LINEAR RECURRENCES OF ORDER TWO

S. CHOWLA, M. DUNTON AND D. J. LEWIS

1. Introduction. A sequence of rational integers $\{f(n)\}$ satisfying a relation

$$f(n+k) = \sum_{i=1}^{k} A_i f(n+k-i) , \qquad A_k \neq 0 ,$$

where the A_i are rational integers, is called an *integral linear recurrence of order* k. Given such a linear recurrence and an integer c, one would like to know for what n does $f(n) = c$? In a very few particular instances (e.g. see [2], [6]) this question has been answered, but in general the question is very difficult. A less exacting problem is the determination of upper and lower bounds on the number, $M(c)$, of distinct n for which $f(n) = c$. We shall call $M(c)$ the multiplicity of c in the recurrence.

Much work has been done by C. L. Siegel [4], K. Mahler [3], Morgan Ward [9], [10], [11] and others concerning the multiplicity of 0 and the pattern of the appearance of 0 in the recurrence. Quite often from information on the multiplicity of 0 in one recurrence one can infer a bound on the multiplicity of all integers in another recurrence. However, as much of the information available concerning the zeros of a recurrence is for recurrences satisfying special conditions on the A_i, one cannot always ascertain in this way whether $M(c)$ is bounded.

Define the *multiplicity of a recurrence* as the least upper bound of the $M(c)$, as c ranges over the integers; and say that the multiplicity of the recurrence is *strictly infinite* if for some integer c, $M(c)$ is infinite. We are interested in examining the following questions:

(I) When is the multiplicity of a recurrence finite? When infinite?

(II) If the multiplicity of a recurrence is finite, what is it or at least what is an upper bound for it?

(III) Can the multiplicity of a recurrence be infinite and not strictly infinite?

Here, we confine our attention to recurrences of order 2. In the direction of the above questions, there is a conjecture that for a recurrence of order 2 either the multiplicity is strictly infinite or it is bounded above by 5. We are unable to resolve this conjecture, but we do obtain reasonably satisfactory answers to the questions for all recurrences of order 2 having $(A_1, A_2) = 1$.

Received August 5, 1960. Part of this work was done while the authors received support from the National Science Foundation.

To simplify notation, we set

$$(1) \qquad f(n+2) = Af(n+1) - Bf(n),\ B \neq 0,\ f(0) = a,\ f(1) = b,$$

The case $a = b = 0$ is trivial, hence we assume that not both a and b are 0. Set

$$(2) \qquad \Delta = A^2 - 4B\,,$$

$$(3) \qquad U = \frac{1}{2}A\,, \qquad \Lambda = \frac{1}{4}\Delta\,, \qquad W = \frac{1}{2}(2b - aA) = b - aU\,.$$

We also assume

$$(4) \qquad (a, b) = 1\,.$$

Clearly, this assumption does not affect the multiplicity of the recurrence.

The equation, $z^2 - Az + B = 0$, will be called the *companion equation* of the recurrence.

If p is rational prime and M is a p-adic number, $||\, M\,||_p$ will denote the exponential p-adic valuation of M, i.e. $||\, M\,||_p$ = maximum integer k such that $p^k \mid M$.

The principal result we obtain is the following:

THEOREM 1. *The multiplicity of a linear recurrence of order* 2, *with* $(A, B) = 1$, *is either strictly infinite or it is bounded by a computable integer* $M(A, B, a, b)$. *If the multiplicity is strictly infinite and the recurrence contains at least two distinct integers then the ratio of the roots of the companion equation is a root of unity.*

More specifically, we prove:

THEOREM 2. *If* $\Delta \geqq 0$, *the multiplicity of the recurrence is either strictly infinite or it does not exceed* 3.

THEOREM 3. *If* $\Delta < 0$ *and if there is a prime* p *such that*

$$||\, \Delta\,||_p = \lambda \geqq \begin{cases} 3 \text{ if } p = 2 \\ 2 \text{ if } p = 3, \text{ while } ||\, U\,||_p = 0 \\ 1 \text{ if } p \geqq 5 \end{cases}$$

then the multiplicity of the recurrence is less than p^λ.

Under additional conditions on A, B, a and b one can obtain a smaller upper bound on the multiplicity of the recurrence than p^λ. Some of these special results are indicated in the course of the proof of Theorem 3. The proof of Theorem 3 uses the p-adic method of Skolem as exemplified in [5], [6].

One of us, in another paper, uses these results on the multiplicity

of recurrences to obtain specific bounds on the number of integral solutions x, y of the equation $x^2 + 7M^2 = N^y$.

2. Some basic Formulas. Set $\alpha = (1/2)(A + \Delta^{1/2}) = U + \Delta^{1/2}$, $\beta = (1/2)(A - \Delta^{1/2}) = U - \Delta^{1/2}$; then α and β are the roots of the companion equation. Also $\alpha + \beta = A$, $\alpha\beta = B$; thus α and β are non-zero complex numbers. Set $y = \sum_{n=0}^{\infty} f(n)x^n$; then $y(1 - Ax + Bx^2) = a + (b - aA)x$.

