ACTA ARITHMETICA
XXXIII (1977)

On a conjecture of Morgan Ward, I

by

K. K. Kubota (Ann Arbor, Mich.)

1. Introduction. A second order linear recurrence is a sequence $a_0, a_1, \ldots$ of rational integers satisfying a relation

$$a_{n+2} = Ma_{n+1} - Na_n, \quad n \geqslant 0, \quad |a_0| + |a_1| \neq 0 \tag{1}$$

where M and N are fixed rational integers.

The problem dealt with in this paper is that of bounding the number $m(d)$ of times a given integer d can occur in a second order linear recurrence. We define the *multiplicity* of the recurrence (1) to be the supremum of the $m(d)$ as d ranges through the integers. It may be that the multiplicity is infinite; for example, the recurrence

$$a_{n+2} = a_{n+1} - a_n, \quad a_0 = 0, \quad a_1 = 1$$

consists of repetitions of the segment

$$0, 1, 1, 0, -1, -1$$

and so $m(0) = m(1) = m(-1) = \infty$.

If we define a recurrence to be *degenerate* when at least one of the roots or the ratio of the roots of the companion equation $x^2 - Mx + N = 0$ is a root of unity, then we see that our example is a degenerate sequence. If a second order linear recurrence is non-degenerate, then it has long been known that $m(d)$ is finite [12].

In the thirties Morgan Ward conjectured that a non-degenerate second order linear recurrence has multiplicity no larger than five. This conjecture is proved in this paper. In addition, it will be shown that in the special case where the recurrence (1) has coefficients satisfying $(M, N) = 1$, the multiplicity is either infinite or bounded above by four. With the same hypothesis, if the recurrence is a Lucas sequence of the first kind (see (2) below) then it will be shown that the multiplicity is either infinite or bounded above by three unless it is the exceptional sequence:

$$U_{n+2} = -U_{n+1} - 2U_n, \quad U_0 = 0, \quad U_1 = 1$$

in which -1 occurs exactly four times and no other integer occurs so often. Finally, an analogue for Lucas sequences of the second kind ((3) below) will be stated without proof.

These results will be proved by Skolem's p-adic method. After recalling earlier results and establishing some preliminary lemmas in Section 2, the p-adic argument will be given in Section 3. This argument is essentially the same as that given by R. Laxton [7] and D. J. Lewis [10]. Also in Section 3, an idea used by R. Apéry [2] is employed to show how the p-adic method applies to prime divisors p of the terms of the Lucas sequence $\{U_n\}$. This is a generalization of Theorem 1 of [1]. In Section 4, the case when $(M, N) = 1$ is treated, and the proof of Ward's conjecture is completed in Section 5.

The author wishes to thank Professor D. J. Lewis through whom he originally learned of the conjecture and without whose encouragement, this paper never would have been written.

2. Formulae, earlier results, and preliminary lemmas. The first systematic investigation of linear recurrences was done by E. Lucas in volume one of the American Journal in 1878. He was interested in *Lucas sequences of the first kind*

$$U_{n+2} = MU_{n+1} - NU_n, \quad U_0 = 0, \quad U_1 = 1 \tag{2}$$

and of the *second kind*

$$V_{n+2} = MV_{n+1} - NV_n, \quad V_0 = 2, \quad V_1 = M. \tag{3}$$

These sequences are often expressed in the form

$$U_n = \frac{\beta_1^n - \beta_2^n}{\beta_1 - \beta_2}, \quad V_n = \beta_1^n + \beta_2^n \tag{4}$$

where β_1 and β_2 are the roots of the *companion polynomial*

$$x^2 - Mx + N = 0. \tag{5}$$

To obtain a formula for the recurrence (1), note that since β_i satisfies (5), we have $\beta_i^{n+2} = M\beta_i^{n+1} - N\beta_i^n$; and so any linear combination $\{A_1\beta_1^n + A_2\beta_2^n\}$ also satisfies this recurrence relation. In particular, with $c = 2a_1 - Ma_0$ and $D = M^2 - 4N$,

$$a_n = \frac{c + a_0\sqrt{D}}{2\sqrt{D}}\,\beta_1^n - \frac{c - a_0\sqrt{D}}{2\sqrt{D}}\,\beta_2^n \tag{6}$$

satisfies (1) and it is easy to check that the sequence indeed begins with a_0 and a_1.

The relation between Lucas sequences of the first kind (2) and general second order recurrences (1):

$$a_{n+m} = U_m a_{n+1} - NU_{m-1}a_n, \quad m \geqslant 1, \ n \geqslant 0 \tag{7}$$

is easily seen by induction. In particular,

$$a_m = U_m a_1 - NU_{m-1}a_0. \tag{8}$$

If $r > 0$ and $i \geqslant 0$, then the subsequence $\{a_{rn+i}\}$ is a second order recurrence. Indeed the recurrence relation

$$a_{r(n+2)+i} = V_r a_{r(n+1)+i} - N^r a_{rn+i} \tag{9}$$

where V_r is given by (3) and (4) is a straightforward consequence of formula (6).

Another expression for a_n can be obtained by expanding

$$\beta_i^n = \left(\frac{M}{2}\right)^n \left(1 \pm \frac{\sqrt{D}}{M}\right)^n$$

via the binomial theorem and substituting the result into (6). This yields

$$a_n = \left(\frac{M}{2}\right)^n \sum_{j=0}^{\infty} \left\{\frac{c}{M} C_{2j+1}^n + a_0 C_{2j}^n\right\} \left(\frac{D}{M^2}\right)^j. \tag{10}$$

To obtain an analogous formula for the sequence $\{a_{rn+i}\}$, first note that $N = \beta_1\beta_2$ and $D = (\beta_1 - \beta_2)^2$; and so the discriminant of the companion equation of the recurrence (9) is, in view of (4), just

$$DU_r^2 = (\beta_1^r - \beta_2^r)^2 = (\beta_1^r + \beta_2^r)^2 - 4\beta_1^r\beta_2^r = V_r^2 - 4N^r.$$

Further the quantity analogous to c is $2a_{r+i} - V_r a_i$; and using (7), (4), and $M = \beta_1 + \beta_2$, it is easy to verify that $2a_{r+i} - V_r a_i = U_r c_i$ where $c_i = 2a_{r+1} - Ma_i$. Comparing (1) and (9) we see then that the analogue of (10) is

$$a_{rn+i} = \left(\frac{V_r}{2}\right)^n \sum_{j=0}^{\infty} \left\{\frac{c_i U_r}{V_r} C_{2j+1}^n + a_i C_{2j}^n\right\} \left(\frac{DU_r^2}{V_r^2}\right)^j. \tag{11}$$

Several results used in later sections will now be stated. For the most part, the reader is referred to the original papers for proofs.

If p is a rational prime and n^2 is an integer, we denote by $v_p(n)$, the number of times p divides n. Part (i) of the next theorem is due to Smiley [15] and the rest is proved in Chowla, Dunton, and Lewis [6].

THEOREM A. *Let $\{a_n\}$ be a non-degenerate second order linear recurrence satisfying* (1) *with* $(a_0, a_1) = 1$.

(i) *If* $M^2-4N \geqslant 0$, *then the multiplicity of* $\{a_n\}$ *is at most three.*

(ii) *If for some prime* p, *one has* $0 < v_p(M^2) < v_p(N)$, *then the multiplicity of* $\{a_n\}$ *is at most* 2.

