ON THE STABILITY OF CERTAIN LUCAS SEQUENCES MODULO 2^k

Walter Carlip and Eliot Jacobson
Ohio University, Athens, OH 45701

(Submitted February 1995)

1. INTRODUCTION

Let $\{u_i | i \in \mathbf{N}\}$ be the two-term recurrence sequence defined by $u_0 = 0$, $u_1 = 1$, and $u_i = au_{i-1} + bu_{i-2}$ for all $i \geq 2$, where a and b are fixed integers. Let m be an integer and consider the corresponding sequence $\{\overline{u}_i\}$, where $\overline{u}_i \in \mathbf{Z}/m\mathbf{Z}$ is obtained via the natural projection $\mathbf{Z} \to \mathbf{Z}/m\mathbf{Z}$.

It is well known that $\{\overline{u}_i\}$ is eventually periodic and, if b is relatively prime to m, such a sequence is purely periodic (see, e.g., [3] or [10]). We will designate by $\lambda(m) = \lambda_{a,b}(m)$ the length of the (shortest) period of $\{\overline{u}_i\}$, and for each $r \in \mathbf{Z}$, we define $\nu(m, r) = \nu_{a,b}(m, r)$ to be the number of occurrences of the residue r (mod m) in one such period. We also define $\Omega(m) = \Omega_{a,b}(m) = \{\nu_{a,b}(m, r) | r \in \mathbf{Z}\}$.

The sequence $\{u_i\}$ is said to be *uniformly distributed* modulo m if each residue modulo m appears an equal number of times in each period, that is, if $|\Omega(m)| = 1$. The sequence $\{u_i\}$ is said to be *stable* modulo the prime p if there is a positive integer N such that $\Omega(p^k) = \Omega(p^N)$ for all $k \geq N$. If N is the least such integer, we say that stability *begins* at N.

Interest in the stability of two-term recurrence sequences developed from the investigation of the uniform distribution of the Fibonacci sequence. A flurry of papers in the early 1970s culminated in the complete characterization of those integers modulo which a two-term recurrence sequence is uniformly distributed. A thorough exposition can be found in [5].

The subject lay dormant until the ground-breaking work of Schinzel [7], who classified the sets $\Omega_{a,1}(p)$ for odd primes p. Pihko extended Schinzel's work to cover some additional two-term recurrence sequences in [6], and Somer explored and extended Schinzel's work in [8] and [9]. In 1992, Jacobson [4] investigated the distribution of the Fibonacci sequence modulo powers of 2 and discovered that the Fibonacci sequence is stable modulo 2. He used this stability to compute $\nu_{1,1}(2^k, r)$, for all $k \in \mathbf{N}$ and $r \in \mathbf{Z}$.

In the present work we explicitly compute $\nu_{a,b}(2^k, r)$ for all $k \geq 5$ and all integers r, whenever a is odd and $b \equiv 1 \pmod{16}$. We will show that $\{u_i\}$ is stable in this case, and that Jacobson's result for the Fibonacci sequence is archetypal for this situation.

Theorem 1.1: Assume that a is odd and $b \equiv 1 \pmod{16}$. Then, for all $k \geq 5$,

$$\nu(2^k, r) = \begin{cases} 1 & \text{if } r \equiv 3 \pmod{4}, \\ 2 & \text{if } r \equiv 0 \pmod{8}, \\ 3 & \text{if } r \equiv 1 \pmod{4}, \\ 8 & \text{if } r \equiv a^2 + b \pmod{32}, \text{ and} \\ 0 & \text{otherwise.} \end{cases}$$

Corollary 1.2: Assume that a is odd and $b \equiv 1 \pmod{16}$. Then $\{u_i\}$ is stable modulo 2, with stability beginning at $N = 5$, and $\Omega_{a,b}(2^k) = \{0, 1, 2, 3, 8\}$ for all $k \geq 5$.

