TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 178, April 1973

MULTIPLICITIES OF SECOND ORDER LINEAR RECURRENCES

BY

RONALD ALTER AND K. K. KUBOTA

ABSTRACT. A second order linear recurrence is a sequence $\{a_n\}$ of integers satisfying $a_{n+2} = Ma_{n+1} - Na_n$ where N and M are fixed integers and at least one a_n is nonzero. If k is an integer, then the number $m(k)$ of solutions of $a_n = k$ is at most 3 (respectively 4) if $M^2 - 4N < 0$ and there is an odd prime $q \neq 3$ (respectively $q = 3$) such that $q | M$ and $q \nmid kN$. Further $M = \sup_{k \text{ integer}} m(k)$ is either infinite or ≤ 5 provided that either (i) $(M, N) = 1$ or (ii) $6 \nmid N$.

I. Introduction.

A sequence of rational integers $\{a_n\}$ satisfying a relation of the form

$$a_{n+2} = Ma_{n+1} - Na_n, \qquad n \geq 0, \tag{1}$$

where M and N are rational integers is called a second order linear recurrence. Such a sequence is clearly determined by (1) and the initial values $a_0 = d$ and $a_1 = e$. The case $d = e = 0$ is trivial, so it will be assumed throughout that not both d and e are 0. Associated with the recurrence is the discriminant $A = 4N - M^2$ and the companion equation $x^2 - Mx + N = 0$.

Given an integer k, its multiplicity $m(k)$ with respect to the sequence $\{a_n\}$ is the number of solutions of $a_n = k$. The multiplicity of the sequence is the least upper bound of the $m(k)$, as k ranges over the rational integers. It is a well-known conjecture that the multiplicity of any second order linear recurrence is either infinite or bounded above by 5. (For references to this conjecture see Ward [10], Lewis [6, p. 66], Chowla, Dunton, and Lewis [4], and Laxton [5].) Some work has been done on this conjecture. Chowla, Dunton, and Lewis [4] prove that if $A \leq 0$, then either the multiplicity of the sequence is infinite or it is bounded above by 3. Further, they show that if $(M, N) = (d, e) = 1$, and if the ratio of the roots of the companion equation is not a root of unity, then the sequence is of finite multiplicity. If, in addition, $A > 0$ and for some prime p one has $p \nmid M/2$ and $p^t \| A$ where $t \geq 1$ for $p \geq 5$ ($t \geq 2$ for $p = 3$, $t \geq 3$ for $p = 2$), then the multiplicity of the sequence is less than p^t.

Received by the editors April 3, 1972.

AMS (MOS) subject classifications (1970). Primary 10A35, 10B40.

Key words and phrases. Linear recurrence, p-adic numbers, prime number, multiplicity, p-adic power series, companion equation.

Laxton [5] proves that if the roots and ratio of roots of the companion equation are not roots of unity, then the multiplicity of the sequence is at most

$$L = \operatorname*{Min}_{p \nmid N,\ p \text{ prime}} L_p \quad \text{where } L_p = \begin{cases} 8 & \text{if } p = 2 \\ 10 & \text{if } p = 3, \\ p^2 & \text{if } p \neq 2, 3. \end{cases}$$

The precise multiplicity of several recurrences has been determined. In particular, Skolem, Chowla and Lewis [8] prove that if $a_0 = a_1 = M = 1$ and $N = 2$ the sequence has multiplicity 3 and -1 occurs exactly three times. P. Chowla, S. Chowla, Dunton and Lewis [3] prove that if $M = 1$, $a_0 = 1$, $a_1 = 1 - 2N$, then $m(1) = 1$ (if, $N > 2$) and $m(1) = 2$ (if $N = 2$). Alter and Kubota [1] determine that if $M = 1$, $N = 3$ and $a_0 = 0$, $a_1 = 1$ then the multiplicity of the sequence is 3 with $m(1) = 3$ and $m(k) \leq 1$ for all $k \neq 1$.

In the present paper it is established that the conjecture is valid for a much larger class of sequences than those previously considered. The main results are the following three theorems.

Theorem 1. *If* $(M, N) = 1$ *then the multiplicity of the recurrence* (1) *is either infinite or bounded above by* 5.

Theorem 2. *If* $6 \nmid N$, *then the multiplicity of the recurrence* (1) *is either infinite or bounded above by* 5.

Theorem 3. *Suppose* (1) *holds with* $A > 0$. *If* q *is an odd prime divisor of* M *such that* $q \nmid Nd$, *then* $m(d) \leq 3$ *when* $q \neq 3$ *and* $m(d) \leq 4$ *if* $q = 3$.

The proofs of the theorems use Skolem's p-adic method, Strassman's lemma (for a statement and proof see Lewis [6, p. 54]) and the above mentioned theorems of Chowla, Dunton, and Lewis and of Laxton. In the next section some preliminary results on linear recurrences of order two are obtained. §3 contains lemmas concerning some special sequences. §4 contains the proofs of the theorems, and in §5 there are some special results and concluding remarks, including two conjectures.