(iii) *If* $M^2-4N < 0$ *and there is a prime divisor* $p \geqslant 5$ *of* M^2-4N *which does not divide* M *nor* $2a_1-a_0M$, *then the multiplicity of* $\{a_n\}$ *is bounded above by* $p-1$.

(iv) *If* $M^2-4N < 0$ *and there is a prime* $p \geqslant 5$ *which does not divide* M *and such that*

$$v_p(2a_1-a_0M) \geqslant v_p(M^2-4N) > 0,$$

then the multiplicity of $\{a_n\}$ *is bounded above by* 2.

Although we are interested in proving results about linear recurrences of rational integers, the proofs involve linear recurrences of quadratic integers. Therefore we define a Lehmer sequence to be a sequence $a_0, a_1, \ldots$ of algebraic integers which satisfies a relation

$$a_{n+2} = \pm M^{1/2}a_{n+1} - Na_n, \quad n \geqslant 0 \tag{12}$$

where M and N are fixed relatively prime rational integers and the sign is constant. The sequence $\{U'_n\}$ satisfying the same relation but starting with $U'_0 = 0$ and $U'_1 = 1$ is called the *associated Lehmer sequence of the first kind*; the sequence $\{V'_n\}$ satisfying the same relation as does $\{a_n\}$ but starting with $V'_0 = 2$ and $V'_1 = \pm\sqrt{M}$ is called the *associated Lehmer sequence of the second kind*. The verification of the analogues of (4), (7), (8), and (9) are left to the reader. The proof of the next result parallels that of the Lucas sequence analogue; see D. H. Lehmer [8] and E. Lucas [11].

THEOREM B. (i) U'_n *and* V'_n *are prime to* N *and* $(U'_n, V'_n) = 1, \sqrt{2}$, *or* 2.

(ii) $(U'_n, U'_m) = |U'_{(m,n)}|$.

(iii) *If for some prime* p, *we have* $p^\alpha \| U'_m$, $\alpha > 0$, *and* $p \nmid k$, *then* $p^{\alpha+\lambda} | U'_{kmp^\lambda}$ *and if* $p^\alpha \neq 2$, *then* $p^{\alpha+\lambda} \| U'_{kmp^\lambda}$.

(iv) *If* p *is an odd prime dividing neither* M *nor* N, *then* $p | U'_{p-\sigma\varepsilon}$ *where* $\sigma = \left(\frac{M}{p}\right)$ *and* $\varepsilon = \left(\frac{M^2-4N}{p}\right)$ *are Legendre symbols. If* p *is an odd prime divisor of* M, *then* $p | U'_{2p}$.

Several lemmas on special kinds of sequences follow.

LEMMA 1. *Let* $\{V'_n\}$ *be a non-degenerate sequence defined by*

$$V'_{n+2} = \pm M^{1/2}V'_{n+1} - NV'_n, \quad V'_0 = 2, \quad V'_1 = \pm M^{1/2}$$

where $M > 0$ *and* N *are integers with* $M^2-4N < 0$. *Then the only case in which*

$$(V'_n)^2 = 1, \quad n \geqslant 0$$

has more than one solution is when $M = 1$ *and* $N = 2$. *In the exceptional case, if the sign is positive, then the solutions are* $n = 1, 4$ *with* $V'_1 = V'_4 = 1$; *if the sign is negative, then the solutions are still* $n = 1, 4$ *but* $V'_1 = -V'_4 = -1$.

Proof. This is a consequence of the theorem in Chowla, Chowla, Dunton, and Lewis [5]. For the reduction, see [1], Lemma 1.

In their solution of Ramanujan's equation $2^{n+2} = x^2+7$, Nagell [13] and Skolem, Chowla and Lewis [14] showed that the Lucas sequence

$$U_{n+2} = U_{n+1} - 2U_n, \quad U_0 = 0, \quad U_1 = 1$$

has multiplicity 3. The next lemma is a generalization of this fact and was proved in Alter and Kubota [1]. A related result is proved by Townes [17].

LEMMA 2. *Any second order recurrence satisfying*

$$a_{n+2} = a_{n+1} - 2a_n, \quad n \geqslant 0$$

is of multiplicity at most three; *any recurrence satisfying*

$$a_{n+2} = -a_{n+1} - 2a_n, \quad n \geqslant 0$$

is of multiplicity at most four.

The proof of the next lemma can also be found in [1].

LEMMA 3. *Let* $\{a_n\}$ *be a recurrence satisfying*

$$a_{n+2} = Ma_{n+1} - Na_n$$

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

LEMMA 4. *Let* $\{a_n\}$ *be a second order linear recurrence satisfying*

$$a_{n+2} = Ma_{n+1} - Na_n, \quad (a_0, a_1) = 1$$

and let $d = d_1d_2$ *where* $(d_1, M, N) = 1$, *and the prime divisors of* d_2 *all lie amongst those of* (M, N). *When it exists, let* r *be the least positive integer for which* U_r *is a multiple of* d_1 *where* $\{U_n\}$ *is the Lucas sequence of the first kind which satisfies the same recurrence as does* $\{a_n\}$. *Suppose* $d_1 | a_0$. *Then for every positive integer* n, a_n *is a multiple of* d_1 *if and only if* r *exists and divides* n.

Proof. There is a positive real number R, a real number M', and an integer N' such that R^2 is an integer, $M = M'R$, $N = N'R^2$, and $(M', N') = 1$. Let $\{U'_n\}$ be the Lehmer sequence of the first kind defined by

$$U'_{n+2} = M'U'_{n+1} - N'U'_n, \quad U'_0 = 0, \quad U'_1 = 1.$$

Then it is easy to verify that $U_n = U'_n R^{n-1}$. Now $(d_1, R^2) = 1$, and so $d_1 | U'_n$ if and only if $d_1 | U_n$. By (8) and the assumption that $d_1 | a_0$, we have $a_n \equiv a_1 U_n \pmod{d_1}$. Since also $(a_0, a_1) = 1$, $d_1 | a_n$ is equivalent to $d_1 | U_n$. Finally by Theorem B (ii) and (iii), we have that r exists and divides n if and only if U'_n is a multiple of d_1. Combining results gives the assertion.

3. The p-adic argument. The next theorem is contained essentially in Laxton [7] and in Lewis [6], [10]. However, some refinements in the arguments are needed; so for the convenience of the reader, it is reproduced here.

THEOREM 1. *Let $\{a_n\}$ be a non-degenerate second order linear recurrence satisfying the relation* (1) *and β_1, β_2 be the roots of the companion polynomial* (5). *Suppose p is a rational prime which does not divide N and π is a prime element in the completion of the ring of integers of $Q(\beta_i)$ at a prime ideal* $\mathfrak{p}$ *lying over p. Let q be a positive integer with*

$$\beta_1^q = \beta_2^q \equiv 1 \pmod{\pi^\varkappa}, \qquad \varkappa = \left[\frac{e}{p-1}\right] + 1$$

where e is the ramification index of $\mathfrak{p}$ *over p, and where q is chosen minimal if $p = 2$. For any rational integer d, consider the equation*

$$a_{qn+i} = d$$

where i is a fixed integer in the range $0 \leqslant i < q$. Then this equation has at most two solutions unless $p = 3$ and at least one of $(\beta_1^q - 1)/3$ and $(\beta_2^q - 1)/3$ is a π-adic unit; in the exceptional case it has no more than three solutions. If p is odd, then there is at most one value of i for which the equation has more than one solution. If $p = 2$ and if the equation has two solutions when $i = i_1$ and also when $i = i_2$ where $0 \leqslant i_1 < i_2 < q$, then $q = 2(i_2 - i_1)$; in particular, there are at most two values of i for which the equation has two solutions.