The reader may wonder if stability also occurs for other choices of the parameters a and b. In fact it does, though the proofs are considerably more delicate. Table 1 gives the value of N at which stability begins for a given pair (a, b). In [2] we proved that $\{u_i\}$ is stable when $b \equiv 5 \pmod{8}$, and in [1] we dealt with the case $b \equiv 3 \pmod{4}$, in which stability apparently occurs less frequently.

TABLE 1. Smallest k for which $\Omega_{a,b}(2^k) = \Omega_{a,b}(2^{k+t})$ for all $t \geq 0$

		a																		
		1	3	5	7	9	11	13	15	17	19	21	23	25	27	29	31	33	35	37
b	1	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5
	3			4	4	4	4					4	4	4	4					4
	5	5	4	4	7	6	4	4	5	5	4	4	6	8	4	4	5	5	4	4
	7	5	4	5	4	6	7	4	6		4	6		5	5	4	4	5	4	5
	9																			
	11		4		4	4		4			4		4	4		4			4	
	13	4	5	7	4	4	6	5	4	4	5	6	4	4	9	5	4	4	5	8
	15	6	3	3	6	5	3	3	5	8	3	3	5	7	3	3	8	7	3	3
	17	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5
	19			4	4	4	4					4	4	4	4					4
	21	7	4	4	5	5	4	4	6	6	4	4	5	5	4	4	11	8	4	4
	23	5	5	4		5	4	6		6	7	4	4	6	4	5	4	5	5	4
	25																			
	27		4		4	4		4			4		4	4		4			4	
	29	4	6	5	4	4	5	9	4	4	7	5	4	4	5	6	4	4	6	5
	31	7	3	3	4	4	3	3	8	6	3	3	4	4	3	3	2		3	3

A missing entry in Table 1 corresponds to a case that we have not yet resolved (but conjecture to be unstable). In particular, as of this writing, the stability of $\{u_i\}$ when $b \equiv 9 \pmod{16}$ is undetermined.

2. PRELIMINARY LEMMAS

In this section we present a few lemmas required for the proof of Theorem 1.1. Throughout this section, assume that a is odd and that $b \equiv 1 \pmod{16}$. As usual, $\{u_i\}$ will denote a two-term recurrence sequence defined by $u_0 = 0$, $u_1 = 1$, and $u_i = au_{i-1} + bu_{i-2}$ for all $i \geq 2$.

The following lemma summarizes some well-known facts about two-term recurrences. The routine induction proofs of each part are left to the reader.

Lemma 2.1: For all $m \geq 1$ and $n \geq 0$,

(a) $u_{m+n} = bu_{m-1}u_n + u_m u_{n+1}$,

(b) $u_{2n+1} = b(u_n)^2 + (u_{n+1})^2$,

(c) $u_{2n} = 2u_n u_{n+1} - a(u_n)^2$, and

(d) u_n divides u_{nm}.

Although the next lemma is stated only for $b \equiv 1 \pmod{16}$, analogs exist for all odd b. The interested reader is invited to discover these congruences.

Lemma 2.2: For all $k \geq 5$,

$$\textit{(a)}\quad u_{3\cdot 2^{k-3}} \equiv \begin{cases} 2^{k-1} \pmod{2^{k+1}} & \text{if } a \equiv 1 \pmod 8 \text{ or } a \equiv 3 \pmod 8, \\ 3\cdot 2^{k-1} \pmod{2^{k+1}} & \text{if } a \equiv 5 \pmod 8 \text{ or } a \equiv 7 \pmod 8, \end{cases}$$

and

$$\textit{(b)}\quad u_{3\cdot 2^{k-3}+1} \equiv \begin{cases} 1+2^{k-2} \pmod{2^{k}} & \text{if } a \equiv 1 \pmod 8 \text{ or } a \equiv 7 \pmod 8, \\ 1+3\cdot 2^{k-2} \pmod{2^{k}} & \text{if } a \equiv 3 \pmod 8 \text{ or } a \equiv 5 \pmod 8. \end{cases}$$

Proof: We will prove the results for $a \equiv 1 \pmod 8$ and leave the analogous proofs when $a \equiv 3, 5$, or $7 \pmod 8$ to the reader. To this end, assume that $a \equiv 1 \pmod 8$. We prove (a) and (b) simultaneously by induction on k. The base step, when $k = 5$, can be checked by explicit computation. Since there are only a finite number of two-term recurrence sequences modulo 2^5 and 2^6, this computation is finite, and we leave it to the reader to verify the result.

