be equalities. Indeed,

$$\begin{aligned} \sum_{j=0}^{2^m - 1} Z_{2^m}(j) &= 1(2^{m-2}) + 3(2^{m-2}) + 2(2^{m-3}) + 16(2^{m-7}) + 2(2^{\lfloor m/2 \rfloor}) \\ &\quad + \sum_{t=3}^{\lfloor (m-3)/2 \rfloor} (2^{t+2})(2^{m-2t-3}) \end{aligned}$$

$$= 2 \cdot 2^{m-1} + 2^{m-2} + 2^{m-3} + 2^{\lfloor (m+2)/2 \rfloor} + 2^{m-1} \sum_{t=3}^{\lfloor (m-3)/2 \rfloor} 2^{-t}$$

$$= 2 \cdot 2^{m-1} + 2^{m-2} + 2^{m-3} + 2^{\lfloor (m+2)/2 \rfloor} + 2^{m-1}(2^{-2} - 2^{-\lfloor (m-3)/2 \rfloor})$$

$$= 2 \cdot 2^{m-1} + 2^{m-2} + 2^{m-3} + 2^{\lfloor (m+2)/2 \rfloor} + 2^{m-3} - 2^{m-1+\lceil (3-m)/2 \rceil}$$

$$= 2 \cdot 2^{m-1} + 2^{m-2} + 2^{m-2} + 2^{\lfloor (m+2)/2 \rfloor} - 2^{\lceil (m+1)/2 \rceil}$$

$$= 2 \cdot 2^{m-1} + 2^{m-1} + 2^{\lfloor (m+2)/2 \rfloor} - 2^{\lfloor (m+2)/2 \rfloor}$$

$$= 3 \cdot 2^{m-1}. \ \blacksquare$$

**4. Determining the distribution of arbitrary maximal period sequences.** Since the distribution of both the Fibonacci numbers and Lucas numbers modulo $2^m$ has been determined, the following theorem will show that the distribution of any maximal period sequence can be obtained from Theorems 1 and 2.

THEOREM 3. *Let* $x_n = x_{n-1} + x_{n-2} \pmod{2^m}$ *where* $X_1 = \{x_1, x_2\}$ *with either* $x_1$ *or* $x_2$ *odd. Suppose* $m \geq 3$. *Then* $X_1$ *is equivalent to* $\{k, k\}$ *or* $\{k, 3k\}$ *for some odd integer* $k$.

Proof. Let

$$A = \{\{k, k\} \mid k \text{ is odd and } 1 \leq k < 2^{m-1}\} \text{ and}$$
$$B = \{\{k, 3k\} \mid k \text{ is odd and } 1 \leq k < 2^{m-1}\}.$$

The claim is that $A \cup B$ generate a complete list of equivalence classes of sequences. Recall that there are $2^{m-1}$ equivalence classes of maximal period sequences and note that $|A| + |B| = 2^{m-1}$. It suffices to show that two elements in $A \cup B$ are inequivalent. This will be done by showing that each sequence has a different frequency distribution function. Clearly no element of $A$ can be equivalent to an element of $B$, since a sequence produced by an element of $A$ will have two occurrences of zero within a period, and a sequence produced by an element of $B$ will never have an occurrence of zero.

Now let $\{x_n\}$ be a sequence with $X_1 = \{k, k\} \in A$. Then $Z_{2^m}(0) = 2$ and so there are only 2 numbers which are consecutively repeated within the sequence. Those are $k$ and $k + 2^{m-1}$. Hence no two elements of $A$ can be equivalent.

Now assume $X_1 = \{k, 3k\} \in B$ and $Y_1 = \{k', 3k'\} \in B$ are equivalent. The result can be verified by listing the equivalence classes in the cases of $3 \leq m \leq 5$. Suppose $m$ is odd and $m \geq 7$. Let $a \equiv k(2 + 5 \cdot 2^{m-3}) \pmod{2^m}$ and $a' \equiv k'(2 + 5 \cdot 2^{m-3}) \pmod{2^m}$. For the sequence produced by $X_1$, $Z_{2^m}(a) = 2^{\lfloor m/2 \rfloor + 1}$ by the distribution theorem. Similarly for the

sequence produced by $Y_1$, $Z_{2^m}(a') = 2^{\lfloor m/2 \rfloor + 1}$. Since these are equivalent sequences and no other residue has a frequency distribution of $2^{\lfloor m/2 \rfloor + 1}$,

