ACTA ARITHMETICA
LXXIV.4 (1996)

Unbounded stability of two-term recurrence sequences modulo 2^k

by

Walter Carlip and Eliot Jacobson (Athens, Ohio)

1. Introduction. Let a and b be fixed integers and let $\{u_i \mid i \in \mathbb{N}\}$ 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 $i \geq 2$. For any positive integer m, consider the sequence $\{\overline{u}_i\}$ obtained by reduction modulo m. If m and b are relatively prime, then $\{\overline{u}_i\}$ is known to be purely periodic, and therefore it is natural to ask how often each residue occurs in one period of the sequence. This question is surprisingly difficult to answer without restrictions. Even the prerequisite problem of determining the length of the (shortest) period as a function of a, b and m is, in general, beyond reach. Consequently, most authors who consider this question either settle for rough bounds on the maximum or minimum number of occurrences of each residue in one period ([7, 8]) or else severely restrict the sequences and moduli studied ([6, 5]). In this context it is no surprise that the present paper restricts a and b to selected congruence classes of odd integers and m to powers of two. However, the tradeoff for this austerity is a complete characterization of the distribution frequencies of $\{u_i\}$ modulo m.

For a fixed two-term recurrence sequence, as defined above, and fixed modulus m and residue r, we denote the number of occurrences (i.e. the "frequency") of the residue r in one (shortest) period of $\{\overline{u}_i\}$ by $\nu_{a,b}(m, r)$ (or $\nu(m, r)$, when a and b are clear). The function $\nu(m, r)$ is called the *frequency distribution function* of $\{u_i\}$ modulo m.

In the early 1970s, interest in the distribution functions of two-term recurrence sequences centered on the characterization of those sequences that have constant frequency distribution functions, i.e., those sequences that are

1991 *Mathematics Subject Classification*: Primary 11B39, 11B50; Secondary 11B37, 11K36.

Key words and phrases: Lucas, Fibonacci, distribution, stability.

Portions of this paper were completed while the first author was visiting Binghamton University.

uniformly distributed. Thus, if we define $\Omega(m) = \Omega_{a,b}(m) = \{\nu_{a,b}(m,r) \mid r \in \mathbb{Z}\}$, then the sequence $\{u_i\}$ is *uniformly distributed modulo* m whenever $|\Omega(m)| = 1$. A detailed exposition of this topic can be found in [4].

In 1992, Jacobson [3] discovered that, though not uniformly distributed, the Fibonacci sequence is nonetheless well-behaved modulo powers of two. In particular, he proved that for all $k \geq 5$, $|\Omega_{1,1}(2^k)| = 5$ and gave an explicit description of $\nu_{1,1}(2^k, r)$. Though not constant, this distribution function exhibited a type of "stability" that generalized the concept of uniform distribution and led to the following definition.

DEFINITION 1.1. The sequence $\{u_i\}$ is *stable* modulo the prime p if there is a positive integer N such that $\Omega(p^k) = \Omega(p^N)$ for all $k \geq N$.

Informally, if N is the smallest integer with the property that $\Omega(p^k) = \Omega(p^N)$ for all $k \geq N$, then we say that stability *begins at generation* N.

In [1], we began a comprehensive study of the stability of two-term recurrence sequences modulo powers of two. In that paper, we identified several families of stable two-term recurrences. The sequences studied in [1] had some other remarkable properties. In addition to being stable, each shared with the Fibonacci sequence the property that $|\Omega_{a,b}(2^k)| \leq 5$ for all $k \geq 5$. Moreover, the actual frequencies that occurred were bounded: $\nu_{a,b}(2^k, r) \leq 8$ for each pair (a, b) studied in [1]. Finally, each of these sequences became stable at relatively early generations, in particular, for each pair (a, b) studied in [1], $\Omega_{a,b}(2^k) = \Omega_{a,b}(2^5)$ for all $k \geq 5$.

In this paper we extend the results of [1] by identifying several more families of stable sequences. The sequences studied here, however, do not become stable quite as readily as those in [1]—the generation at which their stability begins depends strongly on the exact values of a and b. (In fact, it is a function of the greatest power of two that divides either the third or the sixth term of the sequence.) In particular, each family contains sequences that have arbitrarily large frequencies and sequences whose stability begins after an arbitrarily large number of generations. Perhaps surprisingly, the number of frequencies that appear is still well-behaved: $|\Omega_{a,b}(2^k)| \leq 5$ for all $k \geq 4$.

To simplify the statements of our main theorems we introduce the following notation. Fix a prime p and integer m. We write $p^s \parallel m$ if p^s divides m but p^{s+1} does not divide m. We also use the p-adic valuation $\nu_p(m)$, defined by $\nu_p(m) = s$ if $p^s \parallel m$. (Do not confuse the notation $\nu_p(m)$ with the previously defined $\nu_{a,b}(m, r)$.)

We now state our main results. The following three theorems describe the frequency distribution functions of several families of two-term recurrences.

THEOREM 1.2. *Suppose that* $b \equiv 5 \pmod 8$ *and* a *is odd, and assume that* $2^t \parallel u_6$. *Then for all integers* k, *if* $4 \leq k \leq t$, *then*

$$\nu_{a,b}(2^k,r)=\begin{cases}1 & \text{if } r\equiv 3 \pmod 4,\\ 2 & \text{if } r\equiv 6 \pmod 8,\\ 3 & \text{if } r\equiv 1 \pmod 4,\\ 2^{k-2} & \text{if } r=0, \text{ and}\\ 0 & \text{otherwise};\end{cases} \tag{1.1}$$

and, if $k\ge t$,

$$\nu_{a,b}(2^k,r)=\begin{cases}1 & \text{if } r\equiv 3 \pmod 4,\\ 2 & \text{if } r\equiv 6 \pmod 8,\\ 3 & \text{if } r\equiv 1 \pmod 4,\\ 2^{t-2} & \text{if } r\equiv 0 \pmod{2^t}, \text{ and}\\ 0 & \text{otherwise.}\end{cases} \tag{1.2}$$

THEOREM 1.3. *Suppose that* $b\equiv 7 \pmod{16}$ *and* $a\equiv\pm 3 \pmod 8$, *and assume that* $2^t \parallel u_3$. *Then for all integers* k, *if* $4\le k\le t$, *then*

$$\nu_{a,b}(2^k,r)=\begin{cases}1 & \text{if } r\equiv 1 \pmod 2,\\ 2^{k-2} & \text{if } r=0, \text{ and}\\ 0 & \text{otherwise};\end{cases} \tag{1.3}$$

and if $k\ge t$,

$$\nu_{a,b}(2^k,r)=\begin{cases}1 & \text{if } r\equiv 1 \pmod 2,\\ 2^{t-2} & \text{if } r\equiv 0 \pmod{2^t}, \text{ and}\\ 0 & \text{otherwise.}\end{cases} \tag{1.4}$$

THEOREM 1.4. *Suppose that* $b\equiv 15 \pmod{16}$ *and* $a\equiv\pm 7 \pmod{16}$, *and assume that* $2^t \parallel u_3$. *Then for all integers* k, *if* $4\le k\le t$, *then*

$$\nu_{a,b}(2^k,r)=\begin{cases}1 & \text{if } r\equiv \pm 1 \pmod 8,\\ 2^{k-3} & \text{if } r=0, \text{ and}\\ 0 & \text{otherwise};\end{cases} \tag{1.5}$$

and if $k\ge t$,

$$\nu_{a,b}(2^k,r)=\begin{cases}1 & \text{if } r\equiv \pm 1 \pmod 8,\\ 2^{t-3} & \text{if } r\equiv 0 \pmod{2^t}, \text{ and}\\ 0 & \text{otherwise.}\end{cases} \tag{1.6}$$

Theorems 1.2–1.4 have the following interesting consequences. First of all, extending the results of [1], there are additional stable two-term recurrence sequences.