Now assume that (a) and (b) are true for some $k \geq 5$. Since $k \geq 5$, it follows that $2k-4 \geq k+1$ and $2k-2 \geq k+1$. Therefore, by Lemma 2.1 and the induction hypothesis,

$$\begin{aligned} u_{3\cdot 2^{k-2}+1} = u_{2(3\cdot 2^{k-3})+1} &= b(u_{3\cdot 2^{k-3}})^2 + (u_{3\cdot 2^{k-3}+1})^2 \\ &\equiv b(2^{k-1})^2 + (1+2^{k-2})^2 \pmod{2^{k+1}} \\ &\equiv b\cdot 2^{2k-2} + 1 + 2^{k-1} + 2^{2k-4} \pmod{2^{k+1}} \\ &\equiv 1+2^{k-1} \pmod{2^{k+1}}, \end{aligned}$$

as desired.

Now write $u_{3\cdot 2^{k-3}+1} = 1+2^{k-2}+2^k v$ for some integer v. Since $k \geq 4$, it follows that $2k-2 \geq k+2$ and, therefore, by Lemma 2.1 and the induction hypothesis,

$$\begin{aligned} u_{3\cdot 2^{k-2}} = u_{2(3\cdot 2^{k-3})} &= 2(u_{3\cdot 2^{k-3}} u_{3\cdot 2^{k-3}+1}) - a(u_{3\cdot 2^{k-3}})^2 \\ &\equiv (2\cdot 2^{k-1})\cdot(1+2^{k-2}+2^k v) - a(2^{k-1})^2 \pmod{2^{k+2}} \\ &\equiv 2^k(1+2^{k-2}) \pmod{2^{k+2}} \\ &\equiv 2^k \pmod{2^{k+2}}, \end{aligned}$$

as desired. This completes the induction and, hence, the proof of the lemma for $a \equiv 1 \pmod 8$. □

Clearly the residue classes of u_n modulo 2, 4, and 8 depend only upon the residue classes of a and b. These classes will be required below. They may be computed directly, and we list them here for convenience.

Reduction of $\{u_i\}$ modulo 2 yields

$$0, 1, 1, 0, 1, \ldots \text{ for all odd } a \text{ and } b. \tag{2.1}$$

Since $b \equiv 1 \pmod 4$, reduction of $\{u_i\}$ modulo 4 yields

$$\begin{aligned} &0, 1, 1, 2, 3, 1, 0, 1, \ldots \quad \text{if } a \equiv 1 \pmod 4, \\ &0, 1, 3, 2, 1, 1, 0, 1, \ldots \quad \text{if } a \equiv 3 \pmod 4. \end{aligned} \tag{2.2}$$

Finally, since $b \equiv 1 \pmod 8$, reduction of $\{u_i\}$ modulo 8 yields

$$\begin{array}{ll} 0, 1, 1, 2, 3, 5, 0, 5, 5, 2, 7, 1, 0, 1, \ldots & \text{if } a \equiv 1 \pmod 8, \\ 0, 1, 3, 2, 1, 5, 0, 5, 7, 2, 5, 1, 0, 1, \ldots & \text{if } a \equiv 3 \pmod 8, \\ 0, 1, 5, 2, 7, 5, 0, 5, 1, 2, 3, 1, 0, 1, \ldots & \text{if } a \equiv 5 \pmod 8, \\ 0, 1, 7, 2, 5, 5, 0, 5, 3, 2, 1, 1, 0, 1, \ldots & \text{if } a \equiv 7 \pmod 8. \end{array} \tag{2.3}$$

In the next lemma we examine the periods of two-term recurrence sequences defined by our parameters a and b.