If $\Delta = 0$, then $A = 2M$, $B = M^2$ and

$$y = \sum_{n=0}^{\infty} M^{n-1}\{n(b - aM) + aM\}x^n ,$$

i.e. $f(n) = M^{n-1}\{n(b - aM) + aM\}$. If $M = 1$ and $b = aM$, then $\alpha = \beta = M$, and the multiplicity is strictly infinite. In all other cases $\{f(n)\}$ is strictly monotonic for $n \geqq 1$ and the multiplicity is 1 or 2 as $a \neq b$ or $a = b$.

Henceforth we assume that $\Delta \neq 0$, then $\alpha \neq \beta$ and

$$y = \frac{1}{2}\left\{\frac{a + (2W)\Delta^{-(1/2)}}{1 - \alpha x} + \frac{a - (2W)\Delta^{-(1/2)}}{1 - \beta x}\right\} .$$

Define

$$(5) \qquad s(n) = \alpha^n + \beta^n ; \qquad t(n) = (\alpha^n - \beta^n)/(\alpha - \beta) = (\alpha^n - \beta^n)\Delta^{-(1/2)} .$$

It is easily seen that

$$(6) \qquad \begin{aligned} &s(0) = 2,\ s(1) = A,\ s(n+2) = As(n+1) - Bs(n) \text{ for } n \geqq 0 . \\ &t(0) = 0,\ t(1) = 1,\ t(n+2) = At(n+1) - Bt(n) \text{ for } n \geqq 0 . \end{aligned}$$

Thus the sequences $\{s(n)\}$ and $\{t(n)\}$ are recurrences satisfying the functional relation (1). Set

$$(7) \qquad S(n) = \frac{1}{2}s(n) , \qquad T(n) = t(n)$$

then

$$(8) \qquad \alpha^n = S(n) + T(n)\Delta^{1/2}, \text{ for } n \geqq 0 ,$$

$$(9) \qquad S(n+1) = US(n) + \Delta T(n) \text{ for } n \geqq 0 ,$$

$$(10) \qquad T(n+1) = S(n) + UT(n) \text{ for } n \geqq 0 ,$$

$$(11) \qquad f(n) = aS(n) + WT(n) \text{ for } n \geqq 0 ,$$

$$(12) \qquad f(n) = X\alpha^n + Y\beta^n \text{ for } n \geqq 0, \text{ where}$$

$$X = \frac{1}{2}a + W\Delta^{-(1/2)} \text{ and } Y = \frac{1}{2}a - W\Delta^{-(1/2)} .$$

Any function of the form $F(n) = V\bar{\alpha}^n + Z\bar{\beta}^n$, where $\bar{\alpha}$ and $\bar{\beta}$ are conjugate algebraic integers in a quadratic extension field over the rational

field, satisfies a linear relation of order 2. Now α^m and β^m are algebraic integers in $Q(\Delta^{1/2})$ and so satisfy a quadratic equation $z^2 - A_m z + B_m = 0$, with A_m and B_m being rational integers. It follows that the sequence $f(0), f(m), \cdots, f(mk), \cdots$ satisfies a linear recurrence of order 2 with coefficients A_m and B_m. The same conclusion holds for any sequence $\{f(n_i)\}$, where the $\{n_i\}$ are an arithmetic progression of difference m. For later information we observe that if $A_1 = A$ and $B_1 = B$ then $A_2 = A^2 - 2B$ and $B_2 = B^2$.

Suppose that we have a recurrence of order 2, say $\{f(n)\}$, and suppose that $f(m) = f(m + q) = 0$, with $q \neq 0$. In this situation the subrecurrence $\{f(m + nq)\}$ is a sequence of zeros. Furthermore the system of equations $X\alpha^m + Y\beta^m = 0$, $X\alpha^{m+q} + Y\beta^{m+q} = 0$ has a non-trivial solution for X and Y in $Q(\Delta^{1/2})$ and hence $\alpha^m\beta^{m+q} - \beta^m\alpha^{m+q} = 0$, i.e. $(\alpha/\beta)^q = 1$.

Conversely if α/β is a root of unity, either $M(0) = 0$ or $M(0) = \infty$ and there exists an r such that $f(n) = \alpha^n Y\{(\beta/\alpha)^n - (\beta/\alpha)^r\}$. Also if $|\alpha| \neq 1$, i.e. $B \neq \pm 1$, and α/β is a root of unity then 0 is the only integer that can have infinite multiplicity in the recurrence.

Since X and Y are independent of n, when α and β are roots of unity, the number of values appearing in the recurrence must be finite. Summarizing, we have

THEOREM 4. *If in a recurrence of order* 2, $M(0) \geqq 2$ *then* $M(0) = \infty$ *and the ratio of the roots of the companion equation is a root of unity. If the roots of the companion equation are roots unity the recurrence consists of only a finite number of integers, each appearing infinitely often.*

3. Proof of Theorem 2. In view of previous remarks we may suppose $\Delta > 0$. Then $\alpha \neq \beta$.

If $\alpha = -\beta$ then $A = 0$ and the multiplicity of the recurrence is 1 when $B \neq -1$ and is strictly infinite when $B = -1$. In the latter case $\alpha = \pm 1$. If one of α or β has absolute value 1 and the other does not, the multiplicity of the recurrence is at most 2. For the remainder of this proof we suppose $1 \neq |\alpha| \neq |\beta| \neq 1$.