II. **Preliminaries.** In this section some basic results on linear recurrences of order two are established. Some of the well-known results will only be stated. Recalling the definition of the discriminant A of (1), the two-dimensional vector space over the rational numbers Q can be made into a commutative Q-algebra via the multiplication

$$(r, s)(t, u) = (rt - suA, st + ru). \tag{2}$$

If $A = +1$ this is just $Q(\sqrt{-1})$. Define the multiplicative functions $\overline{(r, s)} = (r, -s)$ and $N(r, s) = r^2 + s^2 A = (r, s)\overline{(r, s)}$ and note the identity

$$(r, s)(t/2, u/2)^2 = t(r, s)(t/2, u/2) - [(t^2 + u^2A)/2](r, s). \tag{3}$$

Let $c = 2e - dM$ and define the sequences $\{a_n\}$ and $\{d_n\}$ by

$$(d_n, a_n) = (c, d)(M/2, 1/2)^n. \tag{4}$$

It is easy to verify by induction and (3) that the sequences $\{a_n\}$ and $\{d_n\}$ satisfy (1) with $a_0 = d$, $a_1 = e$, $d_0 = c$ and $d_1 = (cM - Ad)/2$. In particular, the sequences $\{b_n\}$ and $\{c_n\}$ which satisfy (1) with $b_0 = 0$, $b_1 = 1$, $c_0 = 2$, $c_1 = M$ also satisfy

$$(c_n, d_n) = (2, 0)(M/2, 1/2)^n. \tag{5}$$

The sequence $\{b_n\}$ is the Lucas sequence which is associated with the linear recurrence (1). From (3) and the fact that

$$(c_k^2 + b_k^2A)/4 = N(c_k/2, b_k/2) = (N(M/2, 1/2))^k = N^k,$$

it follows that the sequence $\{e_n\}$ defined by $e_n = a_{kn+i}$ $(i \geq 0,\ k > 0)$ satisfies

$$e_{n+2} = c_k e_{n+1} - N^k e_n. \tag{6}$$

If $A > 0$ the ring defined above is just $Q(\sqrt{-A})$. Let $f = \sqrt{-A}$; it follows by (4) that

$$a_n = \frac{1}{2f}\left\{(c + df)\left(\frac{M+f}{2}\right)^n - (c - df)\left(\frac{M-f}{2}\right)^n\right\}. \tag{7}$$

Expanding by the binomial theorem yields

$$a_n\left(\frac{-4}{A}\right)^{(n-1)/2} = \frac{1}{2}\sum_{j=0}^{\infty}\left\{c\binom{n}{2j} + dM\binom{n}{2j+1}\right\}\left(\frac{-M^2}{A}\right)^j, \tag{8}$$

n odd, and

$$a_n\left(\frac{-4}{A}\right)^{n/2} = \sum_{j=0}^{\infty}\left\{d\binom{n}{2j} + \frac{cM}{(-A)}\binom{n}{2j+1}\right\}\left(\frac{-M^2}{A}\right)^j, \tag{9}$$

n even.

The following result of M. Ward [9, Theorem 3] will be useful.

Proposition (Ward). *Let M and N be integers such that the ratio of the roots of $x^2 - Mx + N = 0$ is a primitive kth root of unity. Then M, N, k and the sequence* (1) *satisfy one of the following conditions*:

(i) $M = 2t$, $N = t^2$, $k = 1$, *and* $a_n = (e - d)^n + d$,

(ii) $M = 0$, $N \neq 0$, $k = 2$, *and* $a_n = t^q a_r$,

(iii) $M = t$, $N = t^2$, $k = 3$, *and* $a_n = (-1)^q t^{n-r} a_r$,

(iv) $M = 2t$, $N = 2t^2$, $k = 4$, *and* $a_n = (-1)^q t^{n-r} a_r$,

(v) $M = 3t$, $N = 3t^2$, $k = 6$, *and* $a_n = (-1)^q t^{n-r} a_r$

where t is an integer and q, r satisfy $n = qk + r$, $0 \leq r < k$.

III. **Lemmas.** This section is devoted to the proofs of several lemmas about special linear recurrences. These lemmas as well as Theorem 3 will be used in the proofs of Theorems 1 and 2. Anyone willing to accept the statements of these lemmas can pass directly to the next section.

Lemma 1. *Let $\{c_n\}$ (respectively $\{c'_n\}$) be the sequence $\{c_n\}$ defined in* §II *with $M = 1$ (respectively $M = -1$). If $N \neq 0, 1$, then the equation $c_n = -1$ has no solutions; $c_n = 1$ has no solution $n \neq 1$ except when $N = 2$ and $n = 4$; $c'_n = -1$ has only the solution $n = 1$; and the equation $c'_n = 1$ has only the solution $N = 2$, $n = 4$.*

Proof. The results about $\{c_n\}$ are proven by P. Chowla, S. Chowla, Dunton and Lewis [3]. The results about $\{c'_n\}$ follow immediately from those for c_n since $c'_n = (-1)^n c_n$.

Lemma 2. *Let A_1 (respectively A_2) be the sequence $\{a_n\}$ of* (1), *where $(d, e) = 1$, $N = 2$ and $M = 1$ (respectively $M = -1$). Then A_1 (respectively A_2) has multiplicity ≤ 3 (respectively ≤ 4).*

Proof. It is routine to verify using (8), (9) that if $c = 2e - d$, then A_1 is given by

$$a_n = \frac{1}{2^n} \sum_{j=0}^{\infty} \left\{ d \binom{n}{2j} + c \binom{n}{2j+1} \right\} (-7)^j. \tag{10}$$

Hence $(d, c) = 1$. For $0 \leq i \leq 2$, (10) can be rewritten as

$$\begin{aligned} a_{3t+i} &= (1/2^i)(1+7)^t \left\{ d + c(3t+i) - d\binom{3t+i}{2} 7 - c \binom{3t+i}{3} 7 + 7^2 C(t) \right\} \\ &= (1/2^i) \left\{ d + c(3t+i) - d \binom{3t+i}{2} 7 + 7dt + 7c(3t+i)t + 7^2 D(t) \right\}, \end{aligned} \tag{11}$$

where $C(t)$ and $D(t)$ are 7-adic power series in t.