Proof. Note that even if p is odd, there is no loss of generality in assuming that q is the least positive integer with $\beta_1^q \equiv \beta_2^q \equiv 1 \pmod{\pi^\varkappa}$. Following the notation of Laxton [7], let $\delta_i = \beta_i^q = 1 + \gamma_i \pi^S$ for $i = 1, 2$ where $S \geqslant \varkappa$. Since the β_i are not roots of unity, we may assume S and γ_i chosen so that at least one of the γ_i is a π-adic unit. Now δ_i^x is defined for every p-adic integer x, and $\log \delta_i$ is a p-adic integer [3]. In fact, for $i = 1$ and 2,

$$\log \delta_i = \sum_{r=1}^{\infty} (-1)^{r-1} \gamma_i^r \frac{\pi^{Sr}}{r} = \pi^S \left(\gamma_i + \pi^S \sum_{r=2}^{\infty} (-1)^{r-1} \gamma_i^r \frac{\pi^{S(r-2)}}{r} \right)$$

where the second term is a π-adic non-unit by the choice of S. It follows that for $j = 1$ and 2, $|\log \delta_j|_\mathfrak{p} \leqslant |\pi|_\mathfrak{p}^S$ with equality holding for at least one value of j.

By (6), there are conjugate quadratic numbers A_1 and A_2 such that

$$a_n = A_1 \beta_1^n + A_2 \beta_2^n,$$

and clearly $A_1 A_2 \neq 0$. Suppose that for some i with $0 \leqslant i < q$, $a_{qn+i} = d$ has a least non-negative rational integer solution n_i. Then letting $n = n_i + y$,

$$\begin{aligned} a_{qn+i} - d &= A_1 \beta_1^{qn_i+i} \delta_1^y + A_2 \beta_2^{qn_i+i} \delta_2^y - d \\ &= \pi^k (B_{i1} \delta_1^y + B_{i2} \delta_2^y - d') = \pi^k \delta_2^y h_i(y) \end{aligned}$$

where $k = \min(\operatorname{ord}_\mathfrak{p} A_1, \operatorname{ord}_\mathfrak{p} A_2, \operatorname{ord}_\mathfrak{p} d)$, $d = \pi^k d'$, and $A_j \beta_j^{qn_i+i} = \pi^k B_{ij}$ for $j = 1, 2$. Here k was chosen so that d', B_{i1}, and B_{i2} are p-adic integers not all divisible by π. Further $\operatorname{ord}_\mathfrak{p} B_{ij} = \operatorname{ord}_\mathfrak{p} A_j - k$ and $\operatorname{ord}_\mathfrak{p} d' = \operatorname{ord}_\mathfrak{p} d - k$ are independent of i.

Expanding $h_i(y)$ in p-adic power series and noting that $h_i(0) = 0$, we get

$$h_i(y) = \sum_{r=1}^{\infty} \left\{ B_{i1} \left(\log \frac{\delta_1}{\delta_2} \right)^r - d' (\log \delta_2^{-1})^r \right\} \frac{y^r}{r!}.$$

Note that the coefficient C_r of y^r has p-adic value at most

$$|\pi^{Sr}/r!|_\mathfrak{p} \leqslant |\pi^{\varkappa r}/r!|_\mathfrak{p} < 1$$

since

$$\begin{aligned} \varkappa r - \operatorname{ord}_\mathfrak{p} r! &= \left(\left[\frac{e}{p-1} \right] + 1 \right) r - e \sum_{k=1}^{\infty} \left[\frac{r}{p^k} \right] \\ &\geqslant \left(\frac{e - (p-2)}{p-1} + 1 - \frac{e}{p} \frac{1}{1 - 1/p} \right) r \\ &= \frac{r}{p-1} \to \infty \quad \text{as } r \to \infty \text{ and is } > 0 \end{aligned}$$

and so $h_i(y)$ has p-adic integer coefficients and converges for all p-adic integers y.

We will apply Strassman's Lemma [16] to the effect that if $h(y) = \sum_{r=0}^{\infty} c_r y^r$ is a non-identically zero power series with p-adic integer coefficients which converges for all p-adic integers y, then h has at most $M = \max \{r \mid \operatorname{ord}_\mathfrak{p} c_r \text{ is minimal}\}$ p-adic zeros.

Let $R = \min\left(\operatorname{ord}_\mathfrak{p}(B_{i1} \log \delta_1/\delta_2), \operatorname{ord}_\mathfrak{p}(d' \log \delta_2^{-1})\right)$. R is independent of i and is finite since δ_1/δ_2 is not a root of unity and $A_1 \neq 0$. Let $S' = S - \delta_{2p} e$ where δ_{2p} is the Kronecker δ. Then by the expansion of $h_i(y)$,

$$|C_1|_\mathfrak{p} \leqslant |\pi^R|_\mathfrak{p}, \qquad |C_2|_\mathfrak{p} \leqslant |\pi^{R+S'}|_\mathfrak{p}$$

and in general for $r \geqslant 3$,

$$|C_r|_p = |\{B_{i1}(\log \delta_1/\delta_2)^r - d'(\log \delta_2^{-1})^r\}/r!|_p \leqslant |\pi^{R+S(r-1)}/r!|_p$$
$$= |\pi^{R+S'}|_p\,|\pi^{S(r-2)+\delta_{2p}e}/r!|_p < |\pi^{R+S'}|_p$$

for $r \geqslant 4$ since

$$S(r-2)+\delta_{2p}e - ev_p(r!) > \left(\left[\frac{e}{p-1}\right]+1\right)(r-2)+\delta_{2p}e-\frac{er}{p-1}$$
$$\geqslant \frac{(e+1)(r-2)-er}{p-1}+\delta_{2p}e = \frac{r-2e-2}{p-1}+\delta_{2p}e \geqslant 0$$

because $e \leqslant 2$. The same estimate holds for $r = 3$ unless $p = 3$ and $S = \varkappa = e$ (i.e. $(\beta_j^q - 1)/3$ are p-adic units for $j = 1$ or 2) since $S + \delta_{2p}e - ev_p(6) > 0$.

By Strassman's Lemma it follows that if $h_i(y) = 0$ has two solutions, then $\mathrm{ord}_p C_1 \geqslant R + S'$. Suppose this occurs for two values of i, say i and j where $0 \leqslant i < j < q$. Written as congruences, the corresponding inequalities become

$$\beta_1^i \delta_1^{n_i} A_1 \pi^{-k} \log \frac{\delta_1}{\delta_2} - d' \log \delta_2^{-1} \equiv 0 \pmod{\pi^{R+S'}},$$

$$\beta_1^j \delta_1^{n_j} A_1 \pi^{-k} \log \frac{\delta_1}{\delta_2} - d' \log \delta_2^{-1} \equiv 0 \pmod{\pi^{R+S'}}.$$

Since $S' > 0$, the definition of R and these congruences imply that all three of the terms have p-adic order R. Subtracting and dividing out $A_1 \pi^{-k} \log \delta_1/\delta_2$ yields

$$\beta_1^i \delta_1^{n_i} - \beta_1^j \delta_1^{n_j} \equiv 0 \pmod{\pi^{S'}}$$

and so $\beta_1^{j-i} \equiv 1 \pmod{\pi^{S'}}$ since $\delta_1 \equiv 1 \pmod{\pi^S}$. Now the whole argument can be repeated with β_1 and β_2 interchanged to show that $\beta_2^{j-i} \equiv 1 \pmod{\pi^{S'}}$.