COROLLARY 1.5. *Let* $\{u_i\}$ *be the two-term recurrence sequence defined above, and suppose that one of the following conditions holds*:

(a) $b\equiv 5 \pmod 8$ *and* a *is odd*,
(b) $b\equiv 7 \pmod{16}$ *and* $a\equiv\pm 3 \pmod 8$, *or*
(c) $b\equiv 15 \pmod{16}$ *and* $a\equiv\pm 7 \pmod{16}$.

Then the sequence $\{u_i\}$ *is stable modulo* 2.

P r o o f. Stability of the indicated sequences is an immediate consequence of Theorems 1.2–1.4. ∎

The results of [1] can be combined with the results of this paper to describe the frequency distributions of many two-term recurrence sequences modulo two:

COROLLARY 1.6. *Let* $\{u_i\}$ *be the two-term recurrence sequence defined above, and* $\overline{b}$ *and* $\overline{a}$ *the standard representatives of* b *and* a *modulo* 16. *Then*

$$\Omega_{a,b}(2^k) = \begin{cases} \{0,1,2,3,8\} & \text{if } 5 \le k \text{ and } b \equiv 1 \pmod{16}, \\ \{0,1,2,3,2^{k-2}\} & \text{if } 2^t \parallel u_6,\ 4 \le k \le t, \text{ and } b \equiv 5 \pmod 8, \\ \{0,1,2,3,2^{t-2}\} & \text{if } 2^t \parallel u_6,\ t \le k, \text{ and } b \equiv 5 \pmod 8, \\ \{0,1,2,3\} & \text{if } 4 \le k \text{ and} \\ & \quad (\overline{b},\overline{a}) \in \{(3,5),(3,9),(11,9),(11,13)\}, \\ \{0,1,4\} & \text{if } 4 \le k \text{ and} \\ & \quad (\overline{b},\overline{a}) \in \{(3,7),(3,11),(11,3),(11,7)\}, \\ \{0,1,2^{k-2}\} & \text{if } 2^t \parallel u_3,\ 4 \le k \le t \text{ and} \\ & \quad (\overline{b},\overline{a}) \in \{(7,3),(7,5),(7,11),(7,13)\}, \\ \{0,1,2^{t-2}\} & \text{if } 2^t \parallel u_3,\ t \le k, \text{ and} \\ & \quad (\overline{b},\overline{a}) \in \{(7,3),(7,5),(7,11),(7,13)\}, \\ \{0,1,2\} & \text{if } 4 \le k \text{ and} \\ & \quad (\overline{b},\overline{a}) \in \{(15,3),(15,5),(15,11),(15,13)\}, \\ \{0,1,2^{k-3}\} & \text{if } 2^t \parallel u_3,\ 4 \le k \le t, \text{ and} \\ & \quad (\overline{b},\overline{a}) \in \{(15,7),(15,9)\}, \text{ and} \\ \{0,1,2^{t-3}\} & \text{if } 2^t \parallel u_3,\ t \le k, \text{ and} \\ & \quad (\overline{b},\overline{a}) \in \{(15,7),(15,9)\}. \end{cases}$$

In particular, for each pair $(\overline{b},\overline{a})$ *listed above,* $|\Omega_{a,b}(2^k)| \le 5$ *whenever* $k \ge 5$.

P r o o f. Corollary 1.6 follows immediately from Theorems 1.2–1.4, together with Corollary 1.2 of [1]. ∎

Although the sequences studied in this paper are stable modulo 2, they are not entirely tame. In particular, unlike the sequences studied in [1], they do not all become stable by the fifth generation. In fact, there exist two-term recurrence sequences that become stable only after an arbitrarily large number of generations. Moreover, the actual frequencies that occur are unbounded.

COROLLARY 1.7. *Let* $\{u_i\}$ *be the two-term recurrence sequence defined above. Suppose that one of the following conditions holds*:

(a) $b \equiv 5 \pmod 8$ *and* a *is odd*,

(b) $b \equiv 7 \pmod{16}$ *and* $a \equiv \pm 3 \pmod 8$, *or*

(c) $b \equiv 15 \pmod{16}$ *and* $a \equiv \pm 7 \pmod{16}$

and suppose that N *is a positive integer. Then there exist* a, b, *and* t *such that stability of the the two-term recurrence* $\{u_i\}$ *begins at generation* t *and* $t > N$. *Moreover, there exist* a, b, r, *and* t *such that* $\nu_{a,b}(2^t, r) > N$.

P r o o f. (a) Let $t = \nu_2(u_6)$. By Theorem 1.2, $\Omega_{a,b}(2^k) = \{0, 1, 2, 3, 2^{t-2}\}$ whenever $k \geq t$. On the other hand, if $t > 4$, then $\Omega_{a,b}(2^{t-1}) = \{0, 1, 2, 3, 2^{t-3}\}$. Thus, if $t > 4$, stability begins at generation t and, moreover, $\nu_{a,b}(2^t, 0) = 2^{t-2}$. Since $2^{t-2} > t$ when $t > 4$, it suffices to find a and b such that $b \equiv 5 \pmod 8$, a is odd, and $\nu_2(u_6) > \max(4, N)$.

Choose s such that s is even and $s > \max(4, N)$. Let $a = 1$ and $b = (2^s - 1)/3$. (Note that since s is even, $2^s - 1$ is divisible by 3, so b is an integer.) Now, by (3.1) below, $u_6 = u_3(2u_4 - au_3) = au_3(a^2 + 3b)$. But $\nu_2(u_6) \geq \nu_2(a^2 + 3b) = \nu_2(1 + 2^s - 1) = s > \max(4, N)$.

(b) Let $t = \nu_2(u_3)$. By Theorem 1.3, $\Omega_{a,b}(2^k) = \{0, 1, 2^{t-2}\}$ whenever $k \geq t$. On the other hand, if $t > 4$, then $\Omega_{a,b}(2^{t-1}) = \{0, 1, 2^{t-3}\}$. Thus, if $t > 4$, stability begins at generation t and $\nu_{a,b}(2^t, 0) = 2^{t-2}$. Since $2^{t-2} > t$ when $t > 4$, it suffices to find a and b such that $b \equiv 7 \pmod{16}$, $a \equiv \pm 3 \pmod 8$, and $\nu_2(u_3) > \max(4, N)$.

Choose s such that $s > \max(4, N)$ and let $a = 3$ and $b = 2^s - 9$. Then $u_3 = a^2 + b = 9 + (2^s - 9) = 2^s$. Consequently, $\nu_2(u_3) = s > \max(4, N)$, as desired.

(c) Let $t = \nu_2(u_3)$. By Theorem 1.4, $\Omega_{a,b}(2^k) = \{0, 1, 2^{t-3}\}$ whenever $k \geq t$. On the other hand, if $t > 4$, then $\Omega_{a,b}(2^{t-1}) = \{0, 1, 2^{t-4}\}$. Thus, if $t > 4$, stability begins at generation t and $\nu_{a,b}(2^t, 0) = 2^{t-3}$. Since $2^{t-3} > t$ when $t > 5$, it suffices to find a and b such that $b \equiv 15 \pmod{16}$, $a \equiv \pm 7 \pmod 8$, and $\nu_2(u_3) > \max(5, N)$.

Choose s such that $s > \max(5, N)$ and let $a = 7$ and $b = 2^s - 49$. Then $u_3 = a^2 + b = 49 + (2^s - 49) = 2^s$. Consequently, $\nu_2(u_3) = s > \max(5, N)$, as desired. ∎

2. Quoted results. In this section we present some definitions and terminology required in the proofs of Theorems 1.2–1.4, and summarize some basic lemmas whose proofs may be found in [1]. As usual, $\{u_i\}$ will denote the fixed two-term recurrence sequence defined by $u_0 = 0$, $u_1 = 1$ and $u_i = au_{i-1} + bu_{i-2}$ for all $i \geq 2$ and fixed odd integers a and b.

