ON THE MULTIPLICITY OF LUCAS SEQUENCES

K. K. KUBOTA

UNIVERSITY OF KENTUCKY
LEXINGTON, KENTUCKY

A Lucas sequence of the first kind is a sequence \( \{U_n\} \) of rational integers satisfying a linear recurrence relation

\[
U_{n+2} = M U_{n+1} - N U_n, \quad U_0 = 0, \quad U_1 = 1
\]

where \( M \) and \( N \) are relatively prime integer constants. The recurrence \( \{U_n\} \) is called non-degenerate if the roots and the ratio of the roots of the companion polynomial \( X^2 - MX + N = 0 \) are non-zero non-roots of unity. The multiplicity of \( \{U_n\} \) is the supremum taken over all integers \( c \) of the number \( m(c) \) of times the integer \( c \) occurs in \( \{U_n\} \).

In [4], it was shown that with the single exception of the Lucas sequence of multiplicity 4 corresponding to \( M = -1 \) and \( N = 2 \), non-degenerate Lucas sequences of the first kind have multiplicity at most three. This will be sharpened as follows.

**Theorem.** - A non-degenerate Lucas sequence of the first kind has multiplicity at most two except in the cases \( M = 1 \), \( N = 3 \) or \( 5 \) and \( M = \pm 1 \), \( N = 2 \).

For applications to exponential diophantine equations, a more useful multiplicity is given by \( m(c) + m(-c) \). The above theorem can be made more precise in the following way.

**Theorem.** - If \( c \neq \pm 1 \), then for every non-degenerate Lucas sequence, one has the inequality

\[
m(c) + m(-c) \leq 2
\]

If \( M = \pm 1 \), the same inequality holds for \( c = 1 \) except in the cases \( N = 2, 3, \) and \( 5 \). If \( M \neq \pm 1 \), then \( m(1) + m(-1) \leq 3 \), and inequality (2) holds with \( c = 1 \) provided that \( N \neq 2 \pmod{48} \).
In the cases $M = 1$, $N = 2,3,5$, the multiplicity of all integers occurring more than once in $\{U_n\}$ has been determined [1,12]. These results will be generalized for various infinite classes of Lucas sequences. Amongst others, the following results will be shown.

**Theorem.** Let $\{U_n\}$ be a non-degenerate Lucas sequence of the first kind satisfying Eq. (1) with $M^2 - 4N < 0$ and $N \neq 2,3,5$. If $M = -1$, then the sequence $\{U_n\}$ is of multiplicity one. If $M = 1$, then $U_1 = U_2 = 1$ are the only occurrences of $1$ and no other integer occurs more than once in $\{U_n\}$.

**Theorem.** Let $\{U_n\}$ be a non-degenerate Lucas sequence of the first kind satisfying Eq. (1) with $M^2 - 4N < 0$. Then $\{U_n\}$ is of multiplicity one in each of the following cases.

(i) $M \equiv 3$ or $5 \pmod{8}$ and $N \equiv 1 \pmod{8}$

(ii) $2|M$ and $N \equiv 1 \pmod{8}$

(iii) $4|M$ and $N \equiv 3 \pmod{8}$

$8|M$ and $N \equiv 7 \pmod{16}$ .

The above results, and especially their more precise forms given below yield by a standard translation [6,1], results on the existence and uniqueness of solutions of certain kinds of exponential diophantine equations. One might mention in particular that assertion (c) above suffices to prove a conjecture of Lewis [6, p. 1068] to the effect that the equation $X^2 + 7 = N^2$ where $N$ is a fixed odd integer, has at most one solution.
1. Preliminaries.

A number of definitions and formulas essential to the subsequent argument are collected together in this section. Recall that a second order linear recurrence is a sequence \( \{ a_n \} \) of rational integers satisfying a recurrence relation

\[
a_{n+2} = M a_{n+1} - N a_n, \quad |a_0| + |a_1| > 0
\]

where \( M \) and \( N \) are integer constants which except where otherwise noted are assumed relatively prime. A Lucas sequence of the second kind is a second order linear recurrence satisfying

\[
v_{n+2} = M v_{n+1} - N v_n, \quad v_0 = 2, \quad v_1 = M.
\]

We denote by \( \beta_1, \beta_2 \) (resp. \( \Delta \)) the roots (resp. discriminant) of the companion polynomial \( x^2 - M x + N = 0 \) and say that the recurrence \( \{ a_n \} \) is non-degenerate if \( \beta_1, \beta_2 \) and \( \beta_1/\beta_2 \) are non-zero non-roots of unity. The multiplicity of \( \{ a_n \} \) and the function \( m(c) \) are defined as in the case of Lucas sequences of the first kind.

An easy induction argument shows that

\[
a_n = A_1 \beta_1^n + A_2 \beta_2^n
\]

for \( n \geq 0 \) where \( A_1 \) and \( A_2 \) are determined by the system of equations

\[
A_1 + A_2 = a_0, \quad A_1 \beta_1 + A_2 \beta_2 = a_1.
\]

In particular, one has

\[
v_n = \frac{\beta_1^n - \beta_2^n}{\beta_1 - \beta_2},
\]
(8) \[ V_n = \beta_1^n + \beta_2^n \]

for all \( n \geq 0 \); from these, we derive

(9) \[ \beta_1^n - \beta_2^n = U_n \sqrt{\Delta} \]

(10) \[ \beta_i^n = U_n \beta_i - N U_{n-1} \quad \text{for} \quad n > 0 \]

(11) \[ V_n = M U_n - 2 N U_{n-1} \]

where the square root is chosen so that \( \sqrt{\Delta} = \beta_1 - \beta_2 \).

An induction argument using the recurrence relation (3) shows

(12) \[ a_{n+m} = U_m a_{n+1} - N U_{m-1} a_n \]

for all \( n \geq 0 \), \( m \geq 1 \) where \( \{U_m\} \) is the Lucas sequence of the first kind satisfying the same linear recurrence relation as does \( \{a_n\} \). Some useful special cases of this formula are the following

(13) \[ U_{nd+i} = U_{d+1} U_{(n-1)d+i} - N U_d U_{(n-1)d+i-1} \equiv U_{d+1} U_{(n-1)d+i} \]
\[ \equiv \ldots \equiv U_{d+1}^n U_i \pmod{U_d}, \]

(14) \[ U_{nd+1} = U_{d+1} U_{(n-1)d+1} - N U_d U_{(n-1)d} \equiv U_{d+1} U_{(n-1)d+1} \]
\[ \equiv \ldots \equiv U_{d+1}^n \pmod{U_d^2}, \]

and

(15) \[ U_{nd-1} = U_d U_{nd} - N U_{d-1} U_{nd-1} \equiv (-N U_{d-1}) U_{nd-1} \]
\[ \equiv \ldots \equiv (-N U_{d-1})^{n-1} U_{d-1} \pmod{U_d^2} \]

which can be rewritten as
\[ (16) \quad 1 + N U_{n-1} \equiv 1 - (-N U_{d-1})^n \pmod{U_d^2}. \]

The above congruences are consequences of (12) and the following result of Lucas [9].