Lemma 2.3: If $b \equiv 1 \pmod{16}$ and a is odd, then $\lambda(2^k) = 3 \cdot 2^{k-1}$ for all $k \geq 5$.

Proof: Fix an integer k such that $k \geq 5$. By Lemma 2.2, $u_{3 \cdot 2^{k-1}} \equiv 0 \pmod{2^k}$ and $u_{3 \cdot 2^{k-1}+1} \equiv 1 \pmod{2^k}$. Hence, $\lambda(2^k)$ divides $3 \cdot 2^{k-1}$. But, by Lemma 2.2, $u_{3 \cdot 2^{k-2}+1} \equiv 1 + 2^{k-1} \pmod{2^k}$ (in all cases) so that $\lambda(2^k)$ does not divide $3 \cdot 2^{k-2}$. Since, by (2.2), $u_{2^{k-1}} \not\equiv 0 \pmod 4$, it follows that $u_{2^{k-1}} \not\equiv 0 \pmod{2^k}$ and, hence, $\lambda(2^k)$ does not divide 2^{k-1}. It now follows that $\lambda(2^k) = 3 \cdot 2^{k-1}$. □

We now derive four lemmas that are key to the proof of Theorem 1.1.

Lemma 2.4: Assume that $k \geq 5$. If $n \geq 0$ and $n \not\equiv 0 \pmod 3$, then $u_{n+3 \cdot 2^{k-2}} \equiv u_n + 2^{k-1} \pmod{2^k}$.

Proof: Note that by (2.1) u_n is even if and only if $3|n$; hence, the hypothesis that $n \not\equiv 0$ (mod 3) implies that u_n is odd. Therefore, by Lemmas 2.1 and 2.2,

$$\begin{aligned} u_{n+3 \cdot 2^{k-2}} &= b u_{n-1} u_{3 \cdot 2^{k-2}} + u_n u_{3 \cdot 2^{k-2}+1} \\ &\equiv b u_{n-2} \cdot 0 + u_n u_{3 \cdot 2^{k-2}+1} \pmod{2^k} \\ &\equiv u_n (1 + 2^{k-1}) \pmod{2^k} \\ &\equiv u_n + 2^{k-1} \pmod{2^k}, \end{aligned}$$

as desired. □

Lemma 2.5: Assume that $k \geq 5$. If $n \geq 0$ and $n \equiv 0 \pmod 6$, then $u_{n+3 \cdot 2^{k-3}} \equiv u_n + 2^{k-1} \pmod{2^k}$.

Proof: By Lemma 2.2 we can write $u_{3 \cdot 2^{k-3}+1} \equiv 1 + \ell \cdot 2^{k-2} \pmod{2^k}$ for some odd integer ℓ. Then

$$\begin{aligned} u_{n+3 \cdot 2^{k-3}} &= b u_{n-1} u_{3 \cdot 2^{k-3}} + u_n u_{3 \cdot 2^{k-3}+1} \\ &\equiv b u_{n-1} \cdot 2^{k-1} + u_n (1 + \ell \cdot 2^{k-2}) \pmod{2^k}. \end{aligned}$$

Since both b and u_{n-1} are odd, $b u_{n-1} \cdot 2^{k-1} \equiv 2^{k-1} \pmod{2^k}$. Moreover, by (2.2), $u_6 \equiv 0$ (mod 4) and, by Lemma 2.2, u_6 divides u_n, so $u_n \equiv 0 \pmod 4$. Consequently, $u_n(1 + \ell \cdot 2^{k-2}) \equiv u_n$ (mod 2^k). Thus, $u_{n+3 \cdot 2^{k-3}} \equiv u_n + 2^{k-1} \pmod{2^k}$, as desired. □

We also need a lemma similar to Lemmas 2.4 and 2.5 to cover the case in which $n \equiv 3$ (mod 6). This will require a little more work.

Lemma 2.6: Assume that $k \geq 6$. If $n \geq 0$ and $n \equiv 3 \pmod 6$, then $u_{n+3 \cdot 2^{k-4}} \equiv u_n + 2^{k-1} \pmod{2^k}$.