Consider the equation $a_n = k$, where $k \not\equiv 0 \pmod 7$. If $7 \nmid c$, (11) modulo 7 yields a linear polynomial. By Strassman's lemma [6, p. 54] there is at most one 7-adic solution for each $i = 0, 1, 2$. If $7 | c$, then $7 \nmid d$ and (11) modulo 49 gives the nontrivial quadratic term, $-d(3t^2)/2$. By Strassman's lemma there are at most two solutions of $a_n = k$ in each congruence class modulo 3. (11) modulo 7 gives $k \equiv (1/2^i)d \pmod 7$ and so all solutions lie in the same congruence class modulo 3. Hence if $k \not\equiv 0 \pmod 7$, then $m(k) \leq 3$.

On the other hand, if $7 | k$ then $a_n = k$, (11), and the fact that $(c, d) = 1$ imply that $7 \nmid c$. Applying Strassman's lemma to (11) yields that there is at most one solution of $a_n = k$ in each congruence class modulo 3. This completes the proof of the lemma for the sequence A_1.

To complete the proof of the lemma it suffices to show that whenever $(d, e) = 1$, A_2 has the property that $m(d) \leq 4$. If $2|de$, an induction argument using (1) shows that $a_{n+2} \equiv a_{n+1} \equiv e \pmod 2$, and it follows that $m(d) = 1$. Suppose $2 \nmid de$ and examine each of the possibilities for d and e modulo 8. It can be seen that the solutions of $a_n = d$ lie in at most four different congruence classes modulo 6. The proof is completed by an argument similar to the first part of the lemma. Clearly A_2 can be shown to satisfy

$$(12) \qquad a_n = -\left(\frac{-1}{2}\right)^n \sum_{i=0}^{\infty} \left\{ c\binom{n}{2i+1} - d\binom{n}{2i} \right\} (-7)^i.$$

If $7 \nmid c$, by applying Strassman's lemma to each sequence $\{a_{6t+i}\}$ $(i = 0, 1, \cdots, 5)$ of A_2, one can see that there is at most one solution in each congruence class modulo 6. So, $m(d) \leq 4$. If $7|c$ and so $7 \nmid d$, (12) modulo 7 gives $d \equiv -(-1/2)^n(-d) \pmod 7$ and it follows that all solutions of $a_n = d$ lie in a single congruence class modulo 6. As in the proof for the sequence A_1, one can reduce (12) modulo 49 and apply Strassman's lemma to conclude that $m(d) \leq 2$.

Lemma 3. *Let* $(d, e) = 1$, $N \neq \pm 1$ *and* $a_0 = d$, $a_1 = Me$ *in* (1). *If* $M = 1$ (*respectively* $M = -1$ *and* $N \neq \pm 2$) *then the solutions of* $a_n = d$ *with* $n > 0$ *all lie in the same congruence class modulo* N (*respectively, are all of the same parity*).

Proof. If $M = 1$ it is easy to verify that for $n \geq 2$,

$$(13) \qquad a_n \equiv e - (d + (n-2)e)N \pmod{N^2}.$$

If $d = e = \pm 1$, then $a_n = d$ implies $d \equiv e - (d + (n-2)e)N \equiv d - (n-1)dN \pmod{N^2}$. So $n \equiv 1 \pmod N$ as desired. If $d \neq e$, and $a_n = a_m = d$ for $n \geq 2$, then (13) gives

$$e - (d + (n-2)e)N \equiv e - (d + (m-2)e)N \pmod{N^2}.$$

So $(n - m)e \equiv 0 \pmod N$. If further $(e, N) = 1$, then $n \equiv m \pmod N$ as desired. If $(e, N) \neq 1$, let q be a prime factor of (e, N). By the definition of the sequence, $a_{n+2} \equiv a_{n+1} \pmod q$ and so by induction $a_n \equiv a_1 = e \equiv 0 \pmod q$. Since $q \nmid d$, there are no nonzero solutions of $a_n = d$. Hence the first assertion is established.

Suppose $M = -1$. It can be shown by induction that $a_n \equiv (-1)^n e \pmod N$ for $n \geq 1$. If $a_{2r} = a_{2s+1} = d$, then $d \equiv e \equiv -e \pmod N$. So $2d \equiv 0 \pmod N$ and $2e \equiv 0 \pmod N$. Since $(d, e) = 1$, $N|2$ and this completes the proof of the lemma.

The following result is implicit in a proof of Laxton [5]. Let $\{a_n\}$ be a recurrence satisfying (1) such that neither of the roots r_1, r_2 of the companion equation nor their ratio r_1/r_2 is a root of unity. Suppose q is the smallest positive even integer such that $r_1^q \equiv r_2^q \equiv 1 \pmod 4$. If the r_i are 2-adic integers, the multiplicity of $\{a_n\}$ is at most 4. If the r_i are not 2-adic integers, then for every integer k, the equation $a_n = k$ has at most two solutions in each congruence class modulo q. Further, if two distinct congruence classes $u \pmod q$ and $v \pmod q$ contain two solutions each, then $u - v \equiv q/2 \pmod q$. In the proofs of Lemmas 4 and 5, this result will be referred to as Laxton's theorem.