**Lemma 1.** Let \( \{V_n\} \) (resp. \( \{V_n\} \)) be the Lucas sequence of first (resp. second) kind which satisfies Eq. (1) (resp. Eq. (4)).

(i) For all \( n > 0 \), one has

\[ (U_n, N) = (V_n, N) = 1 \quad \text{and} \quad (U_n, V_n) = 1 \text{ or } 2. \]

(ii) For all \( n, m > 0 \), one has \( (U_n, U_m) = |U_{(m,n)}| \).

(iii) If for some prime \( p \), one has \( p^t \mid U_m, p^u \mid k, t > 0 \), and \( k \geq 0 \), then \( p^{t+u} \mid U_{km} \). If further one has \( p > 2 \), then \( p^{t+u} \mid U_{km} \).

For all integers \( n \geq m \), one has

\[ (17) \quad \frac{U_n^2}{u} = U_{n+m} U_{n-m} + N^{n-m} U_m^2 \]

since by Eq. (9)

\[ \Delta(U_n^2 - U_{n+m} U_{n-m}) = (\beta_1^n - \beta_2^n)^2 - (\beta_1^{n+m} - \beta_2^{n+m})(\beta_1^{n-m} - \beta_2^{n-m}) \]

\[ = -2(\beta_1 \beta_2)^n + \beta_1^{n+m} \beta_2^{n-m} + \beta_1^{n-m} \beta_2^{n+m} = N^{n-m} (\beta_1^m - \beta_2^m)^2 \]

\[ = N^{n-m} \Delta U_m^2. \]

Combining Eqs. (15, 17), one obtains

\[ (18) \quad U_{dn-1}^2 \equiv (-N)^{2(n-1)} U_{d-1}^{2n} \equiv (-N)^{2(n-1)} (U_d U_{d-2} + N^{d-2})^n \equiv N^{nd-2} \pmod{U_d}. \]
The formula
\[ U_n = \sum_{i=0}^{n-1} \binom{n-1}{n-2i-1} M^{n-2i-1} (-N)^i \]
where \( \binom{m}{j} \) is defined to be zero for \( j < 0 \) is useful whenever one needs to express some \( U_n \) as a polynomial in \( M \) and \( N \); it is easily verified using the Pascal triangle identity and Eq. (1). In particular, one has
\[ U_n \equiv M^{n+1} \pmod{N} \]
\[ U_{2n+1} \equiv (-N)^n \pmod{M} \]

If \( r > 0 \) and \( s \geq 0 \) are fixed integers, then \( b_n = a_{rn+s} \) defines a linear recurrence satisfying
\[ b_{n+2} = \sqrt{r} b_{n+1} - N^r b_n, \]
as is easily verified using Eqs. (5, 8) and \( N = \beta_1 \beta_2 \). In particular, the sequences \( \{U_{rn}/r\} \) and \( \{V_{rn}\} \) are Lucas sequences of the first and second kinds respectively. If \( \{a_n\} \) is non-degenerate, then so is \( \{a_{rn+s}\} \) since the roots of the characteristic polynomial \( x^2 - \sqrt{r} x + N^r = 0 \) are just \( \beta_1^r \) and \( \beta_2^r \) by Eq. (8).
2. The \( p \)-adic argument.

The following application of Strassman's Lemma is a refinement of Theorem 1 of \([4]\). The proof does not require \( M \) and \( N \) to be relatively prime.

**Theorem 1.-** Let \( \{a_n\} \) be a non-degenerate rational integer second order linear recurrence satisfying Eq. (3) and \( \{U_n\} \) be the Lucas sequence of the first kind satisfying the same recurrence relation. For \( q \in \mathbb{N}^+ \), \( c \in \mathbb{Z} \), and \( p \) a rational prime not dividing \( N \), set

\[
K = \min (\text{ord}_p U_q, \text{ord}_p (N U_{q-1} + 1))
\]

\[
e = \delta_2 p \quad (\text{Kronecker } \delta).
\]

If \( K > e \), then for each fixed index \( i \) with \( 0 \leq i < q \), the equation

\[
a_{qn+i} = c
\]

has at most one non-negative integer solution \( n \) unless

\[
a_{qm+i} \equiv c \pmod{p^{2K-e}}
\]

for all non-negative integers \( m \).

**Proof.-** With the notation of the last section, one has by the definition of \( K \) and Eq. (10) that \( a_j^1 = U_q b_j - N U_{q-1} \equiv 1 \pmod{p^K} \) for \( j = 1, 2 \). Let \( \delta_j = a_j^1 \). Since \( A_2 b_2^1 = a_1 - A_1 b_1^1 \) by Eq. (5), one has also that
(23) \[ a_{q+n+i} = A_1 \beta_1^i \delta_1^n + A_2 \beta_2^i \delta_2^n \]

\[ = \sum_{j=0}^{\infty} A_1 \beta_1^i \binom{n}{j} (\delta_1 - 1)^j + A_2 \beta_2^i \binom{n}{j} (\delta_2 - 1)^j \]

\[ = a_i + n (a_{q+i} - a_i) + \sum_{j=2}^{\infty} \binom{n}{j} \{ A_1 \beta_1^i (\delta_1 - 1)^j + (a_1 - A_1 \beta_1^i) (\delta_2 - 1)^j \} \]

where \[ h(n) = \sum_{j=2}^{\infty} \binom{n}{j} c_j \]

Now \[ A_1 \beta_1^i \{ (\delta_1 - 1)^j - (\delta_2 - 1)^j \} = \sum_{t=0}^{j-1} (\delta_1 - 1)^{j-t-1}(\delta_2 - 1)^t A_1 (\beta_1 - \beta_2) \beta_1^i U_q \]

since by Eq. (9) one has \[ (\delta_1 - 1) - (\delta_2 - 1) = \beta_1^q - \beta_2^q = (\beta_1 - \beta_2) U_q \]

By Cramer's rule applied to Eq. (6), \[ (\beta_1 - \beta_2) A_j = -1 \beta_1^i \beta_2^j \quad | A_j \in \mathbb{Z} \]

and so it follows that \( p^{K_k} C_k \) for all \( k \geq 2 \). Since \( j ! \binom{n}{j} \) is a polynomial in \( n \) with integer coefficients, it is straightforward to verify that the coefficients of \( h(n) \) considered as a power series in \( n \) are all divisible by \( p^{2K-e} \). The condition \( a_{q+n+i} = c \) can be written

\[ 0 = (a_i - c) + n(a_{q+i} - a_i) + h(n) \]

By Strassman's Lemma [10,11], it follows that the number of solutions of \( a_{q+n+i} = c \) is no more than one unless \( g \)
\[ a_i \equiv a_{q+i} \equiv 0 \pmod{p^{2K-e}}. \]

But then \[ a_{qn+i} \equiv c \pmod{p^{2K-e}} \] for all \( n \geq 0 \) by Eq. (23). This proves Theorem 1.