Proof: Note that, by (2.3), $u_n \equiv 2 \pmod 8$ whenever $n \equiv 3 \pmod 6$. By Lemma 2.2 and the hypothesis that $k \geq 6$, we can find integers ℓ and m such that

$$u_{3\cdot 2^{k-4}+1} = 1 + \ell \cdot 2^{k-3} + m \cdot 2^{k-1},$$

where ℓ is determined by the class of a modulo 8. Also, by Lemma 2.2, there is an odd integer v such that

$$u_{3\cdot 2^{k-4}} \equiv v \cdot 2^{k-2} \pmod{2^k},$$

where v is also determined by the class of a modulo 8. Moreover, note that (2.2) implies that $u_{n-1} \equiv a \pmod 4$ and recall that $b \equiv 1 \pmod{16}$. Combining these congruences, we obtain

$$\begin{aligned} u_{n+3\cdot 2^{k-4}} &= u_{3\cdot 2^{k-4}+1}u_n + bu_{3\cdot 2^{k-4}}u_{n-1} \\ &\equiv (1+\ell \cdot 2^{k-3} + m \cdot 2^{k-1})u_n + b \cdot v \cdot 2^{k-2}u_{n-1} \pmod{2^k} \\ &\equiv u_n + \ell \cdot 2^{k-2} + av2^{k-2} \pmod{2^k} \\ &\equiv u_n + (\ell + av)2^{k-2} \pmod{2^k}. \end{aligned}$$

We now compute:

$a \pmod 8$	ℓ	v	$\ell + av \pmod 4$
1	1	1	$2 \equiv 2 \pmod 4$
3	3	1	$6 \equiv 2 \pmod 4$
5	3	3	$18 \equiv 2 \pmod 4$
7	1	3	$22 \equiv 2 \pmod 4$

In each case $\ell + av \equiv 2 \pmod 4$; therefore, $u_{n+3\cdot 2^{k-4}} \equiv u_n + 2^{k-1} \pmod{2^k}$, as desired. □

Finally, we require an easy generalization of Lemma 2.6.

Lemma 2.7: Assume that $n \geq 0$ and $s \geq 0$. If $n \equiv 3 \pmod 6$ and $k \geq 6$, then $u_{n+3s\cdot 2^{k-4}} \equiv u_n + s \cdot 2^{k-1} \pmod{2^k}$.

Proof: Proceed by induction on s. If $s = 0$, the result is trivial. Fix $s \geq 0$ and assume the lemma is true for this value of s. Then

$$u_{n+3\cdot 2^{k-4}(s+1)} = u_{n+3\cdot 2^{k-4}+3s2^{k-4}}.$$

Observe that $n + 3 \cdot 2^{k-4} \equiv n \equiv 3 \pmod 6$, so by Lemma 2.6 and the induction hypothesis,

$$\begin{aligned} u_{n+3\cdot 2^{k-4}(s+1)} &\equiv u_{n+3\cdot 2^{k-4}} + s \cdot 2^{k-1} \pmod{2^k} \\ &\equiv u_n + 2^{k-1} + s \cdot 2^{k-1} \pmod{2^k} \\ &\equiv u_n + 2^{k-1}(s+1) \pmod{2^k}, \end{aligned}$$

as desired. □

3. PROOF OF THE MAIN THEOREM

In this section we prove Theorem 1.1.

Proof of Theorem 1.1

First, note that, by Lemma 2.3, $\lambda(2^k) = 3\cdot 2^{k-1}$. In particular, $\lambda(2^{k+1}) = 2\cdot\lambda(2^k)$.

Now, proceed by induction on k. For $k=5$ and $k=6$, there are only a finite number of sequences to examine (corresponding to $b \in \{1, 17, 33, 49\}$ and $a \in \{1, 3, 5, 7, \ldots, 61, 63\}$). Direct computation (perhaps with the assistance of a computer) establishes the theorem in these cases.