Lemma 4. *Given the recurrence*

$$a_{n+2} = 2Ma_{n+1} - Na_n, \qquad a_0 = d, a_1 = e \tag{14}$$

where $(d, e) = 1$, $2 \nmid Nd$, $M \neq 0$ *and* $M^2 - 4N < 0$. *If* M *is odd, then* $m(d) \leq 3$ (*respectively* $m(d) \leq 4$), *whenever* $N \equiv 3 \pmod 4$ (*respectively* $N \equiv 1 \pmod 4$). *If* M *is even, then* $m(d) \leq 3$ (*respectively* $m(d) \leq 4$) *if* $N \equiv 1 \pmod 4$ (*respectively* $N \equiv 3 \pmod 4$).

Proof. This is an application of Laxton's theorem. By the proposition of §2, if r_1 and r_2 are the roots of $x^2 - Mx + N = 0$, then r_1/r_2 is not a root of unity. Also it can be shown that if at least one of the r_i is a root of unity, then it is ± 1 and $M^2 - 4N \geq 0$, which is a contradiction. Thus Laxton's theorem is applicable.

The roots of the companion equation are $r_i = M \pm (M^2 - 4N)^{1/2}$; thus

$$r_i^2 = 2M^2 - N \pm 2M(M^2 - N)^{1/2}. \tag{15}$$

If M is odd, then $r_i^2 \equiv 1 + (1 - N \pm 2M(M^2 - N)^{1/2}) \pmod 4$. Hence if $N \equiv 1 \pmod 4$, the integer q in the statement of Laxton's theorem is 2; and so the multiplicity of $\{a_n\}$ is at most 4. If $N \equiv 3 \pmod 4$, then $M^2 - N \equiv 2 \pmod 4$ and so $r_i^2 \not\equiv 1 \pmod 4$. Since $r_i^4 \equiv 1 \pmod 4$ in this case, $q = 4$. By (14) the $\{a_n\}$ are $d, e, 2 + d, 2 + e, d, e, 2 + d, 2 + e, \cdots \pmod 4$. Hence by Laxton's theorem the multiplicity is at most 3.

Suppose M is even. If $N \equiv 3 \pmod 4$, (15) shows that $r_i^2 \equiv 1 \pmod 4$ and so $q = 2$. By Laxton's theorem, the multiplicity is at most 4. If $N \equiv 1 \pmod 4$, then (15) shows that $q = 4$. The sequence $\{a_n\}$ looks like $d, e, 3d, 3e, d, e, 3d, 3e, \cdots \pmod 4$. Hence by Laxton's theorem the multiplicity is at most 3, and the proof is complete.

Lemma 5. *If* $(d, e) = 1$, $2 \nmid MN$ *and neither of the roots nor the ratio of the roots of the companion equation are roots of unity, then the sequence* $\{a_n\}$ *of* (1) *has multiplicity* ≤ 5.

Proof. This is an application of Laxton's theorem. It is straightforward to verify that the roots r_i of the companion equation satisfy $r_i^6 \equiv 1 \pmod 4$. Hence the q in the statement of Laxton's theorem is either 2 or 6. By that theorem, it suffices to consider the case where $q = 6$. Examining the sequence $\{a_n\}$ modulo 4 for the various cases of M, N odd and not both congruent to 3 modulo 4, one can verify that for any d, $a_n = d$ has solutions lying in at most three congruence classes modulo 6. The same can be verified for $M \equiv N \equiv 3 \pmod 4$ by considering the sequence modulo 8. Hence the result follows from Laxton's theorem.

For the proof of Theorem 2, it will be necessary to know something about companion equations. The necessary facts are summarized in the following lemma.

Lemma 6. *Let M and N be integers.*

(i) *If $x^2 - Mx + N = 0$ has a root which is a root of unity, then either $M = \pm 1$, $N = 1$, or $M = 0$, $N = 1$, or $N = \pm M - 1$.*

(ii) *If $x^2 - (M^2 - 2N)x + N^2 = 0$ has a root which is a root of unity, then so does $x^2 - Mx + N = 0$.*

(iii) *If $x^2 - (M^2 - 2N)x + N^2 = 0$ has as a root of unity the ratio of its roots, then so does $x^2 - Mx + N = 0$.*

Proof. The proofs of parts (ii) and (iii) are straightforward using part (i) and the proposition of §II. To prove part (i), let r be such a root and suppose r is a primitive nth root of unity. Its degree over the rationals is at most 2 and is exactly $\phi(n)$, where ϕ is the Euler totient function. Since $\phi(n) \leq 2$ can only occur if $n = 1, 2, 3, 4$, or 6 and since these give rise to the five stated cases, the proof is complete.

The proof of Theorem 2 will require the following result which is implicit in a proof of Laxton [5]. Let $\{a_n\}$ be a recurrence satisfying (1) such that $(d, e) = 1$ and neither of the roots r_1, r_2 of the companion equation nor their ratio r_1/r_2 is a root of unity. For p an odd prime, let q be the smallest positive integer such that $r_1^q \equiv r_2^q \equiv 1 \pmod p$.

(i) If the r_i are p-adic integers, then the multiplicity of the sequence $\{a_n\}$ is at most $2(p-1)$ (respectively 6) if $p \neq 3$ (respectively $p = 3$).

(ii) If the r_i are not p-adic integers and k is any integer, then with the possible exception of one congruence class modulo q, none can contain more than one solution of $a_n = k$. The exceptional class contains at most 2 (respectively 3) solutions if $p \neq 3$ (respectively $p = 3$).

In the proof of Theorem 2, this result will be referred to as Laxton's theorem.

IV. **Proofs of theorems.** This section is devoted to the proof of Theorems 1, 2, and 3 which have already been stated in the Introduction. Since Theorem 3 is used to prove Theorems 1 and 2, it will be proven first. The proof of Theorem 3 combines and uses some of the ideas of Apéry [2] and Laxton [5]. The lemmas of §III are used only in the proofs of Theorems 1 and 2; in particular, Lemmas

1, 2 and 3 are used in proving Theorem 1 while Lemmas 4, 5 and 6 as well as Laxton's Theorem are used to prove Theorem 2.