The next result is a natural analogue of Theorem 2 of [4].

**Theorem 2.** Let \( \{U_n\} \) be a non-degenerate Lucas sequence of the first kind satisfying Eq. (1) with \( \Delta = M^2 - 4N < 0 \). Suppose that for some positive integer \( d \), one has \( p^t \mid U_d \) where \( p \) is a rational prime and \( t > e, e = \delta_{2p} \) (Kronecker delta). Let \( v \) be the multiplicative order of \( -N U_{d-1} \) modulo \( p^{e+1} \), \( p^u \mid (-N U_{d-1})^v - 1 \), and \( c \) be any integer.

(i) If \( u \neq t \) and \( p^t \mid c \), then for each integer \( i \) with \( 0 \leq i < d-1 \) and \( p^t \mid U_{i+1} \) there is at most one occurrence of \( c \) in the subsequence \( \{U_{nd+i}\} \).

(ii) If \( c = 1 \) or \( -1 \) and \( p^{t-2e} \mid N \), then \( c \) occurs at most once in the subsequence \( \{U_{nd-1}\} \).

(iii) The integer \( c \) occurs at most once in each subsequence \( \{U_{dvn+kd}\}, 0 \leq k < v \).

**Proof.** Let \( r \) be the multiplicative order of \( -N U_{d-1} \) modulo \( p^t \) and \( q = dr \). Then \( r = p^w v \) where \( w = \max(0, t-u) \). Further, by Eq. (16) and Lemma 1, the parameter \( K \) of Theorem 1 is at least \( t \). Suppose that \( p \mid c \). If \( p \mid U_i \) for some fixed \( i \), then by Eq. (13) we have \( p \mid U_{dn+i} \) for all \( n \geq 0 \), and so \( c \) does not occur in the subsequence \( \{U_{dn+i}\} \). On the other hand, if \( p \nmid U_i \), then by the same equation and the definition of \( r \), there is for fixed \( i \) at most one integer \( s \) such that \( 0 \leq s < r \) and \( U_{qn+sr+i} \equiv c \pmod{p^t} \) for some and hence all \( n \geq 0 \). For the other values of \( s \), the integer \( c \) cannot occur in \( \{U_{qn+sr+i}\} \).
For the first assertion, one may assume that $p \nmid U_1$. Note that by Eqs. (12,1), one has

\begin{equation}
U_{q+j} - U_j = U_{q+1} U_j - N U_q U_{j-1} - U_j
= (M U_q - N U_{q-1}) U_j - N U_q U_{j-1} - U_j
= (M U_j - N U_{j-1}) U_q - U_j (1 + N U_{q-1})
= U_{j+1} U_q - U_j (1 + N U_{q-1})
\end{equation}

Since $p \nmid U_1$, $U_{1+1}$, one knows that $p \nmid U_{ds+i}$, $U_{ds+i+1}$ by Eq. (13). Further, by Lemma 1 and Eq. (16), one has

$$\text{ord}_p U_q = t + w \neq u + w = \text{ord}_p (1 + N U_{q-1})$$

Therefore, since $w < t - e$, we have by Eq. (24) with $j = ds + i$ that

$$\text{ord}_p (U_{q+ds+i} - U_{ds+i}) = \min(t + w, u + w) < 2t - e \leq 2K - e$$

In particular, $U_{q+ds+i}$ and $U_{ds+i}$ cannot both be congruent to $c$ modulo $p^{2K - e}$, and so by Theorem 1 the integer $c$ can occur at most once in the subsequence $[U_{q+n+ds+i}]$. This proves the first assertion.

For the second assertion, recall that with $i = d - 1$, the integer $s$ was chosen so that $U_{d+1} \equiv c = \pm 1 \pmod{p^t}$. By Eq. (18) with $n = s + 1$, it follows that $N^{d(s+1) - 2} \equiv U_{d+1}^2 \equiv 1 \pmod{p^t}$. Using Eq. (17), one has

$$(-N U_{d-1})^{2(d(s+1)-2)} = (-N)^2 d(s+1) - 2 (U_d U_{d-2} + N^{d-2} d(s+1) - 2)
\equiv (N^{d(s+1) - 2})^d \equiv 1 \pmod{p^t},$$

and so $r | 2(d(s+1) - 2)$. By Theorem 1 applied with $q = rd$, the subsequence
\{U_{q+n+d(s+1)-1}\} can contain more than one occurrence of \(c\) only if

\[U_{d(s+1)-1} \equiv U_{q+d(s+1)-1} \equiv c = \pm 1 \pmod{p^t-e},\]

By Eq. (15), this means

\[(25) \quad (-N)^S U_{d-1}^{s+1} \equiv (-N)^{r+s} U_{d-1}^{r+s+1} \equiv c = \pm 1 \pmod{p^t-e},\]

and so \((-N U_{d-1})^r \equiv 1 \pmod{p^t-e}\). Since \(r|2(d(s+1)-2)\), it follows that

\[(-N U_{d-1})^{2d(s+1)-4} \equiv 1 \pmod{p^t-e}.\]

Combining with Eq. (25) gives \((-N)^{2d-4} \equiv U_{d-1}^{4} \pmod{p^t-e}\), and so by Eq. (17),

\[0 \equiv U_{d-1}^{4} - (-N)^{2d-4} = U_d^2 U_{d-2} + N^{d-2})^2 - N^{2d-4}\]

\[= 2 U_d U_{d-2} N^{d-2} \pmod{p^t-e}.\]

Since \(p \nmid N\) by Lemma 1, it follows that \(p^{t-2e}\) divides \(U_{d-2}\) and so

\[p^{t-2e} | (U_d, U_{d-2}) = |U_{(d, d-2)}| = \left\{ \begin{array}{ll} |U_2| = |M| & \text{if } d \text{ is even} \\ |U_1| = 1 & \text{if } d \text{ is odd} \end{array} \right.\]

which proves the second assertion.