If p is odd, the facts that $0 < j - i < q$ and $S = S'$ give a contradiction with the choice of q; so at most one equation $a_{qn+i} = d$ has more than one solution. If $p = 2$ and $\beta_k^{j-i} \equiv 1 \pmod{\pi^e}$ for $k = 1, 2$, then $\beta_k^{2(j-i)} \equiv 1 \pmod{\pi^{2e}}$ and $2e \geqslant \varkappa$. Hence $q | 2(j-i)$ and $0 < 2(j-i) < 2q$ and so $q = 2(j-i)$. Finally, if $p = 2$ and $\beta_k^{j-i} \not\equiv 1 \pmod{\pi^e}$ for $k = 1$ or 2, then since $S' = S - e \geqslant 1$, we have $e = 2$, $S = 3$, and $\pi | \beta_m^{j-i} - 1$ for $m = 1, 2$; but then $\pi^4 | \beta_m^{4(j-i)} - 1$ and $4 > S$ imply $2q | 4(j-i)$. Since $0 < j - i < q$, it follows that $q = 2(j-i)$. The only possible value for q is therefore $q = 2(j-i)$. Since there cannot be three values for i, every pair of which satisfy this equality, no more than 2 subsequences have more than two occurrences of d.

We know that either γ_1 or γ_2 is a p-adic unit; so suppose that the notation is chosen so that $\gamma_1 \not\equiv 0 \pmod{\pi}$. Now the congruences $C_1 \equiv 0 \pmod{\pi^{R+1}}$ and $C_2 \equiv 0 \pmod{\pi^{R+S'+1}}$ cannot both hold true. For if they did, then one would have

$$\pi^{-R} B_{i1} \log \frac{\delta_1}{\delta_2} - \pi^{-R} d' \log \delta_2^{-1} \equiv 0 \pmod{\pi},$$

$$\pi^{-S} \log \frac{\delta_1}{\delta_2}\left(\pi^{-R} B_{i1} \log \frac{\delta_1}{\delta_2}\right) - \pi^{-S} \log \delta_2^{-1}(\pi^{-R} d' \log \delta_2^{-1}) \equiv 0 \pmod{\pi}.$$

By the definition of R, this is a non-trivial solution of a pair of linear homogeneous equations over the residue field at p. But the determinant of the coefficients is

$$-\pi^{-S} \log \delta_2^{-1} + \pi^{-S} \log \frac{\delta_1}{\delta_2} = \pi^{-S} \log \delta_1 \not\equiv 0 \pmod{\pi}$$

which contradicts Cramer's Rule. Combining this with the estimates on $|C_r|_p$ for $r \geqslant 3$, Strassman's Lemma gives the asserted bounds on the number of occurrences of d in $\{a_{qn+i}\}$ for fixed i. Thus Theorem 1 is proved.

The next two lemmas are corollaries to the theorem.

LEMMA 5. *Let $\{a_n\}$ be a non-degenerate linear recurrence satisfying*

$$a_{n+2} = 2Ma_{n+1} - Na_n, \quad n \geqslant 0,$$

where $M \neq 0$, $M^2 - N < 0$, and $2 \nmid Na_0$. Then the multiplicity $m(a_0)$ of a_0 is at most four. It is no more than three provided that M is even and $N \equiv 1 \pmod 4$.

Proof. This is Lemma 4 of Alter and Kubota [1]; note that a computational error invalidates the proof of the claim made there that $m(a_0) \leqslant 3$ in case M is odd, a_1 is even, and $N \equiv 3 \pmod 4$.

LEMMA 6. *Let $\{a_n\}$ be a non-degenerate linear recurrence which satisfies (1) with M and N both odd. If $N \equiv 1 \pmod 4$, $\{a_n\}$ is of multiplicity at most three, and if $N \equiv 3 \pmod 4$, then $\{a_n\}$ is of multiplicity at most five.*

Proof. It is easy to verify that the roots β_1, β_2 of the companion polynomial (5) satisfy $\beta_1^6 \equiv \beta_2^6 \equiv 1 \pmod 4$ and that if $N \equiv -M \equiv 1 \pmod 4$, then $\beta_1^3 \equiv \beta_2^3 \equiv 1 \pmod 4$. Assuming $(a_0, a_1) = 1$, one verifies that $\{a_n\} \pmod 4$ looks like repetitions of fixed constant multiples of

1, 1, 2, 3, 1, 0	if	$M \equiv -N \equiv 1 \pmod 4$,
1, 1, 0, 1, 3, 2	if	$M \equiv N \equiv 3 \pmod 4$,
1, 1, 0, 3, 3, 0 or 1, 3, 2, 3, 1, 2	if	$M \equiv N \equiv 1 \pmod 4$,
1, 1, 2 or 1, 3, 0	if	$-M \equiv N \equiv 1 \pmod 4$.

The result now follows from Theorem 1 applied with $p = 2$.

Theorem 1 gives bounds on the number of solutions of $a_n = d$ in terms of the least prime which does not divide N. The first step in obtaining a bound independent of the prime is given by the next theorem. Note however that the result requires that in addition to $p \nmid N$, one also has $p \nmid d$. The proof uses an idea of R. Apéry [2] which appeared in his treatment of a generalized form of Ramanujan's equation.

THEOREM 2. *Let $\{a_n\}$ be a non-degenerate second order linear recurrence satisfying the recurrence relation* (1) *with $D = M^2 - 4N < 0$. Suppose p is an odd prime. Let r be a positive integer such that $p \mid U_r$ where $\{U_n\}$ is the Lucas sequence of the first kind which satisfies* (2). *Let s be the multiplicative order of $V_r/2 \pmod p$ where $\{V_n\}$ is the Lucas sequence of the second kind which satisfies* (3). *Let β_1 and β_2 be the roots of the companion polynomial* (5) *and π be a prime element in the completion of the ring of integers of $\boldsymbol{Q}(\beta_1) = \boldsymbol{Q}(\beta_2)$ at some prime ideal* $\mathfrak{p}$ *lying over p. Define*

$$\varepsilon = \begin{cases} 1 & \text{if } p = 3 \text{ and } (\beta_i^{rs} - 1)/3 \text{ for } i = 1 \text{ or } 2 \text{ is a } \pi\text{-adic unit,} \\ 0 & \text{otherwise.} \end{cases}$$

$$\delta = \begin{cases} 1 & \text{if no } a_n \text{ is divisible by } p, \\ 0 & \text{otherwise.} \end{cases}$$

Then if $p \nmid Nd$, then with the possible exception of one value of i in the range $0 \leqslant i < r$, the equation

$$a_{rn+i} = d$$

has at most one solution; the equation corresponding to the exceptional value of i has at most $2 + \varepsilon$ solutions. In particular, if $p \nmid Nd$, then

$$m(d) \leqslant r + \delta + \varepsilon.$$

Remark. If $p \nmid N$, then it follows from Theorem B (iv) that there is an r as in the statement of the theorem.