Proof of Theorem 3. Since Theorem 3 refers only to multiplicity, it can be assumed without loss of generality that $(d, e) = 1$. Since $q \nmid A$, there is a smallest positive integer s for which

$$(16) \qquad (-4/A)^s = 1 + \gamma q^{\alpha}$$

is solvable with $\alpha \geq 1$ and γ a q-adic unit. If n is an odd integer such that $a_n = d$, then reducing (8) modulo q shows that c is not a multiple of q, and that n is of the form $(n-1)/2 = ts + i$ where t and i are integers satisfying $0 \leq i \leq s-1$, and also shows that $d(-4/A)^i = 1/2\, c + \delta q^{\beta}$ for some q-adic unit δ and some $\beta \geq 1$. Substituting these into (8) and expanding into q-adic power series gives

$$(17) \qquad \begin{aligned} &(c/2 + \delta q^{\beta})(1 + \gamma q^{\alpha} t + \gamma^2 q^{2\alpha}(t^2 - t)/2 + \gamma^3 q^{3\alpha}(t^3 - 3t^2 + 2t)/6 + \cdots) \\ &\quad = c/2 + dM(2st + 2i + 1)/2 - (2st + 2i + 1)(st + i)M^2 c/2A \\ &\qquad - (2st + 2i + 1)(st + i)(2st + 2i - 1)M^3 d/6A + \cdots. \end{aligned}$$

The left-hand member of this last equation expands as:

$$(18) \qquad \begin{aligned} &\frac{c}{2} + \delta q^{\beta} + \frac{c\gamma q^{\alpha} t}{2} + \delta\gamma q^{\alpha+\beta} t + \frac{c\gamma^2 q^{2\alpha}(t^2 - t)}{4} \\ &\quad + \frac{\delta\gamma^2 q^{2\alpha+\beta}(t^2 - t)}{2} + \frac{c\gamma^3 q^{3\alpha}(t^3 - 3t + 2t)}{12} + \cdots. \end{aligned}$$

By Strassman's lemma, if (17) has at least three (respectively four) solutions with $q \neq 3$ (respectively $q = 3$), then the terms of lowest q-adic valuation are neither linear nor quadratic. Now the coefficient of t in (18) is $c\gamma q^{\alpha} \pmod{q^{\alpha+1}}$, and that of t^2 in (18) is $c\gamma^2 q^{2\alpha} \pmod{q^{2\alpha+1}}$. Further, the right-hand side of (17) has the coefficient of t congruent to $M(2s)/2 \pmod{q^{V+1}}$ and the coefficient of t^2 congruent to $-Mc\, 2s^2/2A \pmod{q^{2V+1}}$ where $V = v_q(M)$, the q-adic valuation of M. Now the coefficients of t^k for $k \geq 3$ ($k \geq 4$ if $q = 3$) in (17) are congruent to 0 modulo $q^{2\eta+1}$ where $\eta = \min(\alpha, V)$. It follows by Strassman's lemma (Lewis [5, p. 54]) that:

$$(19) \qquad c\gamma q^{\alpha}/2 \equiv dM2s/2 \pmod{q^{\eta+1}},$$

$$(20) \qquad c\gamma^2 q^{2\alpha}/4 \equiv -M^2 c2s^2/2A \pmod{q^{2\eta+1}}.$$

Now since none of 2, c, s, and A are multiples of q, it follows from these congruences that $\alpha = v_q(M\, d)$ and $2\alpha = v_q(M^2)$. Hence $q \nmid d$ and $\alpha = v_q(M) = \eta$. Therefore these congruences can be rewritten as

$$(-4/A)(M/q^{\alpha})^2 s^2 \equiv y^2 \pmod{q}, \qquad (2d/c)(M/q^{\alpha})s \equiv y \pmod{q}.$$

Squaring the second congruence and equating it to the first gives $c^2 + d^2A \equiv 0 \pmod{q}$. It has been shown that the only way that there can be three (four if $q = 3$) or more odd solutions of $a_n = d$ is if $c^2 + d^2A \equiv 0 \pmod{q}$.

A similar argument can be applied to the even solutions of $a_n = d$. One reduces (9) modulo q to see that $q \nmid d$ and $n/2 = st$ for some integer t. (9) becomes

$$d(1 + yq^{\alpha}t + y^2q^{2\alpha}(t^2 - t)/2 + \cdots) = d + cM2ts/(-A) + st(2st - 1)dM^2/(-A) + \cdots.$$

As in the case of odd solutions, the only way for there to be at least three (four if $q = 3$) even solutions of $a_n = d$ is if

(21) $$dyq^{\alpha} \equiv 2cMs/(-A) \pmod{q^{\alpha+1}},$$

(22) $$dy^2q^{2\alpha}/2 \equiv 2dM^2s^2/(-A) \pmod{q^{2\alpha+1}}$$

and $q \nmid c$, $v_q(M) = \alpha$. Solving the congruences gives $c^2 + d^2 A \equiv 0 \pmod{q}$.

Suppose that there are at least two odd and at least two even solutions of $a_n = d$. Then reducing (8) and (9) modulo q implies that $q \nmid c, d$. As in the earlier arguments, Strassman's lemma can be applied and one gets the congruences (19) and (21). Solving these gives $c^2 + d^2 A \equiv 0 \pmod{q}$. It is easy to verify by the definitions of c and A, that this is equivalent to $e^2 + d^2 N \equiv 0 \pmod{q}$. Thus if $e^2 + d^2 N \not\equiv 0 \pmod{q}$, then the multiplicity of d in the sequence of a_n's is at most three (4 if $q = 3$).