Assume that $k \geq 6$ and that Theorem 1.1 is true for this k.

Step 1. If $r \equiv 3$ (mod 4), then $v(2^{k+1}, r) \geq 1$.

Proof: By the induction hypothesis, $v(2^{k+1}, r) = 1$, so there exists an integer n with $u_n \equiv r$ (mod 2^k). Since r is odd, (2.1) implies that $n \not\equiv 0$ (mod 3). Now, either $u_n \equiv r \pmod{2^{k+1}}$ or $u_n \equiv r + 2^k$ (mod 2^{k+1}). In the latter case, Lemma 2.4 implies that $u_{n+3\cdot 2^{k-1}} \equiv u_n + 2^k \equiv r$ (mod 2^{k+1}). Thus, $v(2^{k+1}, r) \geq 1$, as desired. □

Step 2. If $r \equiv 1$ (mod 4), then $v(2^{k+1}, r) \geq 3$.

Proof: By the induction hypothesis, $v(2^k, r) = 3$. Pick indices $0 < n_1 < n_2 < n_3 < 3\cdot 2^{k-1}$ such that $u_{n_1} \equiv u_{n_2} \equiv u_{n_3} \equiv r \pmod{2^k}$.

By Lemma 2.4, $u_{n_i+3\cdot 2^{k-1}} \equiv u_{n_i} + 2^k \pmod{2^{k+1}}$. Also, for each i, either $u_{n_i} \equiv r \pmod{2^{k+1}}$ or $u_{n_i} \equiv r + 2^k \pmod{2^{k+1}}$. Hence, for each i,

$$u_{n_i} \equiv r \pmod{2^{k+1}} \quad \text{or} \quad u_{n_i+3\cdot 2^{k-1}} \equiv r \pmod{2^{k+1}}.$$

For each i, let $m_i \in \{n_i, n_i + 3\cdot 2^{k-1}\}$ be the index that satisfies $u_{m_i} \equiv r$ (mod 2^{k+1}). Then the indices m_1, m_2, and m_3 are congruent modulo $3\cdot 2^{k-1}$ to n_1, n_2, and n_3, respectively. Furthermore, by Lemma 2.3, $\lambda(2^{k+1}) = 3\cdot 2^k$. Thus, the indices m_1, m_2, and m_3 are distinct and satisfy $0 < m_i < \lambda(2^{k+1})$. It follows that $v(2^{k+1}, r) \geq 3$, as desired. □

Step 3. If $r \equiv 0$ (mod 8), then $v(2^{k+1}, r) \geq 2$.

Proof: By the induction hypothesis $v(2^k, r) = 2$. Hence, we can find integers n_1 and n_2 such that $0 < n_1 < n_2 < 3\cdot 2^{k-1}$ and $u_{n_1} \equiv u_{n_2} \equiv r \pmod{2^k}$. Now $u_{n_i} \equiv 0$ (mod 4), so (2.2) implies that $n_1 \equiv n_2 \equiv 0$ (mod 6). By Lemma 2.5, $u_{n_1+3\cdot 2^{k-2}} \equiv u_{n_1} \pmod{2^k}$. It follows that $n_2 = n_1 + 3\cdot 2^{k-2}$.

Now, either $u_{n_1} \equiv r \pmod{2^{k+1}}$ or $u_{n_1} \equiv r + 2^k \pmod{2^{k+1}}$. If $u_{n_1} \equiv r \pmod{2^{k+1}}$, then, by Lemma 2.5, $u_{n_1} \equiv u_{n_1+3\cdot 2^{k-1}} \equiv r$ (mod 2^{k+1}) and, hence, $v(2^{k+1}, r) \geq 2$. On the other hand, if $u_{n_1} \equiv r + 2^k \pmod{2^{k+1}}$, then, by Lemma 2.5, $u_{n_2} = u_{n_1+3\cdot 2^{k-2}} \equiv u_{n_1} + 2^k \equiv r$ (mod 2^{k+1}). Therefore, $u_{n_2} \equiv u_{n_2+3\cdot 2^{k-1}} \equiv r$ (mod 2^{k+1}). Thus, $v(2^{k+1}, r) \geq 2$ in this case as well. □

Step 4. If $r \equiv a^2 + b$ (mod 32), then $v(2^{k+1}, r) \geq 8$.