We begin with a definition of the parameters θ and ξ associated with the sequence $\{u_i\}$. These were originally introduced in greater generality in [1]:

$$\theta = \begin{cases} 5 & \text{if } b \equiv 1 \pmod 4 \text{ and } a \equiv 1 \pmod{16} \text{ or } a \equiv 15 \pmod{16}, \\ 3 & \text{if } b \equiv 1 \pmod 4 \text{ and } a \equiv 3 \pmod{16} \text{ or } a \equiv 13 \pmod{16}, \\ 7 & \text{if } b \equiv 1 \pmod 4 \text{ and } a \equiv 5 \pmod{16} \text{ or } a \equiv 11 \pmod{16}, \\ 1 & \text{if } b \equiv 1 \pmod 4 \text{ and } a \equiv 7 \pmod{16} \text{ or } a \equiv 9 \pmod{16}, \\ 0 & \text{if } b \equiv 3 \pmod 4 \text{ and } a \equiv 1 \pmod{16} \text{ or } a \equiv 15 \pmod{16}, \\ 6 & \text{if } b \equiv 3 \pmod 4 \text{ and } a \equiv 3 \pmod{16} \text{ or } a \equiv 13 \pmod{16}, \\ 2 & \text{if } b \equiv 3 \pmod 4 \text{ and } a \equiv 5 \pmod{16} \text{ or } a \equiv 11 \pmod{16}, \text{ and} \\ 4 & \text{if } b \equiv 3 \pmod 4 \text{ and } a \equiv 7 \pmod{16} \text{ or } a \equiv 9 \pmod{16}; \end{cases}$$

and

$$\xi = \begin{cases} 0 & \text{if } \begin{cases} b \equiv 5 \pmod{16} \text{ and } a \equiv 1 \pmod 8 \text{ or } a \equiv 7 \pmod 8 \text{ or} \\ b \equiv 7 \pmod{16} \text{ and } a \equiv 3 \pmod 8 \text{ or } a \equiv 5 \pmod 8 \text{ or} \\ b \equiv 13 \pmod{16} \text{ and } a \equiv 3 \pmod 8 \text{ or } a \equiv 5 \pmod 8 \text{ or} \\ b \equiv 15 \pmod{16} \text{ and } a \equiv 1 \pmod 8 \text{ or } a \equiv 7 \pmod 8, \text{and} \end{cases} \\ 2 & \text{if } \begin{cases} b \equiv 5 \pmod{16} \text{ and } a \equiv 3 \pmod 8 \text{ or } a \equiv 5 \pmod 8 \text{ or} \\ b \equiv 13 \pmod{16} \text{ and } a \equiv 1 \pmod 8 \text{ or } a \equiv 7 \pmod 8. \end{cases} \end{cases}$$

For reference we reproduce the well-known addition formulas for two-term recurrences and three lemmas describing general congruence relationships first proven in [1].

LEMMA 2.1. *The following formulas hold for all $m \geq 1$ and $n \geq 0$:*

$$\begin{aligned} u_{m+n} &= bu_{m-1}u_n + u_m u_{n+1}, \\ u_{2n+1} &= b(u_n)^2 + (u_{n+1})^2, \\ u_{2n} &= 2u_n u_{n+1} - a(u_n)^2. \end{aligned}$$

Proof. Lemma 2.1 of [1]. ∎

LEMMA 2.2. *The following congruences hold for all integers $k \geq 5$:*

$$\begin{aligned} u_{3\cdot 2^{k-3}} &\equiv \xi 2^{k-1} \pmod{2^{k+1}}, \\ u_{3\cdot 2^{k-3}+1} &\equiv (1 + 2^{k-2})^\theta \pmod{2^{k+1}}. \end{aligned}$$

Proof. Lemma 2.2 of [1]. ∎

LEMMA 2.3. *The following congruences hold for all $k \geq 5$:*

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

Proof. Lemma 2.6 of [1]. ∎

LEMMA 2.4. *Let n be a nonnegative integer.*

(a) *Then u_n is even if and only if $n \equiv 0 \pmod 3$.*

(b) *If $b \equiv 1 \pmod 4$, then $u_n \equiv 0 \pmod 8$ if and only if $n \equiv 0 \pmod 6$.*

(c) *If* $b \equiv 3 \pmod 4$, *then* $u_n \equiv 0 \pmod 4$ *if and only if* $n \equiv 0 \pmod 3$.

Proof. Lemma 2.4 of [1]. ∎

We will designate by $\lambda_{a,b}(2^k)$, or λ_k when a and b are understood, the length of the (shortest) period of $\{\overline{u}_i\}$. Many of these lengths were derived in Lemma 2.5 of [1]. We reproduce the required parts of that lemma here without proof, and extend the result to cover a few additional cases.

Lemma 2.5. *Each sequence* $\{u_i\}$ *has* (*shortest*) *period modulo* 2^k, *for* $k \geq 5$, *of length* λ_k *as follows.*

(a) *If* $b \equiv 1 \pmod 4$, *then* $\lambda_k = 3 \cdot 2^{k-1}$.

(b) *If* $b \equiv 7 \pmod{16}$ *and* $a \equiv 3, 5, 11,$ *or* $13 \pmod{16}$, *then* $\lambda_k = 3 \cdot 2^{k-2}$.

(c) *If* $b \equiv 15 \pmod{16}$ *and* $a \equiv 7$ *or* $9 \pmod{16}$, *then* $\lambda_k = 3 \cdot 2^{k-3}$.

Proof. (a) appears as Lemma 2.5(a) of [1]. We will prove (b) and (c).

First note that Lemma 2.5 of [1] provides us the following formulas:

$$\begin{aligned} u_{3s\cdot 2^{k-3}} &\equiv s\xi 2^{k-1} \pmod{2^{k+1}}, \\ u_{3s\cdot 2^{k-3}+1} &\equiv (1+2^{k-2})^{s\theta} \pmod{2^{k+1}}. \end{aligned} \tag{2.1}$$

(b) Assume that $b \equiv 7 \pmod{16}$ and $a \equiv 3, 5, 11,$ or $13 \pmod{16}$. Then, by definition, $\xi = 0$ and either $\theta = 2$ or $\theta = 6$ and, in either case, $\theta \equiv 2 \pmod 4$.

Now, by Lemma 2.4, $u_{2^{k-2}} \not\equiv 0 \pmod 4$. It follows that $u_{2^{k-2}} \not\equiv 0 \pmod{2^k}$
and therefore that λ_k does not divide 2^{k-2}. Moreover, replacing s by 2 in (2.1) and applying the binomial theorem yields:

$$\begin{aligned} u_{3\cdot 2^{k-2}} &\equiv 2\xi 2^{k-1} \equiv 0 \pmod{2^k}, \\ u_{3\cdot 2^{k-2}+1} &\equiv (1+2^{k-2})^{2\theta} \equiv 1 + 2\theta 2^{k-2} \equiv 1 + \theta 2^{k-1} \equiv 1 \pmod{2^k}. \end{aligned}$$

It follows that λ_k divides $3 \cdot 2^{k-2}$. On the other hand, applying (2.1) with s replaced by 1 yields

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

It follows that λ_k does not divide $3 \cdot 2^{k-3}$. We can now conclude that $\lambda_k = 3 \cdot 2^{k-2}$, as desired.

(c) Assume that $b \equiv 15 \pmod{16}$ and $a \equiv 7$ or $9 \pmod{16}$. Then, by definition, $\xi = 0$ and $\theta = 4$. By Lemma 2.4, $u_{2^{k-3}} \not\equiv 0 \pmod 4$. It follows that $u_{2^{k-3}} \not\equiv 0 \pmod{2^k}$ and therefore that λ_k does not divide 2^{k-3}.

Now, when s is replaced by 1, (2.1) and the binomial theorem yield:

$$\begin{aligned} u_{3\cdot 2^{k-3}} &\equiv \xi 2^{k-1} \equiv 0 \pmod{2^k}, \\ u_{3\cdot 2^{k-3}+1} &\equiv (1+2^{k-2})^{\theta} \equiv 1 + \theta 2^{k-2} \equiv 1 \pmod{2^k}. \end{aligned}$$

It follows that λ_k divides $3 \cdot 2^{k-3}$.