Now suppose that $c^2 + d^2 A \equiv 0 \pmod{q}$. Since $q \nmid d$, $(-A/q) = 1$ (Legendre symbol) and so $f = (-A)^{1/2}$ is a q-adic integer. Also $q \nmid c$. Since $q | M$, it follows that

$$((M \pm f)/2)^{2s} \equiv (-A/4)^s \equiv 1 \pmod{q}.$$

First consider the even solutions of $a_n = d$. These are of the form $n/2 = st$ with t an integer, and so (7) shows that

$$2fd = (c + df)((M + f)/2)^{2st} - (c - df)((M - f)/2)^{2st}.$$

It follows that

$$\frac{2fd}{((M - f)/2)^{2st}} = (c + df)\left(\frac{M + f}{M - f}\right)^{2st} - (c - df).$$

Expanding this into p-adic power series gives

(23) $$2fd \sum_{j=1}^{\infty} \left(\log\left(\frac{M - f}{2}\right)^{-2s}\right)^{j} \frac{t^j}{j!} = (c + df) \sum_{j=1}^{\infty} \left(\log\left(\frac{M + f}{M - f}\right)^{2s}\right)^{j} \frac{t^j}{j!}.$$

Define

$$R = \min\left(v_q\left(2fd \log\left(\frac{M-f}{2}\right)^{-2s}\right), v_q\left((c+df)\log\left(\frac{M+f}{M-f}\right)^{2s}\right)\right)$$

and

$$T = \min\left(v_q\left(\log\left(\frac{M-f}{2}\right)^{-2s}\right), v_q\left(\log\left(\frac{M+f}{M-f}\right)^{2s}\right)\right) > 0.$$

All terms in (23) have coefficients of greater q-adic valuation than $R + T$ except possibly those corresponding to $j = 1, 2, 3$. Those corresponding to $j = 2, 3$ have q-adic valuation at least $R + T$, and those corresponding to $j = 3$ have q-adic valuation greater than $R + T$ unless $q = 3$. If there are at least three (four if $q = 3$) even solutions of $a_n = d$, then Strassman's lemma implies that the term of lowest q-adic valuation is neither linear nor quadratic (nor cubic if $q = 3$), and so

$$(24)\qquad 2fd \log\left(\frac{M-f}{2}\right)^{-2s} - (c+df)\log\left(\frac{M+f}{M-f}\right)^{2s} \equiv 0 \pmod{q^{R+1}},$$

$$(25)\qquad \frac{2fd}{2}\left(\log\left(\frac{M-f}{2}\right)^{-2s}\right)^2 - \frac{(c+df)}{2}\left(\log\left(\frac{M+f}{M-f}\right)^{2s}\right)^2 \equiv 0 \pmod{q^{R+T+1}}.$$

Dividing (24), (25) by q^R and q^{R+T} respectively and solving modulo q gives

$$\frac{1}{q^T}\left(\log\left(\frac{M+f}{M-f}\right)^{2s} - \log\left(\frac{M-f}{2}\right)^{-2s}\right) \equiv 0 \pmod{q}.$$

Thus, $\log((M+f)/2)^{2s} \equiv 0 \pmod{q^{T+1}}$.

The argument of the last paragraph can be repeated by dividing by $((M-f)/2)^{2st}$ instead of $((M+f)/2)^{2st}$. One gets that $\log((M-f)/2)^{2s} \equiv 0 \pmod{q^{U+1}}$ where U is defined by

$$U = \min\left(v_q\left(\log\left(\frac{M+f}{2}\right)^{-2s}\right), v_q\left(\log\left(\frac{M-f}{M+f}\right)^{2s}\right)\right).$$

This together with $\log((M+f)/2)^{2s} \equiv 0 \pmod{q^{T+1}}$ contradicts the definition of T. It follows that there are at most two (three if $q = 3$) even solutions of $a_n = d$.

As for odd solutions of $a_n = d$, these are all of the form $(n-1)/2 = st + i$ and an argument analogous to the above can be carried out. One obtains that there are at most two even solutions if $q \neq 3$ and at most three solutions if $q = 3$. Suppose now that there is more than one odd and more than one even solution of $a_n = d$. Comparing coefficients in (23), Strassman's lemma shows that

$$2fd \log\left(\frac{M-f}{2}\right)^{-2s} - (c+df)\log\left(\frac{M+f}{M-f}\right)^{2s} \equiv 0 \pmod{q^{R+T}}.$$

The analogous congruence for odd solutions is

$$2fd \log\left(\frac{M-f}{2}\right)^{-2s} - \left(\frac{M+f}{2}\right)^{2i+1}(c+df)\log\left(\frac{M+f}{M-f}\right)^{2s} \equiv 0 \pmod{q^{R+T}}.$$

Dividing these last two congruences by q^R and subtracting gives

$$\left[\frac{(c+df)}{q^R}\log\left(\frac{M+f}{M-f}\right)^{2s}\right]\left[\left(\frac{M+f}{2}\right)^{2i+1}-1\right] \equiv 0 \pmod{q^T}.$$

Since the left factor is a q-adic unit, it follows that

$$((M+f),2)^{2i+1} \equiv 1 \pmod{q^T}. \tag{26}$$

On the other hand, using the corresponding equations obtained by dividing (7) by $((M+f)/2)^{2st}$ instead of $((M-f)/2)^{2st}$ yields

$$((M-f)/2)^{2i+1} \equiv 1 \pmod{q^T}. \tag{27}$$

Since $q|M$, (26) and (27) imply $(f/2)^{2i+1} \equiv 1 \equiv (-f/2)^{2i+1} \pmod{q}$. But then $2(f/2)^{2i+1} \equiv 0 \pmod{q}$ which contradicts the fact that $q \nmid f = (-A)^{1/2}$ and that q is odd. Combining results now shows that there are at most three solutions (respectively four solutions) of $a_n = d$ if $q \neq 3$ (respectively $q = 3$). Thus the proof of Theorem 3 is complete.