Proof. If $a_n = d$ has no solutions, there is nothing to prove. If there is at least one solution, we may assume without loss of generality that $a_0 = d$. Since $p \mid U_r$, Theorem B (i) implies that $p \nmid V_r$. By (11), we have since $p \mid U_r$ that

$$a_{rn+i} \equiv \left(\frac{V_r}{2}\right)^n a_i \pmod p. \tag{13}$$

Since $p \nmid a_0$ and $p \nmid V_r$, we see that for each fixed i, there is at most one value of j_i in the range $0 \leqslant j_i < s$ for which $a_{rj_i+i} \equiv d = a_0 \pmod p$. Further every occurrence of d in $\{a_{rn+i}\}$ must lie in $\{a_{rsn+rj_i+i}\}$.

Using (4), it is easy to verify that for each n,

$$\beta_1^n, \beta_2^n = V_n/2 \pm (\beta_1 - \beta_2) U_n/2.$$

In particular, $\beta_k^r \equiv V_r/2 \pmod p$ and $\beta_k^{rs} \equiv 1 \pmod p$ for $k = 1$ and 2. So Theorem 1 applies to the sequence $\{a_{rn+i}\}$ which proves the first assertion.

Suppose $p \mid a_m$ for some m. Choose i with $0 \leqslant i < r$ and $m \equiv i \pmod r$. Then by the congruence (13), we see that since $p \nmid V_r$, we have $p \mid a_m$ implying $p \mid a_i$. Since $p \nmid d$, $\{a_{rn+i}\}$ contains no occurrences of d. Hence at most $r - 1 + \delta$ of the sequences $\{a_{rn+i}\}$ contain occurrences of d. By the first assertion of the theorem, we have therefore that

$$m(d) \leqslant (r - 1 + \delta) + 1 + \varepsilon = r + \delta + \varepsilon,$$

which completes the proof of the theorem.

Remark. In a similar way, using (10), one can prove Theorem A (iii) and (iv).

4. The relatively prime case. In this section, Theorem 2 will be used to treat linear recurrences satisfying (1) with $(M, N) = 1$. This case was studied in Alter and Kubota [1] where, in particular, it is shown that non-degenerate second order linear recurrences with $(M, N) = 1$ have multiplicity at most five. In that paper, it was conjectured that five could be improved to four, and this is the case.

THEOREM 3. *Let $\{a_n\}$ be a non-degenerate second order linear recurrence satisfying*

$$a_{n+2} = Ma_{n+1} - Na_n \quad \text{with} \quad (M, N) = 1.$$

Then $\{a_n\}$ has multiplicity at most four.

COROLLARY. (i) *If $(M, N) = 1$, then any second order linear recurrence satisfying* (1) *has either infinite multiplicity or multiplicity bounded above by four.*

(ii) *The multiplicity of any Lehmer sequence of first or second kind is either infinite or bounded above by four.*

Proof of Corollary. (i) If the recurrence is degenerate, then the corollary follows by M. Ward's characterization [18] of degenerate recurrences. The non-degenerate case is the theorem.

(ii) If the Lehmer sequence satisfies (12) and if M is a square, the assertion is a special case of assertion (i). If M is not a square, then U_n' (resp. V_n') is irrational if and only if n is even and $n > 0$ (resp. n is odd). So one need only bound the multiplicities of $\{U_{2n}/M^{1/2}\}$, $\{U_{2n+1}'\}$, $\{V_{2n}'\}$, and $\{V_{2n+1}'/M^{1/2}\}$. But these are rational integer linear recurrences, and so the first assertion applies.

Proof of Theorem 3. 1. By Theorem A (i), it suffices to consider the case where $M^2 - 4N < 0$. Let d be an integer. We will show that $m(d) \leqslant 4$. Clearly we may assume without loss of generality that $a_0 = d$ and $(a_0, a_1) = 1$. If $d = 0$ and $a_0 = a_m = 0$ for some $m > 0$, then $a_{mn} = 0$

for all $n \geqslant 0$ by (9). But then $\{a_n\}$ is degenerate by Theorem 2. If $d \neq 0$, apply Lemma 4 with $d_1 = d$ and $d_2 = 1$ to prove that every occurrence of d lies in a subsequence $\{a_{rn}\}$, every term of which is divisible by d. Replacing $\{a_n\}$ with $\{a_{rn}/d\}$ we are reduced to the case where $d = 1$.

2. If $U_2 = M$ or $U_3 = M^2 - N$ is divisible by a prime $p \geqslant 5$, then $m(1) \leqslant 4$ by Theorem 2. If M is even, then since $(M, N) = 1$, we have that N is odd; so Lemma 5 implies that $m(1) \leqslant 4$. If M is a multiple of 3, then Theorem 2 implies that $m(1) \leqslant r + \delta + \varepsilon \leqslant 4$. Thus we may assume that $M = \pm 1$ and $M^2 - N = \varepsilon' 2^s 3^t$ where $s, t \geqslant 0$ and $\varepsilon' = \pm 1$. Solving for N yields $N = 1 - \varepsilon' 2^s 3^t$. Since $M^2 - 4N = -3 + \varepsilon' 2^{s+2} 3^t < 0$, we must have $\varepsilon' = -1$.

3. Suppose $t > 0$; then $3 | U_3 = M^2 - N$, $N \equiv 1 \pmod 3$, and $M \equiv \pm 1 \pmod 3$. If $M \equiv 1 \pmod 3$, it is easy to check that the sequence considered modulo 3 consists of repetitions of segments all of which look like one of the following

$$1, 1, 0, -1, -1, 0 \quad \text{or} \quad 1, -1, 1, -1, 1, -1.$$

For the first kind of sequence, Theorem 2 applied with $r = 3$ shows that $m(1) \leqslant 4$. For the second kind of sequence, we can replace $\{a_n\}$ with $\{a_{2n}\}$ or $\{a_{2n+1}\}$. By (9), we see that the new sequence satisfies a recurrence relation with coefficients M and N satisfying $M \equiv -N \equiv -1 \pmod 3$.

For any such recurrence, the sequence considered modulo 3 looks like repetitions of one of the following segments

$$1, 1, 1 \text{ or } -1, -1, -1 \text{ or } -1, 1, 0 \text{ or } 1, -1, 0.$$

Note that $0 \equiv \beta_i^2 - M\beta_i + N \equiv \beta_i^2 - 2\beta_i + 1 \pmod 3$, for $i = 1$ and 2. So $\beta_i \equiv 1 \pmod \pi$ where π is as in the statement of Theorem 2 with $p = 3$. But then $\beta_i^3 \equiv 1 \pmod{3\pi}$ for $i = 1, 2$; so the parameter ε in Theorem 2 is zero. By that same theorem, it follows that $m(1) \leqslant 4$. Thus we are reduced to the case where $t = 0$.

4. If $s = 0$, then $M = \pm 1$ and $N = 2$. So $m(1) \leqslant 4$ by Lemma 2. If $s = 1$, then $M = \pm 1$, $N = 3$, and $U_4 = M(M^2 - 2N) = \mp 5$. When $M = 1$, the sequence considered modulo 5 is a succession of repetitions of a non-zero multiple of one of the following segments

$$1, 1, 3, 0 \text{ or } 1, 2, 4, 3 \text{ or } 1, 4, 1, 4.$$

By Theorem 2 with $p = 5$, we conclude that $m(d) \leqslant 3$. When $M = -1$, then all solutions of $a_n = 1$ except possibly $n = 0$ have the same parity by Lemma 3. Again by Theorem 2 with $p = 5$, we have that $m(1) \leqslant 1 + 1 + 3 = 4$.