If $k \geq 6$, then we can replace k by $k-1$ in (2.1) to obtain

$$u_{3\cdot 2^{k-4}+1} \equiv (1+2^{k-3})^{\theta} \equiv 1+\theta 2^{k-3} \equiv 1+2^{k-1} \pmod{2^k}. \tag{2.2}$$

It follows that λ_k does not divide $3 \cdot 2^{k-4}$ when $k \geq 6$, and hence $\lambda_k = 3 \cdot 2^{k-3}$, as desired.

It remains to verify that (2.2) remains true when $k = 5$. However, we know that $u_3 = a^2 + b \equiv 49 + 15 \equiv 64 \equiv 0 \pmod{2^5}$. Therefore Lemma 2.1 yields

$$\begin{aligned} u_{3\cdot 2+1} &= b(u_3)^2 + (u_4)^2 \\ &\equiv (u_4)^2 \equiv (au_3 + bu_2)^2 \equiv (ba)^2 \pmod{2^5} \\ &\equiv (105)^2 \equiv 17 \equiv 1 + 2^4 \pmod{2^5}, \end{aligned}$$

as desired. ∎

3. Preliminary lemmas. Throughout this section fix odd integers a and b and let $\{u_i\}$ be the two-term recurrence sequence defined above. The work in this paper extends that in [1]. Crucial to this extension is a careful analysis of $\nu_2(u_n)$ for those n that are divisible by three. Determining these values will be our first goal.

LEMMA 3.1. (a) *If* $b \equiv 3 \pmod 4$ *and* $2^t \parallel u_3$, *then* $t \geq 2$.
(b) *If* $b \equiv 1 \pmod 2$ *and* $2^t \parallel u_6$, *then* $t \geq 3$.

Proof. (a) By Lemma 2.4, $u_3 \equiv 0 \pmod 4$ when $b \equiv 3 \pmod 4$. Thus 2^2 divides u_3, as desired.

(b) By Lemma 2.4, $u_6 \equiv 0 \pmod 8$ when $b \equiv 1 \pmod 8$ or $b \equiv 5 \pmod 8$. Thus 2^3 divides u_6 in these cases.

It remains to prove the claim when $b \equiv 3 \pmod 8$ or $b \equiv 7 \pmod 8$. But if so, then $b \equiv 3 \pmod 4$ and, by (a), 2^2 divides u_3. On the other hand, by Lemma 2.1,

$$u_6 = u_{2\cdot 3} = 2u_3u_4 - a(u_3)^2 = u_3(2u_4 - au_3). \tag{3.1}$$

Since u_3 is certainly even, $(2u_4 - au_3)$ is also even, and hence 2^3 divides u_6, as desired. ∎

LEMMA 3.2. *If* $n \geq 0$ *and* $m \geq 0$, *then* u_n *divides* u_{nm}.

Proof. This lemma follows easily from Lemma 2.1 by induction on m. ∎

The next two lemmas were proven by R. D. Carmichael and appear, in part, in Theorem X on p. 42 of [2]. While the methods used there may be extended to prove Lemma 3.3 and Lemma 3.5, for the convenience of the reader we provide elementary proofs.

LEMMA 3.3. *If* $2^t \parallel u_3$, $t \geq 2$, $r \geq 0$, *and* $n \equiv 3 \cdot 2^r \pmod{3 \cdot 2^{r+1}}$, *then* $2^{t+r} \parallel u_n$.

N o t e. In view of Lemma 3.1, the hypothesis that $t \geq 2$ is always true when $b \equiv 3 \pmod 4$. On the other hand, if $b \equiv 1 \pmod 4$, then $u_3 = a^2 + b \equiv 1 + 1 \equiv 2 \pmod 4$, and hence the hypothesis that $t \geq 2$ is false.

P r o o f o f L e m m a 3.3. Proceed by induction on r. First, suppose that $r = 0$. Then $n \equiv 3 \pmod 6$, so we can find an integer k such that $n = 6k + 3$. By Lemma 3.2, u_6 divides u_{6k}, so we can find an integer l such that $u_{6k} = u_6 l$. Moreover, by (3.1), $u_6 = u_3(2u_4 - au_3)$. Thus $u_{6k} = u_3(2u_4 - au_3)l$.

Now, by Lemma 2.1,

$$u_n = u_{6k+3} = bu_{6k-1}u_3 + u_{6k}u_4 = u_3(bu_{6k-1} + (2u_4 - au_3)lu_4).$$

Since 2^t divides u_3, it follows that 2^t divides u_n. Furthermore, by Lemma 2.4, u_{6k-1} is odd, while u_3 is even. Thus $bu_{6k-1} + (2u_4 - au_3)lu_4$ is odd. It now follows that $2^t \parallel u_n$, as desired.

Now suppose $r \geq 0$ and that $2^{t+r} \parallel u_m$ whenever $m \equiv 3 \cdot 2^r \pmod{3 \cdot 2^{r+1}}$. Assume that $n \equiv 3 \cdot 2^{r+1} \pmod{3 \cdot 2^{r+2}}$. Then we can find an integer k such that $n = 3 \cdot 2^{r+1} + 3 \cdot 2^{r+2}k = 3 \cdot 2^{r+1}(1 + 2k)$. Let $l = 1 + 2k$.

By Lemma 2.1,

$$\begin{aligned} u_n &= u_{3 \cdot 2^{r+1} l} = u_{2 \cdot (3 \cdot 2^r l)} = 2u_{3 \cdot 2^r l}u_{3 \cdot 2^r l + 1} - a(u_{3 \cdot 2^r l})^2 \\ &= u_{3 \cdot 2^r l}(2u_{3 \cdot 2^r l + 1} - au_{3 \cdot 2^r l}). \end{aligned}$$

Since $3 \cdot 2^r l = 3 \cdot 2^r(1 + 2k) = 3 \cdot 2^r + 3 \cdot 2^{r+1}k \equiv 3 \cdot 2^r \pmod{3 \cdot 2^{r+1}}$, it follows from the induction hypothesis that $2^{t+r} \parallel u_{3 \cdot 2^r l}$. In particular, we can find an odd integer j such that $u_{3 \cdot 2^r l} = 2^{t+r} j$.

Thus

$$\begin{aligned} u_n &= u_{3 \cdot 2^r l}(2u_{3 \cdot 2^r l + 1} - au_{3 \cdot 2^r l}) = 2^{t+r} j(2u_{3 \cdot 2^r l + 1} - a2^{t+r} j) \\ &= 2^{t+r+1} j(u_{3 \cdot 2^r l + 1} - a2^{t+r-1} j). \end{aligned}$$

By Lemma 2.4, $u_{3 \cdot 2^r l + 1}$ is odd. On the other hand, $t \geq 2$, so $t + r - 1 \geq 2 + r - 1 \geq r + 1 \geq 1$, and therefore $a2^{t+r-1} j$ is even. It follows that $j(u_{3 \cdot 2^r l + 1} - a2^{t+r-1} j)$ is odd, and hence $2^{t+r+1} \parallel u_n$, as desired. ∎

C o r o l l a r y 3.4. *If* $2^t \parallel u_3$, $b \equiv 3 \pmod 4$, *and* $k \geq t$, *then* $u_{3 \cdot 2^{k-t}} \equiv 2^k \pmod{2^{k+1}}$.

P r o o f. By Lemma 3.1, $t \geq 2$. Moreover, by hypothesis, $k - t \geq 0$. Thus we can apply Lemma 3.3 with $k - t$ in place of r, to conclude that $2^{t+(k-t)} \parallel u_{3 \cdot 2^{k-t}}$. Consequently, $u_{3 \cdot 2^{k-t}} \equiv 2^k \pmod{2^{k+1}}$, as desired. ∎

L e m m a 3.5. *If* $2^t \parallel u_6$, $r \geq 1$, *and* $n \equiv 3 \cdot 2^r \pmod{3 \cdot 2^{r+1}}$, *then* $2^{t+r-1} \parallel u_n$.