Set $g(z) = |X||\alpha|^z - |Y||\beta|^z$ and $h(z) = |X||\alpha|^z + |Y||\beta|^z$. Since $\Delta > 0$, we have X and Y are real and $X^2 + Y^2 > 0$, hence $g(z)$ and $h(z)$ are non-constant functions. For if one of them were a constant function then either $X = Y = 0$ or one of α and β has absolute value 1.

Both $g(z)$ and $h(z)$ have continuous derivatives. As $g'(z) = 0$ for at most one value of z, for any given c, $g(z) = c$ for at most two values of z. Furthermore for $z \geqq 0$ either $g(z)$ is monotonic or $g(z)$ does not assume both negative and positive values; hence there is at most one z and one w such that $z \geqq 0$, $w \geqq 0$ and $c = g(z) = \pm g(w)$. Clearly $h(z)$ is a strictly increasing function.

We have

(i) If $XY \geqq 0$, $\alpha \geqq 0$, $\beta \geqq 0$, then $f(n) = \operatorname{sgn}(X)h(n)$.

(ii) If $XY < 0$, $\alpha \geqq 0$, $\beta \geqq 0$, then $f(n) = \operatorname{sgn}(X)g(n)$.

(iii) If $XY \geqq 0$, $\alpha \leqq 0$, $\beta \leqq 0$, then $f(n) = (-1)^n \operatorname{sgn}(X)h(n)$.

(iv) If $XY < 0$, $\alpha \leqq 0$, $\beta \leqq 0$, then $f(n) = (-1)^n \operatorname{sgn}(X)h(n)$.

(v) If $XY \geqq 0$, $\alpha\beta < 0$, then $f(2n) = \operatorname{sgn}(X)h(2n)$ and

$$f(2n+1) = \operatorname{sgn}(X) \operatorname{sgn}(\alpha)g(2n+1) .$$

(vi) If $XY < 0$, $\alpha\beta < 0$, then $f(2n) = \operatorname{sgn}(X)g(2n)$ and

$$f(2n+1) = \operatorname{sgn}(X) \operatorname{sgn}(\alpha)h(2n+1) .$$

Thus, it is easily seen that the multiplicity of the recurrence cannot exceed 3. This completes the proof of Theorem 2.

It is possible to give a second elementary proof of Theorem 2 using a theorem due to M. F. Smiley. Let $\{F(n)\}$ denote a linear recurrence of order 3 satisfying the relation

$$F(n+3) = A_1F(n+2) - A_2F(n+1) + A_3F(n) ,$$

where the A_i are real numbers. Let u, v and w denote the roots of the companion equation. $z^3 - A_1z^2 + A_2z - A_3 = 0$. Smiley [7] proved: *If u, v and w are non-zero real numbers with distinct absolute values then the multiplicity of 0 in the recurrence $\{F(n)\}$ is at most 3.*

Given the recurrence (1) and any integer c, consider the sequence

$$F(n) = f(n) - c = X^n + Y^n - c1^n .$$

This sequence satisfies the relation

$$F(n+3) = (A+1)F(n+2) - (A+B)F(n+1) + BF(n) ,$$

and the companion equation has α, β and 1 as roots and they are real if $\Delta > 0$. If $1 \neq |\alpha| \neq |\beta| \neq 1$, it follows from the quoted theorem of Smiley that $F(n) = 0$, or $f(n) = c$, for at most 3 values of n. The excluded cases are dealt with as in the earlier argument.

4. Construction of p-adic series. In this and the next two sections we assume the hypothesis of Theorem 3.

If E is a p-adic unit and t is a positive integer, we let $\operatorname{ord}_t(E)$ denote the smallest positive integer k such that $E^k \equiv 1 \pmod{p^t}$. Clearly $\operatorname{ord}_t(E)$ is a divisor of $\varphi(p^t)$ and hence $\| \operatorname{ord}_t(E) \|_p < t$. If $p = 2$ and $t \geqq 3$ then $\| \operatorname{ord}_t(E) \|_2 \leqq t - 2$.

We set $K = \operatorname{ord}_\lambda(U)$; and if $p \geqq 5$ we set $H = \operatorname{ord}_1(U)$. It follows that $U^K = 1 + \Delta G$ and $U^H = 1 + pF$, where G and F are p-adic integers. Also $\| H \|_p = 0$, while $\| K \|_p \leqq \lambda - 1 - \rho$, where $\rho = \| 2 \|_p$.