Proof of Theorem 1. It clearly suffices to show that $m(d)$ in the sequence $\{a_n\}$ of (1) is either infinite or bounded above by 5 when $(d, e) = 1$. Further, by the results of Chowla, Dunton, and Lewis [4, Theorems 2 and 4], it suffices to consider the case where $d \neq 0$ and $M^2 - 4N < 0$. By Lemma 4, it is only necessary to prove the theorem for M odd. If q is a prime divisor of M which does not divide d, then Theorem 1 follows from Theorem 3. Suppose q is a prime divisor of M and $q|d$, then $q \nmid c = 2e - dM$. By reducing (8) modulo q it follows that $a_n = d$ is impossible for n odd. Hence the multiplicity of d in $\{a_n\}$ is the same as the multiplicity of d in $\{a_{2n}\}$. By (6) of §II, the sequence $\{a_{2n}\}$ satisfies (1) with companion equation $x^2 - (M^2 - 2N)x + N^2 = 0$. Hence this process can be continued with a prime factor of $M^2 - 2N$. If $a_n = d$ has a nonzero solution, then either this process ends after a finite number of steps or else a recurrence of the form $a_{n+2} = \pm a_{n+1} - Na_n$ is obtained. Since $M^2 - 4N < 0$, one can assume $N > 0$. If $N = 1$, then the companion equation, $x^2 \pm x + 1 = 0$, has roots which are roots of unity, and the desired conclusion follows by Chowla, Dunton, and Lewis [4, Theorem 4]. If $N = 2$, the desired result follows from Lemma 2. If $N > 2$, Lemma 4 allows one to replace the sequence $\{a_n\}$ with either $\{a_{Nn+i}\}$ or $\{a_{2n+i}\}$, i a fixed integer. Unless $i = 0$, this new sequence has $m(d)$ one less than that of the original sequence. Hence, it remains to show that the new sequence has infinite multiplicity or else it is bounded above by 4. The new sequence may be reduced by the method used in the first paragraph of this proof. But in this case the process must terminate unless the sequences $\{c_n\}$ and $\{c_n'\}$ of Lemma 1 have a second ± 1 term. By Lemma 1 this is impossible and the proof of Theorem 1 is complete.

Proof of Theorem 2. Without loss of generality it can be assumed that $(d, e) = 1$. First consider the case where neither of the roots nor the ratio of the roots of the companion equation is a root of unity.

If $2 \nmid N$ then the result is a corollary of Lemmas 4 and 5. Thus it suffices to assume $3 \nmid N$ and apply Laxton's Theorem with $p = 3$.

Suppose first that the roots of the companion equation are 3-adic integers. Then $M^2 - 4N$ is a 3-adic square. Since $3 \nmid N$, it follows that $3 | M$ and $N \equiv 2 \pmod 3$. It is enough to show that $m(d) \leq 5$. If $3 \nmid d$ this follows by Theorem 3. Thus it suffices to consider this case where $3 | d$ and hence $3 \nmid e$. Since $3 | M$, $a_{n+2} \equiv -Na_n \equiv a_n \pmod 3$, it follows that all solutions of $a_n = d$ are even. The even subsequence $\{a_{2n}\}$ is a recurrence with companion equation $x^2 - (M^2 - 2N)x + N^2 = 0$. By Lemma 6, the roots and ratio of roots of this quadratic are not roots of unity. Further, $M^2 - 2N \not\equiv 0 \pmod 3$ and so the roots are not 3-adic numbers. Hence it suffices to treat the case where the roots of the companion equation are not 3-adic integers.

Suppose the roots of the companion equation are not 3-adic integers. One examines each of the possible values for M and N modulo 3, computes q, and applies Laxton's Theorem. Letting $M(N, M; q)$ be the maximum number of congruence classes modulo q which can contain a solution to $a_n = d$, one finds that $M(1, 0; 4) = 2$ while $M(1, 1; 6) = M(1, 2; 3) = M(2, 1; 8) = M(2, 2; 8) = 3$.

Suppose now that the ratio of the roots of the companion equation is a root of unity. Thus $\{a_n\}$ is given by one of the five cases of the proposition of §II. It is easy to verify the theorem if any of the following conditions hold: (1) case (i), (2) $t = \pm 1$, (3) $a_r = 0$ for some r.

If none of these conditions hold, then the sequence, for $q \geq 0$, $\{|a_{qk+r}|\}$ is increasing for each r. Hence the theorem is true in cases (ii), (iii) and (iv). If case (v) holds, then $6 \nmid N$ implies that t is odd. Since it can be assumed that $(d, e) = 1$, it follows that exactly two of the subsequences $\{a_{kq+r}\}$ $(q \geq 0,\ 0 \leq r \leq 5)$ consist of even integers and the other four consist of odd integers. Hence the theorem is true in this case too. Suppose finally that exactly one of the roots of the companion equation is a root of unity. By Lemma 6 (i) $(M, N) = 1$. Hence the remaining case follows from Theorem 1. This completes the proof of Theorem 2..