For the third assertion, we need a formula for \(W_{dn} = U_{dn}/U_d\). Let \(V_n\) be the Lucas sequence of the second kind satisfying Eq. (4). By solving Eqs. (8, 9) with \(n = d\), one obtains

\[\beta_1^d, \beta_2^d = \left(\frac{\sqrt{d}}{2}\right) \left(1 \pm \frac{U_d \sqrt{\Delta}}{V_d}\right)\]

and so

\[\beta_1^{dn}, \beta_2^{dn} = \left(\frac{\sqrt{d}}{2}\right)^n \left(1 \pm \frac{U_d \sqrt{\Delta}}{V_d}\right)^n = \left(\frac{\sqrt{d}}{2}\right)^n \sum_{j=0}^{n} \binom{n}{j} \left(\frac{\sqrt{d} \sqrt{\Delta}}{V_d}\right)^j.\]
Therefore by Eq. (7)

\[ W_{dn} = U_{dn}/U_d = \frac{\beta_1^{dn} - \beta_2^{dn}}{\beta_1^d - \beta_2^d} = \frac{V_d}{2} \left( \frac{\Delta}{V_r} \right)^{n-1} \sum_{j=0}^{2j+1} \binom{n}{2j+1} \left( \frac{\Delta}{V_r^2} \right)^j \]

By Eq. (8, 9), one has

\[ V_d = U_d \sqrt{\Delta} + 2 \beta_2^d \equiv 2 \beta_2^d \pmod{p^{e+1}} \]

and \( p \nmid N = \beta_1 \beta_2 \) by Lemma 1; hence \( V_d/2 \) is a \( p \)-adic unit. Let \( \gamma = (V_d/2)^s \) where \( s \) is the multiplicative order of \( V_d/2 \pmod{p^{e+1}} \). For \( k \) fixed in the interval \( 0 \leq k < s \), one has by Eq. (26)

\[ W_{dsn+dk} = (1 + \gamma)^n \left( \frac{V_r}{2} \right)^{k-1} \sum_{j=0}^{sn+k} \binom{sn+k}{2j+1} \left( \frac{\Delta}{V_d^2} \right)^j \]

\[ = \left( \frac{V_r}{2} \right)^{k-1} \left( \frac{sn+k}{V_d^2} \right) + h(n) \]

where, as it is easy to see, \( h(n) \) is a power series in \( n \) convergent at all \( p \)-adic integers and having coefficients all divisible by \( p^{e+1} \). By Strassman's Lemma [11,10], the quantity \( c/U_d \) can occur at most once in each subsequence \( \{ W_{dsn+kd} \} \), \( 0 \leq k < s \).

By Eq. (11), \( V_d/2 = -N U_{d-1} \pmod{p^{t-e}} \) and so \( s = v \) if \( p^t \neq 4 \). This proves assertion (iii) in the case where \( p \geq 3 \). If \( p = s = 2 \), then by Lemma 1, \( p^{t+1} | U_{dn} \) precisely when \( n \) is even. In particular, \( c/U_d \) occurs at most once in \( \{ W_{dsn} \} \cup \{ W_{dsn+d} \} \). Since \( s = 1 \) when \( p = 2 \) and \( s \neq 2 \), we have in the \( p = 2 \) case that \( c \) occurs at most once in \( \{ U_{dn} \} \). This completes the proof of Theorem 2.

For future reference, we restate Theorems 1 and 2 of [4].
Theorem 3.- Let \( \{a_n\} \) be a non-degenerate second order linear recurrence satisfying Eq. (3) with \( M^2 - 4N < 0 \), \( \{U_n\} \) (resp. \( \{V_n\} \)) be the Lucas sequence of first (resp. second) kind satisfying the same linear recurrence relation, and \( \beta_1, \beta_2 \) be the roots of the characteristic polynomial \( \chi^2 - M\chi + N = 0 \). Suppose that \( c \in \mathbb{Z}, p \) is a rational prime not dividing \( N \), and \( \pi \) is a prime element of the completion of the ring of integers of \( \mathbb{Q}(\beta_1) \) at a prime ideal \( \mathfrak{P} \) lying over \( p \).

(i) Suppose \( p = 2 \) and let \( q \) be the least positive integer with

\[
\beta_1^q \equiv \beta_2^q \equiv 1 \pmod{\pi^e}, \quad e = \left\lfloor \frac{e}{p-1} \right\rfloor + 1
\]

where \( e \) is the absolute ramification index of \( \mathfrak{P} \). Then for \( i \) fixed, the equation \( a_{qn+i} = c \) has at most two solutions with \( n \geq 0 \). Further, if the equation has two solutions when \( i = i_1, i_2 \) where \( 0 \leq i_1 < i_2 < q \), then \( q = 2(i_2 - i_1) \).

(ii) Suppose \( p \geq 3, p|U_r, r \geq 1 \), and \( s \) is the multiplicative order of \( V_r/2 \pmod{p} \). Set

\[
\varepsilon = \begin{cases} 
1 & \text{if } p = 3 \text{ and } \beta_1^{rs} - 1 \not\equiv 0 \pmod{3n} \text{ for } i = 1 \text{ or } 2 \\
0 & \text{otherwise }
\end{cases}
\]

If \( p \nmid c \), then with the possible exception of one value of \( i \) in the interval \( 0 \leq i < r \), the equation \( a_{rn+i} = c \) has at most one solution; for the exceptional value of \( i \), it has at most \( 2 + \varepsilon \) solutions.
3.- The real case.

If $M^2 - 4N \geq 0$, then the situation is very simple as we see in the next proposition.

**Proposition 1.** Let $\{U_n\}$ be a non-degenerate Lucas sequence of the first kind satisfying Eq. (1) with $\Delta = M^2 - 4N \geq 0$. For all integers $c$, one has $m(c) + m(-c) \leq 1$ except when $c = \pm 1$ and $M = \pm 1$. In the exceptional case, $m(1) + m(-1) = 2$.

**Proof.** By Eq. (19), it is clear that replacing $M$ with $-M$ leaves $U_{2n+1}$ fixed and changes only the sign of $U_{2n}$. Therefore to prove the result, it suffices to show in the case where $M > 0$ that $U_n$ for $n > 1$ is a strictly increasing function of $n$. Since $\{U_n\}$ is non-degenerate, one has $MN(M^2-4N) \neq 0$.

If $N > 0$, then $\beta_1, \beta_2 = (M \pm \sqrt{\Delta})/2$ are positive real numbers with $\beta_1 > 1$. The function $f(x) = \sqrt{\Delta}^{-1}(\beta_1^x - \beta_2^x)$ has derivative $f'(x) = \sqrt{\Delta}^{-1}(\beta_1^x \log \beta_1 - \beta_2^x \log \beta_2) > 0$ and so is strictly increasing. Since $U_n = f(n)$ by Eq. (7), the assertion is proved in this case.

If $N < 0$, then by Eq. (19) one has $U_n = \sum_{i=0}^{\left\lfloor \frac{n-1}{2} \right\rfloor} \binom{n-1-i}{i} M^{n-1-2i} (-N)^i$, and so it suffices to observe that the $\binom{n-1-i}{i}$ for $i > 0$ and $i \leq \left\lfloor \frac{n-1}{2} \right\rfloor$ are strictly increasing functions of $n$.
4.- Throughout the rest of this paper, it is implicitly assumed that 
\[ \Delta = M^2 - 4N < 0. \]

The next result is a corollary of a theorem of Chowla, Dunton and Lewis [3]; see [4, Lemma 1].