$$k(2 + 5 \cdot 2^{m-3}) \equiv k'(2 + 5 \cdot 2^{m-3}) \pmod{2^m}.$$

Therefore $k \equiv k' \pmod{2^{m-1}}$ and so $k = k'$. Now assume $m$ is even and $m \geq 6$. For the sequence produced by $X_1$, $Z_{2^m}(a) = 2^{\lfloor m/2 \rfloor}$ if $a \equiv 2k \pmod{2^m}$ or $a \equiv k(2+2^{m-2}) \pmod{2^m}$. Since $m$ is even, these are the only two residues where the values of $a$ are determined modulo $2^m$. Every other case has smaller moduli, which give more values for $a$ where the frequency distribution function is non-zero. The analogous statements are obtained for $Y_1$. Since the frequency distribution functions must be identical, one of two cases must occur. In the first case,

$$2k \equiv 2k' \pmod{2^m} \quad \text{and} \quad k(2 + 2^{m-2}) \equiv k'(2 + 2^{m-2}) \pmod{2^m}.$$

In this case, $k \equiv k' \pmod{2^{m-1}}$ and so $k = k'$. In the second case,

$$2k \equiv k'(2 + 2^{m-2}) \pmod{2^m} \quad \text{and} \quad 2k' \equiv k(2 + 2^{m-2}) \pmod{2^m}.$$

This implies

$$\begin{aligned} 2k &\equiv 2k'(1 + 2^{m-3}) \pmod{2^m} \equiv k(2 + 2^{m-2})(1 + 2^{m-3}) \pmod{2^m} \\ &\equiv k(2 + 2^{m-2} + 2^{m-2} + 2^{2m-5}) \pmod{2^m} \equiv k(2 + 2^{m-1}) \pmod{2^m}, \end{aligned}$$

which leads to the contradiction that $2 \equiv 2 + 2^{m-1} \pmod{2^m}$. Hence, no two elements of $B$ can generate equivalent sequences. Therefore $A \cup B$ is a complete list of equivalence classes. ∎

The proof gives a list of equivalence classes for the maximal period sequences. In addition, it implies that two sequences are equivalent if and only if they have the same frequency distribution functions. To summarize the key points of Theorems 1, 2 and 3, Theorem 4 follows easily from the previous results and by a direct computation.

THEOREM 4. *Let $x_n = x_{n-1} + x_{n-2} \pmod{2^m}$ with either $x_1$ or $x_2$ odd. Suppose $m \geq 3$. Then the sequence is equivalent to either an odd multiple of the Fibonacci numbers or an odd multiple of the Lucas numbers. For any sequence which is an odd multiple of the Fibonacci numbers the sequence is stable modulo 2. In addition, for $m \geq 5$, exactly $21/32$ of the residues have a non-zero frequency distribution. For any sequence which is an odd multiple of the Lucas numbers, the sequence is not stable modulo 2, and asymptotically $61/96$ of the residues have a non-zero frequency distribution.*

**Acknowledgments.** This work was done as part of an internship at the Center for Computing Sciences in Bowie, Maryland. I would like to thank M. L. Robinson for bringing this problem to my attention.

**References**

[1] R. P. Brent, *On the periods of generalized Fibonacci recurrences*, Math. Comp. 63 (1994), 207.

[2] W. Carlip and E. Jacobson, *A criterion for stability of two-term recurrence sequences modulo* $2^k$, Finite Fields Appl. 2 (1996), 369–406.

[3] —, —, *Unbounded stability of two-term recurrence sequences modulo* $2^k$, Acta Arith. 74 (1996), 329–346.

[4] E. Jacobson, *Distribution of the Fibonacci numbers mod* $2^k$, Fibonacci Quart. 30 (1992), 211–215.

[5] L. Kuipers and J. Shiue, *A distribution property of the sequence of Fibonacci numbers*, ibid. 10 (1972), 375–376.

[6] H. Niederreiter, *Distribution of Fibonacci numbers mod* $5^k$, ibid. 10 (1972), 373–374.

Department of Mathematics
University of Maryland
College Park, Maryland 20742
U.S.A.
E-mail: mdm@math.umd.edu

*Received on 5.5.1997* (3177)