Remark. The conclusion of Theorem 2 holds true for all recurrences (1) provided that either one of the roots or the ratio of the roots of the companion equation is a root of unity. In fact, by the proof of Theorem 2, it suffices to verify that $m(d) \leq 5$ in the event that the recurrence (1) is the form: $M = 3t$, $N = 3t^2$, $t \neq 0$, $(d, e) = 1$, d and t even. Since $\{|a_{6q+r}|\}$ is increasing, there is at most one solution of $a_{6q+r} = d$ for fixed r. Further, $d = a_{6q_1+1} = a_{6q_2+2}$ together with the proposition of § II implies

$$d = (-1)^{q_1} t^{6q_1} e = (-1)^{q_2} t^{6q_2+1} (3e - dt).$$

Since e is odd, it follows that $6\ v_q(t) | v_q(d)$ and $6\ v_q(t) | v_q(d/t)$ which gives a contradiction modulo 6.

V. **Remarks.** The technique used in the proof of Theorem 2 can be extended. For example, it can be shown that:

Theorem 2A. *If* $30 \nmid N$, *then the multiplicity of the recurrence* (1) *is either infinite or bounded above by* 8.

Several earlier papers have considered $m(0)$ and also the pattern of the appearance of 0 in recurrences. Chowla, Dunton, and Lewis [4, Theorem 4] prove that if $m(0) \geq 2$, in (1), then 0 appears infinitely often. Sometimes the multiplicity of 0 in a third order linear recurrence can impose a bound on the multiplicity of all integers in some second order recurrence. For third order linear recurrences $m(0)$ has been studied by C. L. Siegel, K. Mahler, M. Ward and several other authors. For references to this work the reader is referred to Ward [10]. The following remarks about $m(0)$, $m(1)$ and $m(p)$ for p prime, in (1) are easy to establish.

Proposition. (i) *If* $|N| > 1$ *and* $a_0 \cdot a_1 \neq 0$, *then either* $m(0) = 0$ *or there exists an* n *such that* $(a_n, a_{n+k}) = |a_n| > 1$ *for all* $k \geq 0$..

(ii) *If* $m(1) > 0$ *in the subsequence* $a_2, a_3, \cdots$, *then* $(M, N) = 1$.

(iii) *If* $m(p) > 0$ *in the subsequence* $a_2, a_3, \cdots$, *then* $(M, N) = 1$ *or* p.

From (iii) above, it follows that if (M, N) is composite and p is a prime, then $m(p) = 0$ in the subsequence $a_2, a_3, \cdots$. Also, if $(M, N) \neq 1$, then at most one prime has a positive multiplicity in the subsequence $a_2, a_3, \cdots$; and if p is that prime, then $(M, N) = p$.. It would be nice to have a characterization of those k (dependent on M, N, d and e) for which $m(k) = 0$, or $m(k) = 1$ or $m(k) > 1$.

Recalling the result of Chowla, Dunton, and Lewis [4] for the case $A \leq 0$ along with Theorem 3 for $A > 0$, one is led to the following conjecture.

Conjecture 1. *The multiplicity of the recurrence* (1) *is either infinite or bounded above by* 4.

Looking at the problem differently one makes the following conjecture.

Conjecture 2. *Given recurrence* (1), *the number of integers* k *for which* $M(k) > 1$ *is finite.*

Conjecture 2 is true for Lehmer numbers (Schinzel [7]) and a special sequence studied by Chowla, Dunton, and Lewis [4, Theorem 8].

REFERENCES

1. R. Alter and K. K. Kubota, *The diophantine equation* $x^2 + 11 = 3^n$, *and a related sequence*, J. Number Theory (to appear).

2. R. Apéry, *Sur une équation diophantienne*, C. R. Acad. Sci. Paris 251 (1960), 1263–1264. MR 22 #10951.

3. P. Chowla, S. Chowla, M. Dunton and D. J. Lewis, *Some diophantine equations in quadratic number fields*, Norske Vid. Selsk. Forh. 31 (1958), 181–183. MR 21 #4132.

4. S. Chowla, M. Dunton and D. J. Lewis, *Linear recurrences of order two*, Pacific J. Math. 11 (1961), 883–845. MR 25 #39.

5. R. R. Laxton, *Linear recurrences of order two*, J. Austral. Math. Soc. 7 (1967), 108–114. MR 34 #7489.

6. D. J. Lewis, *Diophantine equations: p-adic methods*, Studies in Number Theory, Math. Assoc. Amer., distributed by Prentice-Hall, Englewood Cliffs, N. J., 1969, pp. 25–75. MR 39 #2699.

7. A. Schinzel, *The intrinsic divisors of Lehmer numbers in the case of negative discriminant*, Ark. Mat. 4 (1962), 413–416. MR 26 #2999.

8. Th. Skolem, S. Chowla and D. J. Lewis, *The diophantine equation* $2^{n+2} - 7 = x^2$ *and related problems*, Proc. Amer. Math. Soc. 10 (1959), 663–669. MR 22 #25.

9. M. Ward, *Prime divisors of second order recurring sequences*, Duke Math. J. 2 (1936), 472–476.

10. ———, *Some diophantine problems connected with linear recurrences*, Report of the Institute of the Theory of Numbers, University of Colorado, Boulder, 1959, pp. 250–257.

DEPARTMENT OF COMPUTER SCIENCE, UNIVERSITY OF KENTUCKY, LEXINGTON, KENTUCKY 40506

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF KENTUCKY, LEXINGTON, KENTUCKY 40506