**Lemma 2.-** Let \( \{V_n\} \) be a non-degenerate Lucas sequence of the second kind satisfying Eq. (4) with \( M^2 - 4N < 0 \). Then \( V_n^2 = 1 \) has at most one solution \( n \geq 0 \) except in the case \( M = \pm 1, N = 2 \). In the exceptional case, the only solutions are \( n = 1 \) and 4.

**Lemma 3.-** Let \( c \in \mathbb{N}^+ \) and \( \{U_n\}, \{U'_n\} \) be Lucas sequences of the first kind satisfying

\[
U_{n+2} = M U_{n+1} - N U_n
\]

\[
U'_{n+2} = -M U'_{n+1} - N U'_n
\]

where \( M^2 - 4N < 0 \) and either \( M \neq \pm 1 \) or \( N \neq 2 \).

(i) If \( c \neq 1 \) or \( M \neq \pm 1 \), then at least one of the subsequences \( \{U_{2n}\} \), \( \{U_{2n+1}\} \) contains no number of absolute value \( c \).

(ii) Suppose that both \( c \) and \( -c \) occur at most once each in \( \{U_n\} \). If \( M \neq -1 \) or \( c \neq 1 \), then both \( c \) and \( -c \) occur at most once each in \( \{U'_n\} \). If \( M = -1 = c \), then \( U'_1 = U'_2 = 1 \) are the only occurrences of 1 in \( \{U'_n\} \) and \( -1 \) does not occur in \( \{U'_n\} \).

**Proof.-** If \( M \neq \pm 1 \), then assertion (i) is clear since \( M = U_2 \mid U_n \) precisely when is even by Lemma 1(ii-i). Suppose \( M = \pm 1 \) and \( |U_{2n}| = |U_{2m+1}| = c \). Letting \( k = (2n, 2m + 1) \), one has by Lemma 1 that
\[ c = (U_{2n}, U_{2n+1}) = |U_k| U_{2k} \]

and \( U_{2k} \mid U_{2n} = c \). So \( \pm c = U_{2k} = U_k V_k \) and hence \( V_k = \pm 1 \). By Lemma 2, \( k = 1 \) and \( c = |U_k| = 1 \).

For the second assertion, note that by Eq. (19) one has

\[ U'_n = (-1)^{n-1} U_n \]

for \( n \geq 0 \). Thus \( U_{n+1} = U'_{2n+1} \) and \( U_{2n} = -U'_{2n} \) for \( n \geq 0 \). If \( M \neq \pm 1 \) or \( c \neq 1 \), then the second assertion is therefore a consequence of the first.

If \( M = 1 \), then \( U_1 = U_2 = 1 \) and so the hypothesis of assertion (ii) does not hold when \( c = 1 \). Finally, if \( M = -1 \) and \( c = 1 \), then by hypothesis, \( U_1 = U_2 = 1 \) are the only occurrences of \( \pm 1 \) in \( \{U_n\} \). Therefore, by Eq. (27), \( U'_1 = U'_2 = 1 \) are the only occurrences of \( \pm 1 \) in \( \{U'_n\} \).

**Proposition 2.** Let \( \{U_n\} \) be a non-degenerate Lucas sequence of the first kind satisfying Eq. (1) with \( \Delta = M^2 - 4N < 0 \). Let \( d \in \mathbb{N}^+ \) and \( p \) be a prime with \( p \mid |U_d|, p^u \mid |U_{d-1}|, p^v \mid M \), and \( p^{e+1} \mid U_{d+1} \) where \( e = \delta_{2p} \) is the Kronecker \( \delta \) and \( 2e < r = \min(u,t+v) < 2t \).

(i) If \( u \neq t + v \), then the subsequences \( \{U_{nd+1}\} \) and \( \{U_{nd-1}\} \) both have multiplicity one.

(ii) Let \( h = \max(0,u+1-w-k+e-f) \) where \( p^k \mid d \), and \( f \) is 1 if \( p = 2 \), \( u = t + v \) and 0 otherwise. Then for every \( c \in \mathbb{N}^+ \), at least one of \( c \) and \( -c \) does not occur in the union \( \{U_{np^h d-1}\} \cup \{U_{np^h d+1}\} \).

**Proof.** By Eq. (17), one has for every positive integer \( g \) that

\[ U_{g+1}^2 = U_{g+2} U_{g} + N^g, \quad U_{g-1}^2 = U_{g} U_{g-2} + N^{g-2} \]
and so by the recurrence relation (1),

\[(28) \quad (NU_{g-1}+1) (NU_{g-1}) = N^2 U_{g-1} = N^2 U_{g-2} + N^g - 1\]
\[= -N U_g^2 + N U_{g-1} M U_g + (N^g - 1)\]

\[(29) \quad (U_{g+1} - U_1) (U_{g+1} + 1) = U_{g+1} - 1 = U_{g+2} U_g + N^g - 1\]
\[= -N U_g^2 + U_{g+1} M U_g + (N^g - 1)\]

Further, by Eq. (12),

\[(30) \quad U_{2g-1} - U_{g-1} = U_g^2 - (NU_{g-1} + 1) U_{g-1} .\]

Suppose \( g \) is a multiple of \( d \). Since \( p^{e+1} U_{d+1} \), one has

\[1 + NU_{d-1} \equiv U_{d+1} + NU_{d-1} = MU_{d} \equiv 0 \pmod{p^{e+1}} ,\]

and so by Eq. (16), \( 1 + NU_{g-1} \equiv 0 \pmod{p^{e+1}} \) and \( p^e \parallel NU_{g-1} \). Finally, Eq. (14) and \( p^{e+1} U_{d+1} \) imply \( p^{e+1} U_{g+1} \) and \( p^e \parallel U_{g+1} \).

For assertion (i), let \( g = d \). By Eqs (28, 29, 30) and the assumption that \( u \neq t + v \), one has

\[p^{w-e} \parallel NU_{d+1}, U_{d+1} - U_1, U_{2d-1} - U_{d-1} .\]

Further, the assumption that \( 2e < w < 2t \) implies

\[w - e < 2 \text{ min}(w - e, t) - e ,\]

and so assertion (i) follows from Theorem 1 applied with \( q = d \) and \( K \geq \text{min}(w-e, t) \).

For assertion (ii), let \( g = p^h d \), so that \( p^{h+u} \parallel N^{e-1} \) and \( p^{t+h} \parallel U_g \) by Lemma 1. By Eqs. (28, 29), one has
\[ p^{w+h+f-e} \equiv N U_{g-1} \pmod{U_{g-1}} \]

and so by Eqs. (14, 15) and the fact that \( w+h+f-e \leq 2(t+h) \),

\[ U_{ng+1} \equiv U_{gn} \equiv 1 \pmod{p^{w+h+f-e}} \]

\[ U_{ng-1} \equiv (-N U_{g-1})^{n-1} \equiv U_{g-1} \pmod{p^{w+h+f-e}} \]

for all \( n \). If \( U_{g-1} \equiv -1 \pmod{p^{w+h+f-e}} \), then assertion (ii) follows from these congruences. If \( U_{g-1} \equiv -1 \pmod{p^{w+h+f-e}} \), then

\[ 1 - N \equiv 1 + U_{g-1} N \equiv 0 \pmod{p^{w+h+f-e}} \]

and so \( p^{w+h+f-e+k} \equiv N^{d-1} \). It follows by the definition of \( u \) that

\( w + h + f - e + k \leq u \) which is contrary to the definition of \( h \). This proves the proposition.