5. If $s \geqslant 2$, then $N \equiv 1 \pmod 4$. If $M = 1$, then the sequence considered modulo 4 looks like repetitions of segments of the form

$$1, 1, 0, 3, 3, 0 \text{ or } 1, 3, 2, 3, 1, 2 \pmod 4.$$

Also $\beta_i^2 \equiv M\beta_i - N \equiv \beta_i - 1 \pmod 4$ for $i = 1, 2$. So $\beta_i^3 \equiv \beta_i^2 - \beta_i \equiv -1 \pmod 4$ and $\beta_i^6 \equiv 1 \pmod 4$. So the parameter q of Theorem 1 with $p = 2$ is 6; it follows that $m(1) \leqslant 3$. If $M = -1$, then the sequence considered modulo 4 looks like repetitions of segments of one of the following forms

$$1, 1, 2 \text{ or } 1, 3, 0 \text{ or } 3, 1, 0.$$

Also $\beta_i^2 \equiv -\beta_i - 1 \pmod 4$ and so $\beta_i^3 \equiv -\beta_i^2 - \beta_i \equiv 1 \pmod 4$ for $i = 1$ and 2. Theorem 1 with $p = 2$ and $q = 3$ then shows that $m(1) \leqslant 3$. This completes the proof.

The general outline of the last proof can be used to show that better bounds apply to certain more restricted classes of linear recurrences. The next result is a good example of this:

THEOREM 4. *Let $\{U_n\}$ be a non-degenerate Lucas sequence of the first kind which satisfies (2) with $(M, N) = 1$. Either $\{U_n\}$ has multiplicity at most three or else $M = -1$ and $N = 2$. In the exceptional case, -1 occurs exactly four times and no other integer occurs so often.*

Proof. Part 1 of the proof of Theorem 3 can be carried over without changes except that we no longer translate the first occurrence of d to zero and that the reduction is only to $d = \pm 1$. Part 2 can also be repeated except in the case where M is even; note that in applying Theorem 2, the parameter δ is always 0 and so the bounds of four are reduced to three.

Suppose that M is even. The sequence U_n reduced modulo 4 consists of repetitions of the segments

$$\begin{aligned} &0, 1, 2, 1 && \text{if} && 2 \| M \text{ and } N \equiv 3 \pmod 4, \\ &0, 1, 2, 3 && \text{if} && 2 \| M \text{ and } N \equiv 1 \pmod 4, \\ &0, 1, 0, 3 && \text{if} && 4 | M \text{ and } N \equiv 1 \pmod 4, \\ &0, 1 && \text{if} && 4 | M \text{ and } N \equiv 3 \pmod 4. \end{aligned}$$

Since Theorem 1 with $q = 4$ in the $N \equiv 1 \pmod 4$ case and $q = 2$ in the $4 | M$, $N \equiv 3 \pmod 4$ case shows that $m(\pm 1) \leqslant 2$, we may suppose that $2 \| M$, $N \equiv 3 \pmod 4$, and hence that $m(-1) = 0$ and that 1 does not occur in $\{U_{2n}\}$. If U_4 is divisible by a prime greater than 3, then it follows that $m(1) \leqslant 3$ by Theorem 2. Since $\delta = 0$, the same conclusion can be made by Theorem 2 if U_2 (resp. U_3) is divisible by a prime larger than 2 (resp. 3). Thus, we may assume that $U_2 = M = \pm 2$, and that U_3 and U_4 are not divisible by any primes greater than 3. Since $U_3 = M^2 - N$ is odd, either $U_3 = \pm 1$ or $3 | U_3$. In the first case, $N = M^2 \mp 1 = 3$ or 5. In the second case, $3 \nmid U_4$ by Theorem B (ii). Since $U_4/2M = M^2/2 - N$

is odd, it follows that $M^2/2-N=\pm 1$ and so $N=2\mp 1=1$ or 3. But $N\equiv 3 \pmod 4$, and so both cases reduce to $M=\pm 2$, $N=3$. The sequence $\{U_n\}$ reduced modulo 9 begins with 0, 1 and continues with repetitions of the segment

$$\pm 2, 1, \mp 4, -2, \pm 8, 4 \pmod 9.$$

Since $\{U_{2n}\}$ does not contain 1, it follows that U_n can be 1 only when $n=1$ or $n\equiv 3 \pmod 9$. Finally, since $U_6=\mp 10$, we can apply Theorem 2 with $p=5$ and $r=6$ to conclude that 1 occurs at most twice in the subsequence $\{U_{6n+3}\}$, and so $m(1)\leqslant 3$. This completes the case where M is even.

For part 3 of the proof, first suppose that $M\equiv 1 \pmod 3$. Then $0\equiv \beta_j^2-M\beta_j+N\equiv(\beta_j+1)^2 \pmod 3$. So $\beta_j^6\equiv 1 \pmod{3\pi}$ for $j=1,2$. If the sequence consists of repetitions of 1, 1, 0, -1, -1, 0, then Theorem 2 with $p=3$ and $\varepsilon=0$ gives $m(\pm 1)\leqslant 3$. Since $a_0=0$, the second kind of sequence does not occur. The proof in the case $M\equiv -1 \pmod 3$ carries over; $\varepsilon=0$ and $a_0=0$ imply that $m(\pm 1)\leqslant 3$.

Part 5 of the proof carries over without change, and in part 4 with $s=1$, the only change is to note that $a_0\neq\pm 1$. Finally, if $s=0$ and $M=1$, then $m(\pm 1)\leqslant 3$ by Lemma 2. If $M=-1$, note that the sequences

$$U_{n+2}=-U_{n+1}-2U_n, \quad U_0=0, \quad U_1=1$$

and

$$\overline{U}_{n+2}=\overline{U}_{n+1}-2\overline{U}_n, \quad \overline{U}_0=0, \quad \overline{U}_1=1$$

are related by $U_n=(-1)^{n+1}\overline{U}_n$. The solution of Ramanujan's equation given by Skolem, Chowla, and Lewis [14], consists of showing that

$$\overline{U}_1=\overline{U}_2=-\overline{U}_3=-\overline{U}_5=-\overline{U}_{13}=1$$

and that $\overline{U}_n\neq\pm 1$ for all other values of n. It follows that $U_n=-1$ has exactly four solutions and that $n=1$ is the unique solution of $U_n=1$.

Now in the reduction done in part 1 of the proof, the new sequence $\{a_{rn}\}$ satisfies the recurrence relation (9). So $N^r=2$ in this case. Thus $r=1$, and so the only non-degenerate Lucas sequence of the first kind with multiplicity four is that with $M=-1$ and $N=2$. Further -1 is the only integer which occurs four times in this exceptional sequence. This completes the proof.

There is an analogue of Theorem 4 for Lucas sequences of the second kind. The proof can be constructed using Theorem A (iv) and the ideas of this section. We omit the proof.

THEOREM 5. *Let $\{V_n\}$ be a Lucas sequence of the second kind satisfying the recurrence relation (3) with $(M,N)=1$. If the multiplicity of $\{V_n\}$ is finite, then it is bounded above by two except when $M=\pm 2$ and $N=3$.*

In the exceptional cases, ± 2 is the only integer which occurs three times, and no integer occurs more often.

5. Proof of Morgan Ward's conjecture. The conjecture is true in the degenerate case [18]. In the non-degenerate case, we prove

THEOREM 6. *No integer occurs more than five times in a non-degenerate second order linear recurrence.*

Proof. Let $\{a_n\}$ be a non-degenerate second order linear recurrence satisfying the recurrence relation (1), and let d be an integer. We will show that $m(d)\leqslant 5$.