Proof: By the induction hypothesis, $v(2^k, r) = 8$. Choose n such that $u_n \equiv r \pmod{2^k}$. By hypothesis, $b \equiv 1$ (mod 16), and a is odd. Therefore, $a^2 \equiv 1$ (mod 8) and $r \equiv a^2 + b \equiv 2$ (mod 8). It follows from (2.3) that $n \equiv 3$ (mod 6). Hence, Lemma 2.7 yields

$$u_{n+3s\cdot 2^{k-4}} \equiv \begin{cases} u_n \pmod{2^k} & \text{if } s \text{ is even,} \\ u_n + 2^k \pmod{2^k} & \text{if } s \text{ is odd.} \end{cases}$$

By Lemma 2.3, $\lambda(2^k) = 3\cdot 2^{k-1}$. It follows that

$$u_{n+3s\cdot 2^{k-4}} \equiv \begin{cases} r \pmod{2^k} & \text{if } s \in \{0, 2, 4, 6\}, \\ r + 2^{k-1} \pmod{2^k} & \text{if } s \in \{1, 3, 5, 7\}, \end{cases}$$

with all indices $n + 3s\cdot 2^{k-4}$ occurring within one period.

Since, by the induction hypothesis, $v(2^k, r) = 8$, we can now conclude that there are indices n_1 and n_2 such that $0 < n_1 < n_2 < 3\cdot 2^{k-1}$ with $n_2 - n_1 < 3\cdot 2^{k-4}$ and $u_{n_1} \equiv u_{n_2} \equiv r \pmod{2^k}$. As usual, for $i = \{1, 2\}$, either $u_{n_i} \equiv r \pmod{2^{k+1}}$ or $u_{n_i} \equiv r + 2^k \pmod{2^{k+1}}$, and in the second case, Lemma 2.6 implies that $u_{n_i + 3\cdot 2^{k-3}} \equiv r \pmod{2^{k+1}}$. Hence, there are subscripts m_1 and m_2 such that $u_{m_1} \equiv u_{m_2} \equiv r \pmod{2^{k+1}}$ and $m_i \equiv n_i \pmod{3\cdot 2^{k-3}}$.

Consider the set $\Gamma = \{m_i + 3s\cdot 2^{k-2} \mid 0 \le s \le 3 \text{ and } 1 \le i \le 2\}$. By Lemma 2.7, $u_m \equiv r \pmod{2^{k+1}}$ for $m \in \Gamma$. Since $\lambda(2^{k+1}) = 3\cdot 2^k$, it suffices to show that the elements of Γ are incongruent modulo $3\cdot 2^k$.

If $m_i + 3s\cdot 2^{k-2} \equiv m_i + 3t\cdot 2^{k-2} \pmod{3\cdot 2^k}$ (for some s and t such that $0 \le s, t \le 3$), then $3(s-t)\cdot 2^{k-2} \equiv 0 \pmod{3\cdot 2^k}$ and, therefore, $s \equiv t$(mod 4). Thus $s = t$.

Moreover, if $m_1 + 3s\cdot 2^{k-2} \equiv m_2 + 3t\cdot 2^{k-2} \pmod{3\cdot 2^k}$, then $m_i \equiv m_2 \pmod{3\cdot 2^{k-2}}$and, hence, $n_1 \equiv m_1 \equiv m_2 \equiv n_2 \pmod{3\cdot 2^{k-3}}$, which contradicts the choice of n_1 and n_2 to satisfy $n_2 - n_1 < 3\cdot 2^{k-4}$ and $n_1 \ne n_2$.