N o t e. If $b \equiv 3 \pmod 4$, then we can apply Lemma 3.1 and Lemma 3.3 to obtain Lemma 3.5 immediately.

Proof of Lemma 3.5. Proceed by induction on r. First, suppose that $r = 1$. Then $n \equiv 6 \pmod{12}$, so we can find an integer k such that $n = 12k+6$. By Lemma 3.2, u_{12} divides u_{12k}, so we can find an integer l such that $u_{12k} = u_{12}l$. Moreover, by Lemma 2.1, $u_{12} = u_{2\cdot 6} = 2u_6u_7 - a(u_6)^2 = u_6(2u_7 + au_6)$. Thus $u_{12k} = u_6(2u_7 + au_6)l$.

Now, by Lemma 2.1,

$$u_n = u_{12k+6} = bu_{12k-1}u_6 + u_{12k}u_7 = u_6(bu_{12k-1} + (2u_7 + au_6)lu_7).$$

Since 2^t divides u_6, it follows that 2^t divides u_n. Furthermore, by Lemma 2.4, u_{12k-1} is odd while u_6 is even. Thus $bu_{12k-1} + (2u_7 + au_6)lu_7$ is odd. It now follows that $2^t \parallel u_n$, as desired.

Now suppose $r \geq 1$ and that $2^{t+r-1} \parallel u_n$ whenever $n \equiv 3 \cdot 2^r \pmod{3 \cdot 2^{r+1}}$. Assume that $n \equiv 3 \cdot 2^{r+1} \pmod{3 \cdot 2^{r+2}}$. Then we can find an integer k such that $n = 3 \cdot 2^{r+1} + 3 \cdot 2^{r+2}k = 3 \cdot 2^{r+1}(1 + 2k)$. Let $l = 1 + 2k$.

As in the proof of Lemma 3.3, Lemma 2.1 implies that

$$u_n = u_{3\cdot 2^r l}(2u_{3\cdot 2^r l+1} - au_{3\cdot 2^r l}).$$

Since $3 \cdot 2^r l = 3 \cdot 2^r(1 + 2k) = 3 \cdot 2^r + 3 \cdot 2^{r+1}k \equiv 3 \cdot 2^r \pmod{3 \cdot 2^{r+1}}$, it follows from the induction hypothesis that $2^{t+r-1} \parallel u_{3\cdot 2^r l}$. In particular, we can find an odd integer j such that $u_{3\cdot 2^r l} = 2^{t+r-1}j$.

Thus

$$\begin{aligned} u_n &= u_{3\cdot 2^r l}(2u_{3\cdot 2^r l+1} - au_{3\cdot 2^r l}) = 2^{t+r-1}j(2u_{3\cdot 2^r l+1} - a2^{t+r-1}j) \\ &= 2^{t+r}j(u_{3\cdot 2^r l+1} - a2^{t+r-2}j). \end{aligned}$$

By Lemma 2.4, $u_{3\cdot 2^r l+1}$ is odd. On the other hand, by Lemma 3.1, $t \geq 3$, so $t + r - 2 \geq 3 + r - 2 \geq r + 1 \geq 1$, and therefore $a2^{t+r-2}j$ is even. It follows that $j(u_{3\cdot 2^r l+1} - a2^{t+r-2}j)$ is odd, and hence $2^{t+r} \parallel u_n$, as desired. ∎

Corollary 3.6. *If* $2^t \parallel u_6$ *and* $k \geq t$, *then* $u_{3\cdot 2^{k-t+1}} \equiv 2^k \pmod{2^{k+1}}$.

Proof. By hypothesis, $k - t + 1 \geq 1$. Thus, by Lemma 3.5, with $k - t + 1$ in place of r, we conclude that $2^{t+(k-t)} \parallel u_{3\cdot 2^{k-t+1}}$. Therefore $u_{3\cdot 2^{k-t+1}} \equiv 2^k \pmod{2^{k+1}}$, as desired. ∎

The key step in the proof of our main theorem uses the fact that for each integer n, there exists an integer r with the property that $u_{n+3\cdot 2^r} \equiv u_n + 2^k \pmod{2^{k+1}}$ for sufficiently large k. In the next lemmas we identify such values when $n \equiv 0 \pmod 3$.

Lemma 3.7. (a) *If* $2^t \parallel u_3$, $b \equiv 3 \pmod 4$, $n \equiv 0 \pmod 3$, *and* $k \geq t$, *then* $u_{n+3\cdot 2^{k-t}} \equiv u_n + 2^k \pmod{2^{k+1}}$.

(b) *If* $2^t \parallel u_6$, $b \equiv 1 \pmod 2$, $n \equiv 0 \pmod 6$, *and* $k \geq t$, *then* $u_{n+3\cdot 2^{k-t+1}} \equiv u_n + 2^k \pmod{2^{k+1}}$.

Proof. (a) We treat the cases $k = t$ and $k = t + 1$ first, then consider $k \geq t + 2$.

Suppose that $k = t$. Since $2^t \parallel u_3$ and $n \equiv 0 \pmod 3$, Lemma 3.2 implies that 2^t divides u_n. Therefore, since both a and b are odd, it follows that $bu_2u_n \equiv u_n \pmod{2^{t+1}}$. Similarly, since $2^t \parallel u_3$ and, by Lemma 2.4, u_{n+1} is odd, it follows that $u_3u_{n+1} \equiv 2^t \pmod{2^{t+1}}$. Thus, by Lemma 2.1,

$$u_{n+3\cdot 2^{k-t}} = u_{3+n} = bu_2u_n + u_3u_{n+1} \equiv u_n + 2^t \pmod{2^{t+1}},$$

as desired.

Next, suppose that $k = t + 1$. By Corollary 3.4, $u_6 \equiv 2^{t+1} \pmod{2^{t+2}}$. Since, by Lemma 2.4, u_{n+1} is odd, it follows that $u_6u_{n+1} \equiv 2^{t+1} \pmod{2^{t+2}}$. Since $n \equiv 0 \pmod 3$, Lemma 3.2 implies that 2^t divides u_n. On the other hand, reduction of the sequence $\{u_i\}$ modulo 4 yields one of the following two sequences:

$$\begin{aligned} &0,1,1,0,3,3,0,1,\ldots \quad \text{if } b \equiv 3 \pmod 4 \text{ and } a \equiv 1 \pmod 4,\\ &0,1,3,0,1,3,0,1,\ldots \quad \text{if } b \equiv 3 \pmod 4 \text{ and } a \equiv 3 \pmod 4. \end{aligned} \tag{3.2}$$

Consequently, $bu_5 \equiv 3\cdot 3 \equiv 1 \pmod 4$. It follows that $bu_5u_n \equiv u_n \pmod{2^{t+2}}$. Thus, by Lemma 2.1,

$$u_{n+3\cdot 2^{k-t}} = u_{6+n} = bu_5u_n + u_6u_{n+1} \equiv u_n + 2^{t+1} \pmod{2^{t+2}},$$

as desired.