By Theorem A (i), it suffices to consider the case where $M^2-4N<0$. By Theorem 3, we may assume $(M,N)>1$. By Lemma 4, it suffices to treat the case where all prime divisors of d are divisors of (M,N). Also we lose nothing in assuming that $a_0=d$ and that $(a_0,a_1)=1$.

By Lemmas 5 and 6, we may assume N is even. Suppose $3\nmid N$. Then $3\nmid d$ and at least one of $U_2=M$, $U_3=M^2-N$, and $U_4=(M^2-2N)M$ is divisible by three. Hence by Theorem 2 applied with $p=3$, either $m(d)\leqslant 5$ or else $3\mid M^2-2N$ and $\delta=1$. The second possibility does not occur since if $3\mid M^2-2N$ and $3\nmid N$, then $M\equiv\pm 1 \pmod 3$, $N\equiv -1 \pmod 3$, and it is easy to verify that all sequences considered modulo 3 look like repetitions of segments of the form

$$1, 1, -1, 0, -1, -1, 1, 0 \quad \text{if} \quad M\equiv 1 \pmod 3$$

or

$$1, -1, -1, 0, -1, 1, 1, 0 \quad \text{if} \quad M\equiv -1 \pmod 3.$$

Thus we may assume that N is a multiple of three.

Suppose that $U_2=M$ has an odd prime divisor p. If p does not divide N, then $p\nmid d$ and so by Theorem 2, $m(d)\leqslant 2+\delta+\varepsilon\leqslant 4$. Thus we can assume that every prime divisor of M divides N. Further if for some prime p, we have $0<v_p(M^2)<v_p(N)$, then $m(d)\leqslant 2$ by Theorem A (ii). So we can assume that $v_p(M^2)\geqslant v_p(N)$ for all prime divisors p of M. Finally by the recurrence relation (1), every prime divisor of (M,N) divides a_n for every $n\geqslant 2$; so we may assume that every prime divisor of (M,N) divides d.

There is a positive real number R and real numbers M' and N' satisfying

$$M=M'R, \quad N=N'R^2, \quad (M'^2,N')=1, \quad \text{and} \quad R^2, N', M'^2\in\boldsymbol{Z}.$$

Let $\{b_n\}$ be the sequence defined by $a_n=R^{n-1}b_n$, so that

$$b_{n+2}=M'b_{n+1}-N'b_n, \quad b_0=Ra_0, \quad b_1=a_1.$$

Let $\{U'_n\}$ (resp. $\{U_n\}$) be the Lehmer (resp. Lucas) sequence of the first kind which satisfies the same recurrence relation as does $\{b_n\}$ (resp. $\{a_n\}$).

Then $U_n = R^{n-1}U'_n$, and by (8) we have

$$a_n = a_1 U_n - N a_0 U_{n-1},$$
$$b_n = a_1 U'_n - N' R a_0 U'_{n-1}. \tag{14}$$

Let

$$P = \Big(\prod_{\substack{p|M\\ p\text{ prime}}} p\Big)\Big/\Big(\prod_{\substack{\sqrt{p}|M'\\ p\text{ prime}}} \sqrt{p}\Big).$$

Since $(P^2, N') = 1$, Theorem B (iv) guarantees that there is a least positive integer r with $P|U'_r$. Let $t = r\big(\prod_{\substack{p|M\\ p\text{ prime}}} p\big)$. By (14) and Theorem B (ii) and (iii), we have $P|b_n$ if and only if $P|U'_n$ if and only if $r|n$.

Now there is at most one solution of $a_n = \pm d$ with $r \nmid n$. In fact, let s be the least index with $r \nmid s$ and $a_s = \pm d$. Since $r \nmid s$, we have $P \nmid b_s$; so there is a prime p with $v_p(P) > v_p(b_s)$. We have

$$\begin{aligned} v_p(d) &= v_p(a_s) = v_p(R^{s-1}b_s) = (s-1)v_p(R) + v_p(b_s) \\ &< (s-1)v_p(R) + v_p(P) \leqslant s v_p(R). \end{aligned}$$

Therefore, if $s' > s$, then

$$v_p(a_{s'}) = v_p(R^{s'-1}b_{s'}) \geqslant (s'-1)v_p(R) \geqslant s v_p(R) > v_p(d),$$

and so $a_{s'} \neq \pm d$ for any $s' > s$.

By Theorem B (iii), t is the least positive integer such that $v_p(U'_t) > v_p(U'_r)$ for all prime divisors p of M. There is at most one solution of $a_n = \pm d$, $r|n$, $t \nmid n$. In fact, if $s < s'$ are two, then

$$(s'-1)v_p(R) + v_p(b_{s'}) = v_p(a_{s'}) = v_p(a_s) = (s-1)v_p(R) + v_p(b_s)$$

and so $v_p(b_{s'}) < v_p(b_s)$. Choosing p so that $v_p(t) > v_p(s)$; we have by (14),

$$v_p(b_{s'}) \geqslant v_p(U'_{s'}) \geqslant v_p(U'_r) = v_p(b_s)$$

which is a contradiction.

Let $\{V'_n\}$ (resp. $\{V_n\}$) be the Lehmer (resp. Lucas) sequence of the second kind which satisfies the same recurrence relation as does $\{b_n\}$ (resp. $\{a_n\}$). Then $V_n = R^n V'_n$. Now $\sqrt{3} \nmid V'_r, V'_t$. In fact, if $3|M$, then $3|(M, N)$ and so $\sqrt{3}|U'_r, U'_t$ and the assertion follows by Theorem B (i). On the other hand, if $3 \nmid M$, then $3 \nmid V_n$ for any n by the recurrence relation (3) and the fact that $3|N$. A fortiori, $\sqrt{3} \nmid V'_r, V'_t$.

Suppose there is a prime $p \geqslant 5$ such that $\sqrt{p}|V'_r$ (resp. V'_t). By Theorem B (i), $\sqrt{p} \nmid U'_r$ (resp. U'_t); and so by the choice of r and by Theorem B (ii), we know that p does not divide R^2 and d. Furthermore, since $\sqrt{p}|V'_r$, we know $\sqrt{p} \nmid N'$. Thus $p \nmid Nd$, $p|U_{2r}$, U_{2t}. By Theorem 2, it follows that

$\{a_{rn}\}$ (resp. $\{a_{tn}\}$) contains at most three occurrences of d, and so $m(d) \leqslant 4$ (resp. 5). Thus we are reduced to the case where

$$V'_r = \varepsilon' 2^k \quad \text{and} \quad V'_t = \varepsilon'' 2^u,$$

where $\varepsilon', \varepsilon'' = \pm 1$ and $2k, 2u \in \boldsymbol{Z}$.