Consequently

$$\alpha^H = (U + \Delta^{1/2})^H = \sum_{i=1}^{H} \binom{H}{i} U^{H-i} \Delta^{(1/2)i}$$

$$(13) \qquad = \left\{U^H + \binom{H}{2} U^{H-2}\Delta + \cdots\right\} + \Delta^{1/2}\left\{HU^{H-1} + \binom{H}{3} U^{H-3}\Delta + \cdots\right\}$$

$$= 1 + p\boldsymbol{D} + \Delta^{1/2}\boldsymbol{E} ;$$

where $\boldsymbol{E}$ is a p-adic unit and $\boldsymbol{D}$ is a p-adic integer. Similarly

$$(14) \qquad \alpha^K = 1 + \Delta\mathfrak{b} + \Delta^{1/2}\mathfrak{a} ,$$

where $\mathfrak{a}$ and $\mathfrak{b}$ are p-adic integers and where

$$|| \mathfrak{a} ||_p = || K ||_p = \mu \leqq \lambda - 1 - \rho ,$$

and

$$\mathfrak{b} \equiv G + \binom{K}{2} U^{K-2} \pmod{p} .$$

If $\mu > \rho$ then $p^{1+\rho} \mid K$ and hence $\left\| \binom{K}{2} \right\|_p > 0$ while $|| G ||_p = 0$; for if $p \mid G$ then $U^K \equiv 1 \pmod{p^{1+\lambda}}$ and hence $U^{(K/p)} \equiv 1 \pmod{p^\lambda}$ contrary to the definition of K. We set $\nu = || \mathfrak{b} ||_p$; and it follows that if $\mu > \rho$ then $\nu = 0$.

Now

$$\alpha^{Hn} = (1 + p\boldsymbol{D} + \Delta^{1/2}\boldsymbol{E})^n = \sum_{i=1}^{n} \binom{n}{i} (p\boldsymbol{D} + \Delta^{1/2}\boldsymbol{E})^i$$

$$= S(Hn) + T(Hn)\Delta^{1/2} ,$$

where

$$S(Hn) = 1 + np\boldsymbol{D} + \binom{n}{2}(p^2\boldsymbol{D}^2 + \Delta\boldsymbol{E}^2) + \cdots$$

$$= 1 + \sum_{i=1}^{n} \binom{n}{i} D_i^* ,$$

and

$$T(Hn) = n\boldsymbol{E} + \binom{n}{2} 2p\boldsymbol{D}\boldsymbol{E} + \cdots$$

$$= \sum_{i=1}^{n} \binom{n}{i} E_i^* .$$

The D_i^* and E_i^* are p-adic integers independent of n, and

$$|| D_i^* ||_p \geqq [(i+1)/2]; \quad || E_i^* ||_p \geqq [i/2] , \qquad (i = 1, 2, \cdots, n) .$$

By induction, using (9) and (10), we obtain

$$(15) \qquad S(Hn + r) = L_r + \sum_{i=1}^{n} \binom{n}{i} (L_r D_i^* + K_r E_i^*) , \qquad (0 \leqq r < H) ,$$

$$T(Hn + r) = K_r + \sum_{i=1}^{n} \binom{n}{i} (L_r E_i^* + K_r D_i^*) , \qquad (0 \leqq r < H) , \tag{16}$$

where

$$L_r \equiv U^r \pmod{p^\lambda} \text{ and } K_r \equiv r U^{r-1} \pmod{p^\lambda} . \tag{17}$$

Let

$$J_r = aL_r + WK_r , \qquad I_r = a\Delta K_r + WL_r . \tag{18}$$

Then by (11) we obtain

$$\begin{aligned} f(Hn + r) &= J_r + \sum_{i=1}^{n} \binom{n}{i} (D_i^* J_r + E_i^* I_r) , && (0 \leqq r < H) , \\ &= J_r + \sum_{i=1}^{n} n(n-1) \cdots (n-i+1) M_i^* , && (0 \leqq r < H) , \end{aligned} \tag{19}$$

where the M_i^* are p-adic numbers independent of n.

Similarly, we obtain

$$\begin{aligned} \alpha^{Kn} &= (1 + \Delta\mathfrak{b} + \Delta^{1/2}\mathfrak{a})^n = \sum_{i=0}^{n} \binom{n}{i} (\Delta\mathfrak{b} + \Delta^{1/2}\mathfrak{a})^i \\ &= S(Kn) + T(Kn)\Delta^{1/2} , \end{aligned}$$

where

$$\begin{aligned} S(Kn) &= 1 + \sum_{i=1}^{n} \binom{n}{i} D_i , \\ T(Kn) &= \sum_{i=1}^{n} \binom{n}{i} E_i , \end{aligned}$$

with

$$\begin{aligned} D_i &= \sum_{j=0}^{\infty} \binom{i}{2j} \mathfrak{b}^{i-2j} \Delta^{i-j} \mathfrak{a}^{2j} , \\ E_i &= \sum_{j=0}^{\infty} \binom{i}{2j+1} \mathfrak{b}^{i-2j-1} \Delta^{i-j-1} \mathfrak{a}^{2j+1} , \end{aligned} \tag{20}$$

In particular, we have

$$D_1 = \mathfrak{b}\mathfrak{a}, \; E_1 = \mathfrak{a}, \; D_2 = \mathfrak{b}^2\Delta^2 + \Delta\mathfrak{a}^2, \; E_2 = 2\mathfrak{a}\mathfrak{b}\Delta . \tag{21}$$

Let $\chi = \min(2\nu + \lambda, 2\mu)$, then

$$\begin{aligned} \| D_i \|_p &\geqq [(i+1)/2]\lambda + [i/2]\chi , \\ \| E_i \|_p &\geqq [i/2]\lambda + [(i-1)/2]\chi + \mu . \end{aligned}$$

Again using (11) we obtain

$$(22)\quad f(nK+r) = J_r + \sum_{i=1}^{n}\binom{n}{i}(D_iJ_r + E_iI_r)$$
$$= J_r + \sum_{i=1}^{n} n(n-1)\cdots(n-i+1)M_i\,, \qquad (0 \leqq r < K)\,.$$

Since the D_i and E_i are independent of n so are the M_i.