Finally, suppose that $k \geq t + 2$. Then $k - t \geq 2$, and hence Lemma 2.2 shows that

$$u_{3\cdot 2^{k-t}+1} \equiv (1 + 2^{k-t+1})^\theta \pmod{2^{k-t+4}}.$$

Therefore we can find an integer l such that

$$u_{3\cdot 2^{k-t}+1} = (1 + 2^{k-t+1})^\theta + l2^{k-t+4}.$$

Now, by the binomial theorem, we can find an integer s such that

$$u_{3\cdot 2^{k-t}+1} = 1 + \theta 2^{k-t+1} + s2^{2(k-t+1)} + l2^{k-t+4}. \tag{3.3}$$

Since n is divisible by 3, there exists a unique integer r such that $r \geq 0$ and $n \equiv 3 \cdot 2^r \pmod{3 \cdot 2^{r+1}}$. Moreover, $b \equiv 3 \pmod 4$, so, by Lemma 3.1, we know that $t \geq 2$. Therefore, by Lemma 3.3, $2^{t+r} \parallel u_n$. Thus there is odd integer j such that $u_n = 2^{t+r}j$. Combining this result with (3.3) yields

$$u_nu_{3\cdot 2^{k-t}+1} = u_n + j\theta 2^{k+r+1} + js2^{2k-t+r+2} + jl2^{k+r+4}.$$

Since $r \geq 0$ and $k - t \geq 0$,

$$u_nu_{3\cdot 2^{k-t}+1} \equiv u_n \pmod{2^{k+1}}. \tag{3.4}$$

Now, Lemma 2.4 implies that u_{n-1} is odd. Since b is also odd, Corollary 3.4 yields

$$bu_{n-1}u_{3\cdot 2^{k-t}} \equiv 2^k \pmod{2^{k+1}}.$$

Finally, by Lemma 2.1,

$$u_{n+3\cdot 2^{k-t}} = bu_{n-1}u_{3\cdot 2^{k-t}} + u_n u_{3\cdot 2^{k-t}+1} \equiv u_n + 2^k \pmod{2^{k+1}},$$

as desired.

(b) We treat the case $k = t$ and then consider $k \geq t+1$.

Suppose that $k = t$. Then $u_{n+3\cdot 2^{k-t+1}} = u_{n+6}$. As in (a), $u_{n+6} = bu_5u_n + u_6u_{n+1}$. By Lemma 2.4, u_{n+1} is odd and, by hypothesis, $2^t \parallel u_6$. Thus $u_6u_{n+1} \equiv 2^t \pmod{2^{t+1}}$. On the other hand, b and u_5 are both odd and, by Lemma 3.2, $2^t \mid u_n$. Therefore $bu_5u_n \equiv u_n \pmod{2^{t+1}}$. It now follows that

$$u_{n+3\cdot 2^{k-t+1}} = u_{n+6} \equiv u_n + 2^t \pmod{2^{t+1}},$$

as desired.

Now suppose that $k \geq t+1$. Then $k-t+1 \geq 2$, and hence Lemma 2.2 shows that

$$u_{3\cdot 2^{k-t+1}+1} \equiv (1+2^{k-t+2})^\theta \pmod{2^{k-t+5}}.$$

Therefore we can find an integer l such that

$$u_{3\cdot 2^{k-t+1}+1} = (1+2^{k-t+2})^\theta + l2^{k-t+5}.$$

Now, by the binomial theorem, we can find an integer s such that

$$u_{3\cdot 2^{k-t+1}+1} = 1 + \theta 2^{k-t+2} + s2^{2(k-t+2)} + l2^{k-t+5}. \tag{3.5}$$

Since n is divisible by 6, there is a unique integer r such that $r \geq 1$ and $n \equiv 3\cdot 2^r \pmod{3\cdot 2^{r+1}}$. Therefore, by Lemma 3.5, $2^{t+r-1} \parallel u_n$. Thus there is an odd integer j such that $u_n = 2^{t+r-1}j$. Combining this result with (3.5) yields

$$u_n u_{3\cdot 2^{k-t+1}+1} = u_n + j\theta 2^{k+r+1} + js2^{2k-t+r+3} + jl2^{k+r+4}.$$

Since $r \geq 0$ and $k-t \geq 0$,

$$u_n u_{3\cdot 2^{k-t+1}+1} \equiv u_n \pmod{2^{k+1}}. \tag{3.6}$$

Now, Lemma 2.4 implies that u_{n-1} is odd. Since b is also odd, Corollary 3.6 yields

$$bu_{n-1}u_{3\cdot 2^{k-t+1}} \equiv 2^k \pmod{2^{k+1}}.$$

Finally, by Lemma 2.1,

$$u_{n+3\cdot 2^{k-t+1}} = bu_{n-1}u_{3\cdot 2^{k-t+1}} + u_n u_{3\cdot 2^{k-t+1}+1} \equiv u_n + 2^k \pmod{2^{k+1}},$$

as desired. ∎

4. Proofs of the main theorems. In this section we will prove Theorems 1.2–1.4. The proofs of these theorems are similar, each using a counting argument modeled after the argument in [3]. We will provide complete proofs for Theorems 1.2 and 1.3, followed by an outline of the proof of Theorem 1.4.

Proof of Theorem 1.2. Fix integers a and b such that $b \equiv 5 \pmod 8$ and a is odd, and let $\{u_i\}$ be the two-term recurrence sequence

defined by $u_0 = 0$, $u_1 = 1$ and for all $i \geq 2$, $u_i = au_{i-1} + bu_{i-2}$. Note that, by Lemma 2.5, $\lambda_k = 3 \cdot 2^{k-1}$. We break the proof into five easy pieces.

Step 1. *For all* $k \geq 3$,

$$\nu_{a,b}(2^k, r) \geq \begin{cases} 1 & \text{if } r \equiv 3 \pmod 4, \\ 2 & \text{if } r \equiv 6 \pmod 8, \\ 3 & \text{if } r \equiv 1 \pmod 4. \end{cases} \tag{4.1}$$

Proof. Proceed by induction on k. The induction may be started with $k = 3$, 4 and 5 by an explicit (computer assisted) computation of the frequencies.

Now fix $k \geq 5$ and assume (4.1).

Suppose that $r \equiv 3 \pmod 4$. Then, by the induction hypothesis, $\nu(2^k, r) \geq 1$. Thus we can find an integer n such that $0 \leq n < \lambda_k$ and $u_n \equiv r \pmod{2^k}$. It follows that either $u_n \equiv r \pmod{2^{k+1}}$ or $u_n \equiv r + 2^k \pmod{2^{k+1}}$. In the first case, $\nu(2^{k+1}, r) \geq 1$, as desired. In the second case, Lemma 2.3, together with the induction hypothesis and the binomial theorem yields

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

and therefore $\nu(2^{k+1}, r) \geq 1$, as desired.

Next, suppose that $r \equiv 6 \pmod 8$. By the induction hypothesis, $\nu(2^k, r) \geq 2$, so we can find two integers n_1 and n_2 such that $0 \leq n_1 < n_2 < \lambda_k$ and $u_{n_1} \equiv u_{n_2} \equiv r \pmod{2^k}$. It follows that $u_{n_1} \equiv r \pmod{2^{k+1}}$ or $u_{n_1} \equiv r + 2^k \pmod{2^{k+1}}$ and similarly $u_{n_2} \equiv r \pmod{2^{k+1}}$ or $u_{n_2} \equiv r + 2^k \pmod{2^{k+1}}$. If $u_{n_1} \equiv r \pmod{2^{k+1}}$, then Lemma 2.3 and the fact that r is even imply that $u_{n_1} \equiv u_{n_1+3\cdot 2^{k-1}} \equiv r \pmod{2^{k+1}}$, and therefore $\nu(2^{k+1}, r) \geq 2$. Similarly, if $u_{n_2} \equiv r \pmod{2^{k+1}}$, then $u_{n_2} \equiv u_{n_2+3\cdot 2^{k-1}} \equiv r \pmod{2^{k+1}}$, and $\nu(2^{k+1}, r) \geq 2$. Therefore we can assume that $u_{n_1} \equiv u_{n_2} \equiv r + 2^k \pmod{2^{k+1}}$. Then, since $r \equiv 2 \pmod 4$, Lemma 2.3, the induction hypothesis, and the binomial theorem yield

$$\begin{aligned} u_{n_1+3\cdot 2^{k-2}} &\equiv bu_{n-1}\xi 2^k + u_n(1 + 2^{k-1})^\theta \pmod{2^{k+1}} \\ &\equiv u_n(1 + 2^{k-1})^\theta \pmod{2^{k+1}} \\ &\equiv (r + 2^k)(1 + \theta 2^{k-1}) \pmod{2^{k+1}} \\ &\equiv r + 2^k + r\theta 2^{k-1} \pmod{2^{k+1}} \\ &\equiv r \pmod{2^{k+1}}. \end{aligned}$$

Similarly, $u_{n_2+3\cdot 2^{k-2}} \equiv r \pmod{2^{k+1}}$. It follows that $\nu(2^{k+1}, r) \geq 2$, as desired.