Parts (ii) and (iii) of the last theorem stated in the introduction are very

special cases of the next result.

**Corollary 1.** Let \( \{U_n\} \) be a Lucas sequence of the first kind satisfying Eq. (1)

with \( M^2 - 4N < 0 \). Suppose \( 2^s | M \) and \( 2^r | N - c \) where \( c = \pm 1 \), \( r \geq 2 \),

and \( s \geq 1 \).

(i) The subsequence \( \{U_{2n}\} \) is of multiplicity one. If \( r + 1 \neq 2s \), then the

subsequences \( \{U_{4n+1}\} \) and \( \{U_{4n+3}\} \) are also of multiplicity one.

(ii) If \( r < 2s \), then for all \( n \geq 0 \) one has

\[ U_{4n+1} \equiv 1 \pmod{2^{r+1}} \quad \text{and} \quad U_{4n+3} \equiv -c + 2^r \pmod{2^{r+1}} \].

In particular, if \( r + 1 < 2s \), then \( m(c) + m(-c) \leq 1 \) for odd integers \( c \).
(iii) If either \( c = 1 \) and \( r + 1 \neq 2s \) or else \( c = -1 \) and \( r + 1 < 2s \), then
the sequence \( \{U_n\} \) is of multiplicity one.

**Proof.** Apply Proposition 2 with \( p = 2 \) and \( d = 4 \). Since

\[
2^{s+1} \mid U_4 = M(M^2 - 2N), \quad 2^{r+2} \mid N^4 - 1, \quad \text{and} \quad 2^s \mid M,
\]

the parameters are \( t = s + 1 \), \( u = r + 2 \), and \( v = s \). Further,

\[
U_5 = M^4 - 3M^2N + N^2 \equiv 1 \pmod{4}
\]

and \( 2e < w = \min (r + 1, 2s) + 1 < 2t \). Proposition 2 (i) shows that
\( \{U_{4n+1}\} \) and \( \{U_{4n+3}\} \) are of multiplicity one whenever \( r + 1 \neq 2s \).

Theorem 2 (iii) applied with \( d = 4 \), \( v = 1 \) shows that the subsequence
\( \{U_{4n}\} \) is of multiplicity one. By Lemma 1, \( 2^{s+1} \mid U_{2n} \) if and only if \( n \) is even;
hence the subsequences \( \{U_{4n+2}\} \) and \( \{U_{4n}\} \) have no elements in common. To com-
plete the proof of the first assertion, it therefore suffices to show that
\( \{U_{4n+2}\} \) is of multiplicity one. By Eq. (22), the sequence of \( a_n = U_{2n}/U_2 \) is a
Lucas sequence of the first kind satisfying the recurrence relation

\[
a_{n+2} = V_2 a_{n+1} - N^2 a_n, \quad a_0 = 0, \quad a_1 = 1
\]

where \( V_2 = M^2 - 2N \equiv 2 \pmod{4} \) and \( 2^{r+1} \mid N^2 - 1 \). By the last paragraph, it
follows that \( \{a_{4n+1}\} \) and \( \{a_{4n+3}\} \) are each of multiplicity one. Since the se-
quence \( \{a_n\} \) reduced modulo 4 consists of repetitions of the segment 0, 1, 2, 3
\( \pmod{4} \), the two subsequences \( \{a_{4n+1}\} \) and \( \{a_{4n+3}\} \) have no elements in common.
Thus the union \( \{a_{4n+1}\} \cup \{a_{4n+3}\} \) has multiplicity one. Since one has

\[
\{U_{4n+2}\} = \{U_{8n+2}\} \cup \{U_{8n+6}\} = \{U_2 a_{4n+1}\} \cup \{U_2 a_{4n+3}\},
\]

the subsequence \( \{U_{4n+2}\} \) is also of multiplicity one, and the first assertion is
proved.

\[\end{proof}\]
If \( r < 2s \), then \( U_3 = M^2 - N = -c + 2^r \pmod{2^{r+1}} \), and so \(-N U_3 \equiv 1 \pmod{2^{r+1}}\). By Eqs. (15,14) and the inequality \( r + 1 \leq 2s \), one has

\[
U_{4n-1} \equiv (-N U_3)^{n-1} U_3 \equiv U_3 \equiv -c + 2^r \pmod{2^{r+1}}
\]

\[
U_{4n+1} \equiv U_5^n = (M^4 - 3M^2 N + N^2)^n \equiv N^{2n} \equiv 1 \pmod{2^{r+1}}
\]

Since by Lemma 1, \( U_n \) is odd precisely when \( n \) is odd, assertion (ii) follows from these congruences and the first assertion. Assertion (iii) follows from the first two assertions and the observation that when \( c = 1 \), the sequence \( \{U_n\} \) reduced modulo 4 consists of repetitions of the segment \( 0, 1, M, -1 \pmod{4} \).

This completes the proof.

**Proposition 3.** Let \( \{U_n\} \) be a non-degenerate Lucas sequence of the first kind satisfying Eq. (1) with \( \Delta = M^2 - 4N < 0 \). Suppose that \( p^t \mid U_3 \), \( p^u \mid M^3 + 1 \), and \( w = \min(u,t) \) where \( p \) is a prime and \( \delta = \delta_2 \) is the Kronecker \( \delta \). If \( u \neq t \), then and either \( w > 2e \) or \( w = u = 2 \), then the recurrence \( \{U_n\} \) has multiplicity one.

**Proof.** Since \( U_3 = M^2 - N \), one has

\[
1 + N U_2 = 1 + N M = (1 + M^3) - M U_3 \equiv 0 \pmod{p^w}
\]

By Theorem 2 (iii) applied with \( d = 3 \), \( v = 1 \), the sequence \( \{U_{3n}\} \) has multiplicity one. Further, the parameter \( K \) of Theorem 1 with \( q = 3 \) satisfies \( K \geq w > e \). Since

\[
U_4 - U_1 = M^3 - 2MN - 1 = 2 M U_3 - (1 + M^3),
\]

\[
U_5 - U_2 = M^4 - 3M^2 N + N^2 - M = U_5^2 - M(1 + M^3) + M^2 U_3,
\]

the \( p \)-adic order of \( U_4 - U_1 \) and \( U_5 - U_2 \) are \( \min(t+e,u) \) and \( w \) respectively.
It follows by Theorem 1, that the multiplicities of the subsequences \( \{U_{3n+1}\} \) and \( \{U_{3n+2}\} \) are both one. Since the sequence \( \{U_n\} \) reduced modulo \( p^{e+1} \) consists of repetitions of the segment \( 0, 1, -1 \ (\text{mod } p^{e+1}) \), a given integer can occur in at most one of the subsequences \( \{U_{3n}\} \), \( \{U_{3n+1}\} \), \( \{U_{3n+2}\} \). This proves the proposition.