5. Properties of the the p-adic series. Let $1 \leqq v = \sum_{j=0}^{r} b_j p^j$, where the b_j are rational integers such that $0 \leqq b_j < p$, then

$$\| v! \|_p = \sum_{i=1}^{\infty}[v/p^i] = \sum_{i=1}^{r}\sum_{j=i}^{r} b_j p^{j-i} = \sum_{j=i}^{r} b_j \sum_{i=1}^{j} p^{i-1}$$
$$= \sum_{j=1}^{r} b_j(p^j-1)/(p-1) = \Big(v - \sum_{j=0}^{r} b_j\Big)\Big/(p-1)\,.$$

Let

$$G(p,e,k) = ke - \| (2k+1)! \|_p\,,$$
$$G\#(p,e,k) = (k-1)e - \| (2k)! \|_p\,,$$
$$H(p,e,k) = \begin{cases} ke - 2k(p-1)^{-1} & \text{if } p \geqq 3\,, \\ ke - 2k + 1 & \text{if } p = 2\,. \end{cases}$$

If p is odd and $2k = \sum_{j=0}^{r} b_j p^j$ then $\sum_{j=0}^{r} b_j p^j \geqq 2$; hence for p odd,

$$G(p,e,k) \geqq ke - 2k/(p-1) = H(p,e,k)$$

and $G\#(p,e,k) \geqq (k-1)e - 2(k-1)/(p-1) = H(p,e,k-1)$. While for $p = 2$, $G(2,e,k) = e + G\#(2,e,k)$ and $G(2,e,k) \geqq H(2,e,k)$.

If $p \geqq 5$ and $e \geqq 1$ then $(p-1)e - 2 \geqq (p-3)e$; while if $p = 3$ and $e \geqq 2$ then $(p-1)e - 2 \geqq (p-2)e = e$. Hence

(i) If $p \geqq 7$ and $e \geqq 1$ then $H(p,e,k) > e$ for $k \geqq 2$.

(ii) If $e \geqq 1$ then $H(5,e,2) = 2e - 1 \geqq e$ and $H(5,e,k) > e$ for $k \geqq 3$.

(iii) If $e \geqq 2$ then $H(3,e,2) = 2(e-1) \geqq 2$ and $H(3,e,k) > e$ for $k \geqq 3$.

(iv) If $e \geqq 3$ then $H(2,e,k) \geqq k+1$ if $k \geqq 1$ and in particular $H(2,e,k) > e$ if $k \geqq e$.

(v) $H(p,\lambda,k) > 0$ for all primes p and all positive k.

We say that the subrecurrence $\{f(nK+r)\}$ has property P_d if there exists a positive integer q and polynomial $Q(n)$ of degree d over the p-adic integers having some coefficient other than the constant term which is not divisible by p^q and such that all the polynomials

$$f(nK+r) - Q(n)$$

are polynomials whose coefficients are divisible by p^q.

Suppose $\| W \|_p = 0$; then $\| I_r \|_p = 0$ for all r. If $p \geqq 5$ then $\| M_1^* \|_p = 0$ while $\| M_1^* \|_p \geqq H(p,1,[i/2]) > 0$ for $i \geqq 2$. Hence each of

the subrecurrences $\{f(nH + r)\}$, $(r = 0, 1, \cdots, H - 1)$ have property P_1. If $p = 2$ or 3 then $|| M_1 ||_p = \mu < \lambda - \rho$, while $|| M_2 ||_p \geqq \lambda - \rho$ and $|| M_i ||_p \geqq \mu + [i/2]\lambda - || i! ||_p \geqq \mu + H(p, \lambda, [i/2]) > \mu$ for $i \geqq 3$. So in this case each of the subrecurrences $\{f(nK + r)\}$, $(r = 0, 1, \cdots, K - 1)$ have property P_1.

Since $(a, b) = 1$ and $|| U ||_p = 0$, if $|| W ||_p > 0$ then $|| a ||_p = 0$ and hence $|| J_r ||_p = 0$ for all r. Set $\tau = || W ||_p$ then $|| I_r ||_p \geqq \min(\lambda, \tau)$. For the remainder of this section we assume that $\tau > 0$.

It is impossible that for some r, $M_1 = M_2 = 0$. For suppose such were the case, then we have that

$$\mathfrak{b}\Delta J_r + \mathfrak{a} I_r = 0, \quad (\mathfrak{b}^2\Delta^2 + \Delta\mathfrak{a}^2)J_r + 2\mathfrak{a}\mathfrak{b}\Delta I_r = 0 .$$

Multiplying the first equation by $2\mathfrak{b}\Delta$ and subtracting from the second gives $(\mathfrak{a}^2 - \mathfrak{b}^2\Delta)\Delta J_r = 0$. Now $\Delta \neq 0$ and J_r being a p-adic unit is non-zero, therefore $\mathfrak{a}^2 = \mathfrak{b}^2\Delta$; as $\mathfrak{a} \neq 0$, it follows that $\mathfrak{b} \neq 0$. Then

$$\mathfrak{a}^2 I_r^2 = \mathfrak{b}^2\Delta I_r^2 = \mathfrak{b}^2\Delta^2 J_r^2 ,$$

and so $I_r^2 = \Delta J_r^2$ yielding $(a^2\Delta - W^2)(L_r^2 - K_r^2\Delta) - 0$ As L_r is a p-adic unit the second factor is non-zero and hence $a^2\Delta = W^2$, contrary to the assumption that $\Delta < 0$.