It follows that the eight elements of Γ are distinct modulo $\lambda(2^{k+1})$ and, consequently, $v(2^{k+1}, r) \ge 8$. □

Step 5. Conclusion

Proof: We have established that $v(2^{k+1}, r) \ge v(2^k, r)$ in each case of Lemma 1.1 for which $v(2^k, r) > 0$. Now observe:

$$\begin{aligned} \lambda(2^{k+1}) &= 3\cdot 2^k \\ &= \sum_{r=0}^{2^{k+1}-1} v(2^{k+1}, r) \\ &\ge \sum_{r\equiv 3 \,(\text{mod } 4)} v(2^{k+1}, r) + \sum_{r\equiv 1 \,(\text{mod } 4)} v(2^{k+1}, r) + \sum_{r\equiv 0 \,(\text{mod } 8)} v(2^{k+1}, r) + \sum_{r\equiv a^2+b \,(\text{mod } 32)} v(2^{k+1}, r) \\ &\ge \frac{1}{4}\cdot 2^{k+1}\cdot 1 + \frac{1}{4}\cdot 2^{k+1}\cdot 3 + \frac{1}{8}\cdot 2^{k+1}\cdot 2 + \frac{1}{32}\cdot 2^{k+1}\cdot 8 \\ &= 2^{k-1} + 3\cdot 2^{k-1} + 2^{k-1} + 2^{k-1} = 3\cdot 2^k = \lambda(2^{k+1}). \end{aligned}$$

It follows that all of the inequalities obtained in Steps 1-4 above are equalities. This shows that $v(2^{k+1}, r) = v(2^k, r)$ for all $r \in \mathbf{Z}$, and completes the induction and the proof of Theorem 1.1. □

Remark 3.1: As mentioned above, the techniques described in this paper may be extended to show stability of two-term recurrence sequences determined by other values of the parameters a and b. Originally, this work contained delicate arguments to handle a number of other such cases. Because subsequently developed methods have shown that only the case that $b \equiv 1 \pmod{16}$ needs to be singled out in this way, we leave the extension of this "direct approach" to the reader. We would like to thank the referee for suggesting this lighter approach to the presentation.

REFERENCES

1. W. Carlip & E. Jacobson. "A Criterion for Stability of Two-Term Recurrence Sequences Modulo 2^k." *J. Finite Fields* (submitted).
2. W. Carlip & E. Jacobson. "Unbounded Stability of Two-Term Recurrence Sequences Modulo 2^k." *Acta. Arith.* (to appear).
3. R. D. Carmichael. "On Sequences of Integers Defined by Recurrence Relations." *Quart. J. Pure and Appl. Math.* **48** (1920):343-72.
4. Eliot T. Jacobson. "Distribution of the Fibonacci Numbers Mod 2^k." *The Fibonacci Quarterly* **30.3** (1992):211-15.
5. Wladyslaw Narkiewicz. *Uniform Distribution of Sequences of Integers in Residue Classes.* Lecture Notes in Mathematics, Vol. 1087. New York: Springer-Verlag, 1984.
6. Jukka Pihko. "A Note on a Theorem of Schinzel." *The Fibonacci Quarterly* **29.4** (1991): 333-38.
7. A. Schinzel. "Special Lucas Sequences, Including the Fibonacci Sequence, Modulo a Prime." In *A Tribute to Paul Erdös*, pp. 349-57. Ed. A. Baker, B. Bollobás, and A. Hajnal. Cambridge: Cambridge University Press, 1990.
8. Lawrence Somer. "Distribution of Residues of Certain Second-Order Linear Recurrences Modulo p." In *Applications of Fibonacci Numbers*, pp. 311-24. Ed. A. N. Phillipou, A. F. Horadam, and G. E. Bergum. Dordrecht: Kluwer, 1988.
9. Lawrence Somer. "Distribution of Residues of Certain Second-Order Linear Recurrences Modulo p—II." *The Fibonacci Quarterly* **29:1** (1991):72-78.
10. D. D. Wall. "Fibonacci Series Modulo m." *Amer. Math. Monthly* **67** (1960):525-32.

AMS Classification Numbers: 11B39, 11B50, 11B37

❖❖❖