If M is odd, then since N is even, the recurrence relation (3) implies that V_n is odd for all $n > 0$, and so V'_r and V'_t are both ± 1 which contradicts Lemma 1. Thus M is even, $2|(M, N)$, and $2 \| t/r$. By (4) and the fact that $t/2r$ is odd, we have $V'_{2r}|V'_t$. So $V'_{2r} = \varepsilon''' 2^m$ where $m \in \boldsymbol{Z}$ and $\varepsilon''' = \pm 1$. Also by (4), $V'_{2r} = (V'_r)^2 - 2N'^r$ and so

$$\varepsilon''' 2^m = 4^k - 2N'^r.$$

By (4), $(\beta_1 - \beta_2)U'_r + 2\beta_2^r = V'_r$ and so $k > 0$ since $\sqrt{2}|U'_r$. Therefore $m \geqslant 1$ and we have

$$\varepsilon''' 2^{m-1} = 2^{2k-1} - N'^r.$$

Since $2|(M, N)$, by the choice of R, we have N' odd. So either $m = 1$ or $k = 1/2$, and we have a solution to the Catalan Equation: $x^n \pm y^m = 1$. By a result of LeVeque [9], [4] and the facts that $r \geqslant 2$, we see that the only possible solutions are given by the following table:

$k = 1/2$	$m = 1$	$\varepsilon''' = 1$	$N'^r = 0$	
$k = 1/2$	$m = 2$	$\varepsilon''' = 1$	$N'^r = -1$	
$k = 1/2$	$m = 4$	$\varepsilon''' = -1$	$N' = 3$	$r = 2$
$k = 1$	$m = 1$	$\varepsilon''' = 1$	$N'^r = 1$	
$k = 2$	$m = 1$	$\varepsilon''' = -1$	$N' = 3$	$r = 2$

The first two and the fourth cases are impossible since they imply that the discriminant $V_{2r}^2 - 4N^{2r} = R^{4r}(4^m - 4N'^{2r})$ of β_t^{2r} is non-negative contrary to assumptions. The third case also does not occur since on the one hand $V'_r = \varepsilon' \sqrt{2}$ and on the other $V'_r = V'_2 = M'^2 - 2N' \in \boldsymbol{Z}$. In the fifth case, $\varepsilon' 4 = V'_r = V'_2 = M'^2 - 2N' = M'^2 - 6$ and so $M' = \pm\sqrt{2}$ or $\pm\sqrt{10}$.

If $M' = \pm\sqrt{10}$, $N' = 3$, and $r = 2$, then $10r|t$. So there are at most two occurrences of d in $\{a_n\}$ which are not in $\{a_{10rn}\}$. Using (3), one can verify that $V'_{5r} = V'_{10} = -236 \equiv 0 \pmod{59}$. Now $\{a_{10n}\}$ satisfies

$$a_{10(n+2)} = V_{10} a_{10(n+1)} - N^{10} a_{10n},$$

and $59 \nmid N$ since $N' = 3$ and $U'_r = U'_2 = M' = \pm\sqrt{10}$. Also $59|U_{20} = V_{10}U_{10}$. Applying Theorem 2 with $p = 59$ to the sequence $\{a_{10n}\}$ then shows that there are at most three occurrences of d in the sequence, and therefore $m(d) \leqslant 5$.

If $M' = \pm\sqrt{2}$, $N' = 3$, and $r = 2$, then $M'^2 - 4N' = -10 \equiv 0 \pmod 5$. Also $5 \nmid R$ since $5 \nmid U'_r = U'_2 = \pm\sqrt{2}$. So $5 \| M^2 - 4N$. By Theorem A (iii) and (iv), we conclude that $m(d) \leqslant 4$. This completes the proof of Theorem 6.

References

[1] R. Alter and K. K. Kubota, *Multiplicities of second order linear recurrences* Trans. Amer. Math. Soc. 178 (1973), pp. 271–284.

[2] R. Apéry, *Sur une équation diophantienne*, Comptes Rendus, Paris, 251 (1960), pp. 1263–1264.

[3] Z. Borevič and I. R. Šafarevič, *Number Theory*, Academic Press, New York 1966.

[4] J. W. S. Cassels, *On the diophantine equation* $a^x - b^y = 1$, Amer. J. Math. 75 (1953), pp. 159–162.

[5] P. Chowla, S. Chowla, M. Dunton, and D. J. Lewis, *Some diophantine equations in quadratic number fields*, Det. Kong. Norske Videnskabers Selskabs Forhandlinger 31 (1958), pp. 181–183.

[6] S. Chowla, M. Dunton, and D. J. Lewis, *Linear recurrences of order two*, Pacific J. Math. 11 (1961), pp. 833–845.

[7] R. R. Laxton, *Linear recurrences of order two*, J. Austral. Math. Soc. 7 (1967), pp. 108–114.

[8] D. H. Lehmer, *An extended theory of Lucas functions*, Ann. of Math. 31 (1930), pp. 419–448.

[9] W. J. LeVeque, *On the equation* $a^x - b^y = 1$, Amer. J. Math. 74 (1952), pp. 325–331.

[10] D. J. Lewis, *Diophantine equations: p-adic methods*, Studies in Number Theory, Math. Assoc. of Amer., Washington, D. C., 1969.

[11] E. Lucas, *Théorie des fonctions simplement périodiques*, Amer. J. Math. 1 (1878), pp. 184–240.

[12] K. Mahler, *Eine arithmetische Eigenschaft der Taylor-koeffizienten rationaler Funktionen*, Proc. Amsterdam Acad. 38 (1935), pp. 50–60.

[13] T. Nagell, *The Diophantine equation* $x^2 + 7 = 2^n$, Norsk Mat. Tidsskr. 30 (1948), pp. 62–64; Ark. f. Mat. 4 (1960), pp. 185–187.

[14] 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), pp. 663–669.

[15] M. F. Smiley, *On the zeros of a cubic recurrence*, Amer. Math. Monthly 63 (1956), pp. 171–172.

[16] R. Strassman, *Über der Wertevorrat von Potenzreihen in Gebiet det p-adischen Zahlen*, J. Reine Angew. Math. 159 (1928), pp. 13–28.

[17] S. B. Townes, *Note on the Diophantine equation* $x^2 + 7y^2 = 2^{n+2}$, Proc. Amer. Math. Soc. 13 (1962), pp. 864–869.

[18] M. Ward, *Prime divisors of second order recurring sequences*, Duke Math. J. 21 (1954), pp. 607–614.

Received on 23. 4. 1975
and in revised form on 30. 12. 1975 (698)

ACTA ARITHMETICA
XXXIII (1977)

On a conjecture of Morgan Ward, II

by

K. K. Kubota (Ann Arbor, Mich.)

1. Introduction. This is a continuation of a study [3] of the number of times an integer d occurs in a sequence $\{a_n\}$ of rational integers satisfying a second order linear recurrence relation

$$a_{n+2} = Ma_{n+1} - Na_n, \quad n \geqslant 0, \quad |a_0| + |a_1| \neq 0$$

where M and N are constant integers.

The multiplicity of such a sequence is the supremum of the numbers $m(d)$ as d ranges through the rational integers. The standard conjecture due to Morgan Ward was that the multiplicity of a second order linear recurrence is either infinite or bounded above by five. This conjecture was verified in [3]. In earlier work [1], it was conjectured that in fact the bound of five could be improved to four, and this was verified in the case where $(M, N) = 1$, [3]. As will be seen, the general case is more troublesome and is the main result of this paper.

THEOREM. *The multiplicity of a second order linearly recurring sequence of rational integers is either infinite or bounded above by four.*

As in the first part of this paper, the proof uses Skolem's p-adic method, the only essential difference being a systematic use of exponential diophantine equations of kinds studied by Nagell and Ljunggren. Knowledge of the exact solution sets of these equations allows one to know the sequences for which certain "good" primes do not exist. Since the solutions are quite rare, the exceptional cases can be dealt with individually.

The proof is divided into several parts. In the next section, several reductions are made and the notation is established. The diophantine equations appear in Section 3; and the next two sections are devoted to several special classes of sequences needed in the proof given in the final section. Because we will constantly be making reference to results in [3], the numbering of lemmas begun there will be continued in this paper; any reference without a bracketed number is either to this paper or to [3].