**Corollary 2.** Let \( \{U_n\} \) be a non-degenerate Lucas sequence of the first kind satisfying Eq. (1) with \( M^2 - 4N < 0 \). Suppose that \( p^t \parallel U_3 \), \( p^u \parallel M^3 - 1 \), and \( w = \min (u, t) \) where \( p \) is a prime and \( e = \delta_2 p \) is the Kronecker \( \delta \). Assume that \( u \neq t \), \( t + e \), and either \( w > 2e \) or \( w = u = 2 \). If \( M \neq 1 \), then the sequence \( \{U_n\} \) has multiplicity one. If \( M = 1 \), then \( U_1 = U_2 = 1 \) are the only occurrences of 1, the integer -1 does not occur in \( \{U_n\} \), and \( m(c) \leq 1 \) for all \( c \neq 1 \).

**Proof.** This is a consequence of Proposition 3 and Lemma 3.

The next result is the third theorem of the introduction.

**Corollary 3.** Let \( \{U_n\} \) be a non-degenerate Lucas sequence of the first kind satisfying Eq. (1) with \( \Delta = M^2 - 4N < 0 \), \( M = \pm 1 \), and \( N \neq 2, 3 \) or 5. If \( M = -1 \), then the sequence \( \{U_n\} \) has multiplicity one. If \( M = 1 \), then \( U_1 = U_2 = 1 \) are the only occurrences of 1, the integer -1 does not occur in \( \{U_n\} \), and \( m(c) \leq 1 \) for all \( c \neq 1 \).

**Proof.** This follows from Proposition 3 and Corollary 2 by taking for \( p \) the largest prime divisor of \( U_3 = M^2 - N = 1 - N \). The hypotheses are satisfied except when \( 1 - N = -1, -2, \) or \( -4 \).

**Remark.** The exceptional where \( M = \pm 1 \) and \( N = 2, 3, 5 \) have been treated. By Lemma 3, it suffices to treat the case \( M = 1 \). In the case \( M = 1, N = 2 \), Skolem, Chowla and Lewis [10] showed that
\[ U_1 = U_2 = -U_3 = -U_5 = -U_{13} = 1 \]

are the only solutions of \( U_n^2 = 1 \); Townes [12] completed the result by showing that \( U_4 = U_8 = -3 \) are the only occurrences of \(-3\) and that no integer \# ± 1, -3 occurs more than once in \( \{U_n\} \). In Alter and Kubota [1], it was shown that in the case \( M = 1, N = 3 \), the only occurrences of 1 are \( U_1 = U_2 = U_5 \), that \( -1 \) does not occur in \( \{U_n\} \), and that \( m(c) \leq 1 \) for all \( c \neq 1 \). Finally, Alter (unpublished) has shown that in the case \( M = 1, N = 5 \), the only occurrences of 1 are \( U_1 = U_2 = U_7 \), that \( -1 \) does not occur in \( \{U_n\} \), and that \( m(c) \leq 1 \) for all \( c \neq 1 \).

The next result contains part (i) of the last theorem stated in the introduction.

**Corollary 4.** Let \( \{U_n\} \) be a non-degenerate Lucas sequence of the first kind satisfying Eq. (1) with \( M^2 - 4N < 0 \). Suppose \( 2^s \mid |M - \epsilon|, 2^r \mid |N - 1| \) where \( \epsilon = \pm 1, s \geq 2, r \geq 3, \) and \( s \neq r, r + 1 \). If \( M \neq 1 \), then the sequence \( \{U_n\} \) is of multiplicity one. If \( M = 1 \), then \( U_1 = U_2 = 1 \) are the only occurrences of 1, \( m(-1) = 0 \), and \( m(c) \leq 1 \) for all \( c \neq 1 \). If \( r + 1 < s \), then for every odd positive integer \( c \), one has \( m(c) + m(-c) \leq 1 \) except that \( m(1) + m(-1) = 2 \) in case \( M = \pm 1 \).

**Proof.** Apply Proposition 3 and Corollary 2 with \( p = 2 \) and \( u = s \). Since

\[ 2^t \mid |U_3 = (M^2 - 1) - (N - 1) = 2^{s+1} - 2^r \pmod{2^\min(r,s+1)+1}, \]

one has \( t \geq \min(s+1,r) \geq 3 \), and so \( w > 2 \) or \( w = s = 2 \). Also, \( u \neq t, t+1 \) since \( s \neq r, r+1 \) respectively. The above mentioned results therefore show the first two assertions.
If \( r+1 < s \), then the first two assertions imply that the subsequence 
\[ \{ U_m \}_{2n} \] for \( m > 0 \) is of multiplicity one. By Eq. (22), the subsequence 
\[ \{ U_k \}_{2n} \] for \( k \geq 0 \) satisfies
\[
\begin{align*}
& V_{2k(n+2)} = V_k U_{2k(n+1)} - N^k U_{2n} \\
& 2^k \end{align*}
\]
where \( \{ V_n \} \) is the Lucas sequence of the second kind satisfying the same recurrence relation as does \( \{ U_n \} \). If one defines \( r(k) \), \( s(k) \), and \( e(k) \) by
\[
2^r(k) || N^k - 1, 2^s(k) || V_k - e(k), \text{ and } e(0) = e, e(k) = -1 \text{ for } k > 0,
\]
then evidently \( r(k) = r+k \) and further \( r(k) \leq s(k) \). In fact, the assertion is clear for \( k = 0 \), for \( k = 1 \), one has
\[
V_2 + 1 = (2^2 - 1) - 2(N - 1) \equiv 0 \pmod{2^{r+1}}.
\]
and by induction using Eq. (8),
\[
2^k = V_{2^{k-1} - 2^k} = (V_{2^{k-1} - 1}) = 2(N^{k-1} - 1) \equiv -1 \pmod{2^{r+k}}.
\]
Proposition 2 (ii) applied to \( \{ U_k \}_{2n} \) with the parameters \( p = 2, d = 3 \), \( u = r+k, v = 0, t = \min(s(k)+1, r(k)) = r+k, w = r+k, \) and \( e = f = 1 \)
shows that the union \( \{ U_{3, 2^{k+1} n-2^k} \} \cup \{ U_{3, 2^{k+1} n+2^k} \} \) cannot contain both an integer and its additive inverse. Further by Lemma 3, if \( V_{2^k} \neq 1 \) (resp. \( V_{2^k} = 1 \)), then the intersection
\[
\{ U_{2^k+1} \}_{2n} \cap \{ U_{2^{k+1} n+2^k} \}_{2n}
\]
is empty (resp. contains only \( \{ U_k \}_{2n} \)). Finally, \( 2|U_{3n} \) for all \( n \geq 0 \) by Lemma 1.