Suppose $\lambda \leqq \tau$ and so $|| I_r ||_p \geqq \lambda$, If $\lambda \leqq 2(\mu - \nu)$ then $\mu + \rho < \lambda \leqq 2\mu$; hence $\mu > \rho$ and $\nu = 0$ and thus $\chi = \lambda$. It follows that $|| M_1 ||_p = \lambda$, $|| M_i ||_p \geqq \{[(i + 1)/2] + [i/2]\}\lambda - || i! ||_p > \lambda$ for $i \geqq 2$; and hence the recurrences $\{f(nK + r)\}$ have property P_1. If $\lambda > 2(\mu - \nu)$ then $\chi = 2\mu$ and $|| M_2 ||_p = 2\mu + \lambda - \rho$ while $|| M_i ||_p \geqq \lambda + 2\mu + H(p, \lambda, [i/2]) > \lambda + 2\mu$ for $i \geqq 3$; hence the subrecurrences $\{f(nK + r)\}$ have property P_2.

Suppose $1 \leqq \tau < \lambda$, then $|| I_r ||_p = \tau$. If $\mu = 0$ then $|| M_1 ||_p = \tau < \lambda$, $|| M_2 ||_p = \lambda - \rho$, $|| M_i ||_p \geqq \tau + H(p, \lambda, [i/2]) > \tau$ for $i \geqq 3$; hence the subrecurrences $\{f(nK + r)\}$ have property P_2. If $p = 2$ and $\mu = \rho = 1$, then $\chi = 2$ and $|| M_2 ||_p = \lambda + 1$, while $|| M_i ||_p > \lambda + 1$ for $i \geqq 3$; hence the subrecurrences once again have property P_2.

Now suppose that $1 \leqq \tau < \lambda$ and $\mu > \rho$; then $\nu = 0$ and since $\lambda < \mu + \rho$ we have $\chi \geqq 2 + 2\rho$ and $|| M_i ||_p > \lambda$ for $i \geqq 2$. If $|| M_1 ||_p \leqq \lambda$ for $i \geqq 2$ then the $(f(nK + r)\}$ have property P_1. If $|| M_1 ||_p > \lambda$ then $\mu + \tau = \lambda$ and $|| M_i ||_p \geqq 2\lambda + H(p, 2 + 2\rho, [i/2]) > 2\lambda$ for $i \geqq 3$. If $|| M_2 ||_p \leqq 2\lambda$, then $\{f(nK + r)\}$ have property P_2. If $|| M_1 ||_p > \lambda$ and $|| M_2 ||_p > 2\lambda$ then since M_1 and M_2 are not both zero, $1 \leqq \gamma = \min(|| M_1 ||_p - \lambda, || M_2 ||_p - 2\lambda)$ exists. Also in this case

$$|| \mathfrak{a}^2 - \mathfrak{b}^2\Delta ||_p \geqq \lambda + \gamma ,$$

hence $2\mu = \lambda$, and $\mu = \tau$. One easily computes that $I_r^2 \equiv \Delta J_r^2 \pmod{p^{\lambda+\gamma}}$, and $I_r\mathfrak{a} + J_r\Delta\mathfrak{b} \equiv 0 \pmod{p^{\lambda+\gamma}}$. Combining these facts and relation (20) we obtain

$$(k!)M_k \equiv (J_r\mathfrak{a} + I_r\Lambda\mathfrak{b})(2^{k-1}\mathfrak{b}^{k-1}\Lambda^{k-1}) \equiv 0 \pmod{p^{k\lambda+\gamma}}$$

for $k \geqq 3$. Now

$$k\lambda + \gamma - \| k! \|_p \geqq 2\lambda + \gamma + H(p, \lambda, [k/2]) > 2\lambda + \gamma ,$$

for $k \geqq 3$. Thus it follows that the subrecurrences have property P_2.

If a recurrence has property P_1 it certainly possesses property P_2. Thus we have proved:

Assuming the hypothesis of Theorem 3 *the subrecurrences* $\{f(nK+r)\}$ *have property* P_1 *when* $\| W \|_p = 0$ *and they have property* P_2 *when* $\| W \|_p > 0$.

6. Proof of Theorem 3. Let x be an indeterminate and consider the polynomial

$$F_{n,r}(x) = \sum_{i=0}^{n} M_i x(x-1)\cdots(x-i+1) ,$$

i.e. $F_{n,r}(x)$ is the polynomial obtained by replacing the n in the expansion (22) for $f(nK + r)$ by x. If the subrecurrence $\{f(nK + r)\}$ has property P_d, then for each integer c,

$$F_{n,r}(x) - c \equiv Q_{n,r,c}(x) \pmod{p^q}$$

where $Q_{n,r,c}(x)$ is a polynomial of degree d with p-adic integer coefficients not all of which are divisible by p^q. By a Theorem of Strassman [6], [8], the polynomial equation $F_{n,r}(x) - c = 0$ has at most d p-adic integer solutions, hence at most d rational integer solutions.