Finally, suppose that $r \equiv 1 \pmod 4$. Then, by the induction hypothesis, $\nu(2^k, r) \geq 3$. Therefore we can find integers n_1, n_2, and n_3 such that $0 \leq n_1 < n_2 < n_3 < \lambda_k$ and $u_{n_i} \equiv r \pmod{2^k}$. Again, for each i, Lemma 2.3 implies that either $u_{n_i} \equiv r \pmod{2^{k+1}}$ or $u_{n_i + 3\cdot 2^{k-1}} \equiv r \pmod{2^{k+1}}$. Since $\lambda_k = 3 \cdot 2^{k-1}$, it follows that $n_i + 3 \cdot 2^{k-1} \geq 3 \cdot 2^{k-1} = \lambda_k$, for each $i \in \{1, 2, 3\}$, and hence the integers n_1, n_2, n_3, $n_1 + 3 \cdot 2^{k-1}$, $n_2 + 3 \cdot 2^{k-1}$, and $n_3 + 3 \cdot 2^{k-1}$ are distinct. It follows that $\nu(2^{k+1}, r) \geq 3$, as desired. ∎

Step 2. *If* $4 \leq k \leq t$ *and* $r = 0$, *then*

$$\nu(2^k, r) \geq 2^{k-2}. \tag{4.2}$$

Proof. Fix k such that $4 \leq k \leq t$. Since, by definition, $2^t \parallel u_6$, it is clear that $u_6 \equiv 0 \pmod{2^t}$. But $k \leq t$, so $u_6 \equiv 0 \pmod{2^k}$. It follows from Lemma 3.2 that $u_{6m} \equiv 0 \pmod{2^k}$ for all nonnegative integers m. By Lemma 2.5, $\lambda_k = 3 \cdot 2^{k-1}$. Thus, if m satisfies $0 \leq m < 2^{k-2}$, then $0 \leq 6m < 3 \cdot 2^{k-1}$ and consequently the elements $\{u_{6m} \mid 0 \leq m < 2^{k-2}\}$ lie in one period of the sequence $\{u_i\}$ modulo 2^k. Therefore $\nu(2^k, 0) \geq 2^{k-2}$, as desired. ∎

Step 3. *If* $k \geq t$ *and* $r \equiv 0 \pmod{2^t}$, *then*

$$\nu(2^k, r) \geq 2^{t-2}. \tag{4.3}$$

Proof. Proceed by induction on k. The first step of the induction, when $k = t$, follows from Step 2.

Now fix $k \geq t$ and r such that $r \equiv 0 \pmod{2^t}$, and assume (4.3). Choose l such that $u_l \equiv r \pmod{2^k}$. Note that, since $u_l \equiv 0 \pmod{2^t}$, it follows from Lemma 2.4 that $l \equiv 0 \pmod 6$. Thus, by Lemma 3.7,

$$u_{l+3\cdot 2^{k-t+1}} \equiv u_l + 2^k \pmod{2^{k+1}},$$

and therefore there is an integer n such that $u_n \equiv r \pmod{2^{k+1}}$. By Lemma 3.7,

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

and hence, for all nonnegative integers m,

$$u_{n+m\cdot 3\cdot 2^{k-t+2}} \equiv r \pmod{2^{k+1}}. \tag{4.4}$$

In particular, since $\lambda_{k+1} = 3 \cdot 2^k$, the elements $\{u_{n+m\cdot 3\cdot 2^{k-t+2}} \mid 0 \leq m < 2^{t-2}\}$ lie in one period of the sequence $\{u_i\}$ modulo 2^{k+1} and satisfy (4.4). Therefore $\nu(2^{k+1}, r) \geq 2^{t-2}$, as desired. This completes the induction. ∎

Step 4. *If* $4 \leq k \leq t$, *then* (1.1) *holds.*

P r o o f. Let k be an integer such that $4 \le k \le t$. By Lemma 2.5, $\lambda_k = 3 \cdot 2^{k-1}$. Consequently, the inequalities proven in Steps 1 and 2 imply that

$$\begin{aligned}\lambda_k = 3 \cdot 2^{k-1} &= \sum_{r=0}^{2^k-1} \nu(2^k, r) \\ &\ge \sum_{r \equiv 3 \,(\mathrm{mod}\ 4)} \nu(2^k, r) + \sum_{r \equiv 6 \,(\mathrm{mod}\ 8)} \nu(2^k, r) \\ &\quad + \sum_{r \equiv 1 \,(\mathrm{mod}\ 4)} \nu(2^k, r) + \nu(2^k, 0) \\ &\ge 1 \cdot 2^{k-2} + 2 \cdot 2^{k-3} + 3 \cdot 2^{k-2} + 2^{k-2} = 6 \cdot 2^{k-2} = \lambda_k.\end{aligned}$$

It follows that each inequality proven in Steps 1 and 2 is an equality. This proves (1.1). ∎

Step 5. *If* $k \ge t$, *then* (1.2) *holds.*

P r o o f. Let k be an integer such that $k \ge t$. By Lemma 2.5, $\lambda_k = 3 \cdot 2^{k-1}$. Consequently, the inequalities proven in Steps 1 and 3 imply that

$$\begin{aligned}\lambda_k = 3 \cdot 2^{k-1} &= \sum_{r=0}^{2^k-1} \nu(2^k, r) \\ &\ge \sum_{r \equiv 3 \,(\mathrm{mod}\ 4)} \nu(2^k, r) + \sum_{r \equiv 6 \,(\mathrm{mod}\ 8)} \nu(2^k, r) \\ &\quad + \sum_{r \equiv 1 \,(\mathrm{mod}\ 4)} \nu(2^k, r) + \sum_{r \equiv 0 \,(\mathrm{mod}\ 2^t)} \nu(2^k, r) \\ &\ge 1 \cdot 2^{k-2} + 2 \cdot 2^{k-3} + 3 \cdot 2^{k-2} + 2^{t-2}2^{k-t} = 6 \cdot 2^{k-2} = \lambda_k.\end{aligned}$$

It follows that each inequality proven in Steps 1 and 3 is an equality. This proves (1.2). ∎

This completes the proof of Theorem 1.2. ∎

The proof of Theorem 1.3 follows the same general outline as the proof of Theorem 1.2.

P r o o f o f T h e o r e m 1.3. Fix integers a and b such that $b \equiv 7 \pmod{16}$ and $a \equiv \pm 3 \pmod 8$, and let $\{u_i\}$ be the two-term recurrence sequence defined by $u_0 = 0$, $u_1 = 1$ and for all $i \ge 2$, $u_i = au_{i-1} + bu_{i-2}$. Note that, by Lemma 2.5, $\lambda_k = 3 \cdot 2^{k-2}$. As in the proof of Theorem 1.2, we break the proof into five easy pieces.

Step 1. *For all* $k \ge 4$, *if* $r \equiv 1 \pmod 2$, *then*

$$\nu_{a,b}(2^k, r) \ge 1. \tag{4.5}$$

P r o o f. Proceed by induction on k. The induction may be started with $k = 4$ and 5 by an explicit (computer assisted) computation of the frequencies.

Now fix $k \geq 5$ and r such that $r \equiv 1 \pmod 2$, and assume (4.5).