Since the M_i are independent of n, when $j \geqq 0$,

$$F_{n+j,r}(x) = F_{n,r}(x) + (x-n)H_{n,j,r}(x) ,$$

where $H_{n,j,r}(x)$ is a polynomial with p-adic integer coefficients. Thus if $F_{n,r}(n) = c$ then $F_{n+j,r}(n) = c$ for all $j \geqq 0$.

If $n_1 < n_2 < \cdots < n_d < n_{d+1}$ are positive integers such that $f(n_iK+r)=c$, $(i = 1, 2, \cdots, d+1)$, then $F_{n_{d+1},r}(x) = c$ has $d+1$ rational integer solutions, contrary to the Theorem of Strassman. Thus if the subrecurrence $\{f(nK + r)\}$ has property P_d then the multiplicity of that subrecurrence is at most d. Hence, if for each r, the subrecurrences have property P_d then the multiplicity of the recurrence $\{f(n)\}$ is at most Kd.

When $\| W \|_p = \tau > 0$, we have seen that a is a p-adic unit and so $f(nK + r) \equiv aU^r \pmod{p^\varepsilon}$ for every r, here $\varepsilon = \min(\tau, \lambda)$. Let $\gamma = \max(\rho, \varepsilon - 1)$. If

$$f(nK + r) = f(mK + s) = c \text{ for } K > r \geqq s \geqq 0 , \tag{23}$$

then $U^{r-s} \equiv 1 \pmod{p^s}$; consequently $K \mid (r-s)p^{\lambda-1-\gamma}$, and thus either $r = s$ or $K > r \geqq s + Kp^{\gamma+1-\lambda} > s \geqq 0$. Hence if $\tau \geqq \lambda$ and (23) holds then $r = s$. While if (23) holds and $1 \leqq \tau < \lambda$ then c is a unit and can appear in at most $p^{\lambda-\gamma-1}$ subrecurrences. Thus we have—*If all the subrecurrences* $\{f(nK+r)\}$ *have the property* P_1 *the multiplicity of* $\{f(n)\}$ *is at most* $K < p^\lambda$, *while if some of the subrecurrences have property* P_2 *and not* P_1 *then* $\| W \|_p = \tau > 0$ *and the multiplicity of the recurrence* $\{f(n)\}$ *is at most* $2p^{\lambda-\gamma-1} < 2p^{\lambda-1-\rho} < p^\lambda$. This completes the proof of Theorem 3.

We have also shown:

THEOREM 5. *If* $A^2 - 4B < 0$ *and there exists a prime* $p \geqq 5$ *such that* $\| A^2 - 4B \|_p > 0$, $\| A \|_p = 0$, $\| 2b - aA \|_p = 0$ *then the multiplicity of the recurrence* (1) *is at most* $H < p - 1$.

COROLLARY 1. *If* $A^2 - 4B < 0$ *and there is a prime* $p \geqq 5$ *such that* $\| A^2 - 4B \|_p > 0$, $\| A \|_p = 0$ *then the multiplicity of the recurrence* $\{T(n)\}$ *defined in* (7) *is at most* $p - 1$.

In specific cases we can compute the H and the K and often obtain a bound on the multiplicity which is lower than $p-1$ or p^λ, e.g. if $A = 1$, $B = 2$, $a = 0$, $b = 1$ then $A^2 - 4B = 7$ and $K = 3$; in this case the multiplicity is exactly 3, see [6].

Futhermore, we have shown:

THEOREM 6. *If* $A^2 - 4B < 0$ *and if there exists a prime* p *such that*

$$\left\| \frac{1}{2}(2b - aA) \right\|_p \geqq \left\| \frac{1}{4}(A^2 - 4B) \right\|_p = \lambda \geqq \begin{cases} 3 & \text{if } p = 2 \\ 2 & \text{if } p = 3 \\ 1 & \text{if } p \geqq 5 \end{cases}$$

and $\| (1/2)A \|_p = 0$, *then the multiplicity of the recurrence* $\{f(n)\}$ *defined by* (1) *is at most* 2.

The result of Miss P. Chowla [1] is a special case of the above theorem.

7. Some special results.

THEOREM 7. *If there exists a prime* p *such that* p *divides* A *and* p *does not divide* B *then the multiplicity of a recurrence* $\{f(n)\}$ *defined by* (1) *is finite and is bounded by a function depending on* A, B, a *and* b.

Proof. Recall that the subrecurrences $\{f(2n)\}$ and $\{f(2n+1)\}$ satisfy the relation

$$f(2n+4+i) = A_2 f(2n+2+i) - B_2 f(2n+1)\,, \qquad i = 0 \text{ or } 1\,,$$

where $A_2 = A^2 - 2B$, $B_2 = B^2$ and $\Delta_2 = A^2\Delta$. If p is an odd prime divisor of A which does not divide B then $|| \Delta_2 ||_p \geqq 2 || A ||_p \geqq 2$ and $|| A_2 ||_p = 0$. If 2 divides A and does not divide B then $\Delta = 4(U^2 - B)$ and $|| A_2 ||_2 = 1$ while $|| \Delta_2 ||_2 \geqq || \Delta ||_2 + 2 || A ||_2 \geqq 5$. Thus in either case we can apply Theorem 3 to obtain a bound on the multiplicity of the recurrences $\{f(2n)\}$ and $\{f(2n+1)\}$, and hence of $\{f(n)\}$, in terms of A, B, a, and b.

THEOREM 8. *If there exists a prime p such that $0 < 2 || A ||_p < || B ||_p$ then the multiplicity of a recurrence $\{f(n)\}$ defined by* (1) *is at most* 2 *and only a finite number of integers have a multiplicity of* 2.

Proof. Assuming the hypothesis, one of the following is true.

(i) There exists an integer N such that either

$$|| f(N) ||_p = || A ||_p + || f(N-1) ||_p$$

or

$$|| f(N) ||_p = || B ||_p + || f(N-2) ||_p$$

and

$$|| f(n) ||_p > || A ||_p + || f(n-1) ||_p = || B ||_p + || f(n-2) ||_p$$

for $2 \leqq n < N$.

(ii) $|| f(n) ||_p > || A ||_p + || f(n-1) ||_p = || B ||_p + || f(n-2) ||_p$ for $n \geqq 2$.

In the first case

$$|| f(n) ||_p = \begin{cases} n\{|| B ||_p - || A ||_p\} + || a ||_p & \text{for } 2 \leqq n < N \\ (n-N) || A ||_p + || f(N) ||_p & \text{for } n \geqq N. \end{cases}$$

Thus $f(m) = f(q)$ implies $0 \leqq m < N \leqq q$ and hence the multiplicity is at most 2 and only a finite number of integers have multiplicity 2.

In the second case $|| f(n) ||_p = n\{|| B ||_p - || A ||_p\} + || a ||_p$. for all n, and hence the multiplicity is one.

8. Proof of Theorem 1. We assume that $\{f(n)\}$ is a recurrence defined by (1) with $(A, B) = 1$. In view of Theorem 2 we need only consider the case where $\Delta < 0$. If $|A| \neq 1$, Theorem 7 assures us of the existence of the desired bound. If $|A| = 1$, then $\Delta = 1 - 4B = -3^a C$, where a is non negative integer and C is an odd positive integer prime to 3. If $C > 1$ or if $a \geqq 2$, Theorem 3 provides the desired bound. Now $\Delta \neq -1$, hence the only unresolved case in when $A = \pm 1$ and $\Delta = -3$, whence $B = 1$. The roots of the companion equation are

primitive cube roots of unity when $A = 1$ and are primitive sixth roots of unity when $A = -1$. In each case only a finite number of values appear in the recurrence $\{f(n)\}$ and hence the multiplicity is strictly infinite.

9. A conjecture. We conjecture that the assumption in Theorem 1 that $(A, B) = 1$ is unnecessary. When $(A, B) = D > 1$, it is easily seen that $D^{[n/2]}$ is a factor of $f(n)$ and hence the multiplicity is never strictly infinite. The theorems and methods described in the preceding sections enable one to show that most recurrences have finite multiplicity, nevertheless they do not appear to be adequate to prove the conjecture.

REFERENCES

1. P. Chowla, *A class of diophantine equations*, Proc. National Acad. Science (U. S. A.), **45** (1959), 569-560.
2. P. Chowla, S. Chowla, M. Dunton and D. J. Lewis, *Some diophantine equations in quadratic number fields*, Det. Kong. Norske Videnskabers Selskabs Fordhandlinger, **31** (1958), Nr. 39, 181-183.
3. K. Mahler, *Eine arithmetische Eigenshaft der Taylor-koeffizienten rationaler Funktionen*, Proc. Amsterdam Acad., **38** (1935) 50-60.
4. C. L. Siegel, *Über die Koeffizienten in der Taylorschen Entwicklung rationaler Funktionen*, Tohoku Jul., **20** (1921), 26-31.
5. Th. Skolem, *Ein Verfahren zur Behandlung gewisser exponentialer Gleichungen und diophantischer Gleichungen*, 8de Skand. Mat. Kongr. Forh., Stockholm, (1934), 163-188.
6. 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.
7. M. F. Smiley, *On the zeros of a cubic recurrence*, Amer. Math. Monthly, **63** (1956), 171-172.
8. R. Strassman, *Über den Wertevorrat von Potenzreihen im Gebeit det p-adischen Zahlen*, J. Reine Angew. Math., **159** (1928), 13-28.
9. Morgan Ward, *Note on an arithmetical property of recurring series*, Math. Zeitschr., **39** (1934), 211-214.
10. ———, *On the vanishing of the sum of the N-th powers of the roots of a cubic equation*, Amer. Math. Monthly, **41** (1934), 313-316.
11. ———, *On the number of vanishing terms in an integral cubic recurrence*, Amer. Math. Monthly, **62** (1955), 155-160.

UNIVERSITY OF COLORADO
UNIVERSITY OF NOTRE DAME