By the induction hypothesis, $\nu(2^k, r) \geq 1$. Thus we can find an integer n such that $0 \leq n < \lambda_k$ and $u_n \equiv r \pmod{2^k}$. It follows that either $u_n \equiv r \pmod{2^{k+1}}$ or $u_n \equiv r + 2^k \pmod{2^{k+1}}$. In the first case, $\nu(2^{k+1}, r) \geq 1$, as desired. In the second case, Lemma 2.3, together with the induction hypothesis and the binomial theorem implies that $u_{n+3\cdot 2^{k-2}} \equiv r \pmod{2^{k+1}}$, and therefore $\nu(2^{k+1}, r) \geq 1$, as desired. ∎

Step 2. *If* $4 \leq k \leq t$ *and* $r = 0$, *then*

$$\nu(2^k, r) \geq 2^{k-2}. \tag{4.6}$$

P r o o f. Fix k such that $4 \leq k \leq t$. Since, by definition, $2^t \parallel u_3$, it is clear that $u_3 \equiv 0 \pmod{2^t}$. But $k \leq t$, so $u_3 \equiv 0 \pmod{2^k}$. It follows from Lemma 3.2 that $u_{3m} \equiv 0 \pmod{2^k}$ for all nonnegative integers m. By Lemma 2.5, $\lambda_k = 3 \cdot 2^{k-2}$. Thus, if m satisfies $0 \leq m < 2^{k-2}$, then $0 \leq 3m < 3 \cdot 2^{k-2}$ and consequently the elements $\{u_{3m} \mid 0 \leq m < 2^{k-2}\}$ lie in one period of the sequence $\{u_i\}$ modulo 2^k. Therefore $\nu(2^k, 0) \geq 2^{k-2}$, as desired. ∎

Step 3. *If* $k \geq t$ *and* $r \equiv 0 \pmod{2^t}$, *then*

$$\nu(2^k, r) \geq 2^{t-2}. \tag{4.7}$$

P r o o f. Proceed by induction on k. The first step of the induction, when $k = t$, follows from Step 2.

Now fix $k \geq t$ and r such that $r \equiv 0 \pmod{2^t}$, and assume (4.7). Choose l such that $u_l \equiv r \pmod{2^k}$. Note that, since $u_l \equiv 0 \pmod{2^t}$, it follows from Lemma 2.4 that $l \equiv 0 \pmod 3$. Thus, by Lemma 3.7,

$$u_{l+3\cdot 2^{k-t}} \equiv u_l + 2^k \pmod{2^{k+1}},$$

and therefore there is an integer n such that $u_n \equiv r \pmod{2^{k+1}}$. By Lemma 3.7,

$$\begin{aligned} u_{n+3\cdot 2^{k-t+1}} &\equiv u_{n+3\cdot 2^{k-t}} + 2^k \pmod{2^{k+1}} \\ &\equiv u_n \pmod{2^{k+1}} \\ &\equiv r \pmod{2^{k+1}}, \end{aligned}$$

and hence, for all nonnegative integers m,

$$u_{n+m\cdot 3\cdot 2^{k-t+1}} \equiv r \pmod{2^{k+1}}. \tag{4.8}$$

In particular, since $\lambda_{k+1} = 3 \cdot 2^{k-1}$, the elements $\{u_{n+m\cdot 3\cdot 2^{k-t+1}} \mid 0 \leq m < 2^{t-2}\}$ lie in one period of the sequence $\{u_i\}$ modulo 2^{k+1} and satisfy (4.8). Therefore $\nu(2^{k+1}, r) \geq 2^{t-2}$, as desired. This completes the induction. ∎

Step 4. *If* $4 \le k \le t$, *then* (1.3) *holds.*

Proof. Let k be an integer such that $4 \le k \le t$. By Lemma 2.5, $\lambda_k = 3 \cdot 2^{k-2}$. Consequently, the inequalities proven in Steps 1 and 2 imply that

$$\lambda_k = 3 \cdot 2^{k-2} = \sum_{r=0}^{2^k-1} \nu(2^k, r) \ge \sum_{r \equiv 1 \pmod 2} \nu(2^k, r) + \nu(2^k, 0)$$
$$\ge 1 \cdot 2^{k-1} + 2^{k-2} = 2 \cdot 2^{k-2} + 2^{k-2} = \lambda_k.$$

It follows that each inequality proven in Steps 1 and 2 is an equality. This proves (1.3). ∎

Step 5. *If* $k \ge t$, *then* (1.4) *holds.*

Proof. Let k be an integer such that $k \ge t$. By Lemma 2.5, $\lambda_k = 3 \cdot 2^{k-2}$. Consequently, the inequalities proven in Steps 1 and 3 imply that

$$\lambda_k = 3 \cdot 2^{k-2} = \sum_{r=0}^{2^k-1} \nu(2^k, r) \ge \sum_{r \equiv 1 \pmod 2} \nu(2^k, r) + \sum_{r \equiv 0 \pmod{2^t}} \nu(2^k, r)$$
$$\ge 1 \cdot 2^{k-1} + 2^{t-2} 2^{k-t} = 2 \cdot 2^{k-2} + 2^{k-2} = \lambda_k.$$

It follows that each inequality proven in Steps 1 and 3 is an equality. This proves (1.4). ∎

This completes the proof of Theorem 1.3. ∎

The proof of Theorem 1.4 follows the same general outline as the proof of Theorems 1.2 and 1.3. We omit the details, providing instead an outline of the required steps.

Proof of Theorem 1.4. Fix integers a and b such that $b \equiv 15 \pmod{16}$ and $a \equiv \pm 7 \pmod{16}$, and let $\{u_i\}$ be the two-term recurrence sequence defined by $u_0 = 0$, $u_1 = 1$ and for all $i \ge 2$, $u_i = au_{i-1} + bu_{i-2}$. As in the proof of Theorem 1.2, we break the proof into five easy pieces.

Step 1. *For all* $k \ge 3$, *if* $r \equiv \pm 1 \pmod 8$, *then* $\nu_{a,b}(2^k, r) \ge 1$.

Step 2. *If* $4 \le k \le t$, *then* $\nu(2^k, 0) \ge 2^{k-3}$.

Step 3. *If* $k \ge t$ *and* $r \equiv 0 \pmod{2^t}$, *then* $\nu(2^k, r) \ge 2^{t-3}$.

Step 4. *If* $4 \le k \le t$, *then* (1.5) *holds.*

Step 5. *If* $k \ge t$, *then* (1.6) *holds.*

These five steps complete the proof of Theorem 1.4. ∎

References

[1] W. Carlip and E. Jacobson, *Stability of two-term recurrence sequences modulo* 2^k, Fibonacci Quart., to appear.
[2] R. D. Carmichael, *On the numerical factors of the arithmetic forms* $\alpha^n \pm \beta^n$, Ann. of Math. (2) 15 (1913), 30–70.
[3] E. T. Jacobson, *Distribution of the Fibonacci numbers* mod 2^k, Fibonacci Quart. 30 (1992), 211–215.
[4] W. Narkiewicz, *Uniform Distribution of Sequences of Integers in Residue Classes*, Lecture Notes in Math. 1087, Springer, New York, 1984.
[5] J. Pihko, *A note on a theorem of Schinzel*, Fibonacci Quart. 29 (1991), 333–338.
[6] A. Schinzel, *Special Lucas sequences*, *including the Fibonacci sequence*, *modulo a prime*, in: A Tribute to Paul Erdős, A. Baker, B. Bollobás, and A. Hajnal (eds.), Cambridge University Press, 1990, 349–357.
[7] L. Somer, *Distribution of residues of certain second-order linear recurrences modulo p*, in: Applications of Fibonacci Numbers, A. N. Philippou, A. F. Horadam, and G. E. Bergum (eds.), Kluwer, 1988, 311–324.
[8] —, *Distribution of residues of certain second-order linear recurrences modulo p–II*, Fibonacci Quart. 29 (1991), 72–78.

Department of Mathematics
Ohio University
Athens, Ohio 45701
U.S.A.
E-mail: carlip@oucsace.cs.ohiou.edu
jacobson@oucsace.cs.ohiou.edu

Received on 27.3.1995
and in revised form on 1.8.1995 (2765)