If \( c \) is an odd positive integer with \( m(c) + m(-c) \neq 0 \), let \( k \) be the least non-negative integer for which there is an \( n \) with \( 2^k || n \) and \( |U_{n}| = c \).
If \( V_{2^k} \neq 1 \) or \( c \neq |U_{2^k}| \), then by Lemma 1 and the last paragraph, all occurrences of \( c \) and \( -c \) lie in
\[
2^{k+1} \cdot 3.
\]
\[ \{ U_{2^{k+1}n+2} \} \cap (\{ U_{3n+1} \} \cup \{ U_{3n+2} \}) \]

\[ = \{ U_{2^{k+1}3n+2} \} \cup \{ U_{2^{k+1}3n-2} \}, \]

and so \( m(c) + m(-c) = 1 \). If \( V_{2k} = \pm 1 \) and \( c = |U_{2k}| \), then by Eqs. (7,8), one has \( |U_{2^{k+1}3n+2} = |U_{2^k}V_{2^k} = c \), and so \( m(c) + m(-c) = 2 \). By Eq. (31), \( V_{2k} \neq 1 \) for \( k > 0 \), and by Lemma 2 \( V_{2k} = \pm 1 \) can happen for at most one value of \( k \geq 0 \). Therefore, if \( V_1 = M = \pm 1 \), then \( m(1) + m(-1) = 2 \) and \( m(c) + m(-c) \leq 1 \) for all odd \( c' > 1 \). The proof would be complete if we could show that \( V_k \neq -1 \) for \( k > 0 \).

One has \( V_k \neq -1 \) for \( k > 0 \). In fact, if \( V_2 = M^2 - 2n = -1 \), then \( N = (M^2 - 1)/2 + 1 \equiv \text{mod} \ 2^8 \) and so \( s \leq r \) contrary to hypothesis. If \( V_4 = -1 \), then by Eq. (11), one has

\[ -1 = V_4 = MU_4 - 2NU_3 = -M^4 + 2(M^2 - N)^2 = -4^4 + 2U_2^2. \]

Thus \( x = U_2, y = U_3 \) is a solution of the diophantine equation \( x^4 - 2y^2 = 1 \).

By Ljunggren [8], it follows that \( U_2 \) or \( U_3 \) is zero. Thus \( \{ U_n \} \) has an infinite number of zeros by Lemma 1; this is contrary to the non-degeneracy of \( \{ U_n \} \), [4]. Finally, if \( V_k = -1 \) with \( k \geq 3 \), then Eq. (31) shows that \( x = V_{2^{k-1}n}, y = 2^{-k-3} \) are a solution of the diophantine equation \( x^2 - 2y^4 = -1 \).

A well known theorem of Ljunggren [7] and Eq. (31) imply that \( (V_{2^{k-1}}, N_{2^{k-3}}) \) is either \((-1,1)\) or \((239,13)\). The first possibility implies that \( \{ U_{2^{k-1}} \} \) and hence \( \{ U_n \} \) is degenerate. The second possibility implies that \( k = 3 \), \( N = 13 \), and

\[ V_2 = V_4 + 2N^2 = 239 + 2.13^2 = 577 \]

which is absurd since 577 is non-square. This completes the proof.
5.-

The next three lemmas are applications of Theorem 3 preliminary to the proof of the first theorem of the introduction.

Lemma 4.- Let \( \{U_n\} \) be a non-degenerate Lucas sequence of the first kind satisfying Eq. (1) with \( \Delta = M^2 - 4N < 0 \) and \( 2 \nmid MN \). Then

\[
U_{6n+1} \equiv 1 \pmod{4} \quad \text{and} \quad U_{6n+5} \equiv -N \pmod{4}
\]

for all \( n \geq 0 \); further, each subsequence \( \{U_{6n+1}\} \), \( \{U_{6n-1}\} \) contains at most two occurrences of \( 1 \) and \(-1\). If \( M \neq \pm 1 \), then all occurrences of \( +1 \) and \(-1\) lie in these two sub sequences. In particular, if \( M \neq \pm 1 \), then \( m(-1) = 0 \) when \( N \equiv 3 \pmod{4} \) and \( m(1) \), \( m(-1) \leq 2 \) when \( N \equiv 1 \pmod{4} \).

Proof.- \( U_3 \) is even, \( U_2 = M \) and \( U_4 \) are odd; therefore by Eq. (12)

\[
U_7 = U_4^2 - NU_3^2 \equiv 1 \pmod{4}, \quad \text{and} \quad U_5 = U_3^2 - NU_2^2 \equiv -N \pmod{4}.
\]

By Eqs. (13, 14), it follows that \( U_{6n+1} \equiv 1 \pmod{4} \) and \( U_{6n+5} \equiv -N \pmod{4} \). Further, using Eq. (10) to check the multiplicative order \( \pmod{4} \) of the roots of the companion polynomial, one can apply Theorem 3 with \( p = 2 \) and

\[
q = 6 \quad (q = 3 \text{ if } M \equiv -N \equiv 3 \pmod{4})
\]

to show that \( \{U_{6n+1}\} \) and \( \{U_{6n-1}\} \) have multiplicity at most two. Finally, by Lemma 1, \( 2|U_{3n} \) and \( M = U_2|U_{2n} \) for all \( n \geq 0 \); therefore, if \( M \neq \pm 1 \), then all occurrences of \( \pm 1 \) must lie in \( \{U_{6n-1}\} \cup \{U_{6n+1}\} \).

Lemma 5.- Let \( \{U_n\} \) be a non-degenerate Lucas sequence of the first kind satisfying Eq. (1) with \( \Delta = M^2 - 4N < 0 \). If \( 9|M \), then \( m(1) \), \( m(-1) \leq 2 \).

Proof.- If \( \beta_i \) for \( i = 1,2 \) are the roots of the companion polynomial, then by Eq. (10), one has \( \beta_1^2 \equiv -N \pmod{9} \) and \( \beta_1^4 \equiv N^2 \pmod{9} \). Thus \( \beta_1^k \equiv 1 \pmod{9} \) where \( k = 4,6,12,6,12,2 \) in case \( N \equiv 1,2,4,5,7,8 \pmod{9} \) respectively. The
sequence \( \{ U_n \} \) reduced modulo 9 consists of repetitions of the following segments

\[
\begin{align*}
0,1,0,8 & \quad \text{if } N \equiv 1 \pmod{9} \\
0,1,0,7,0,4 & \quad \text{if } N \equiv 2 \pmod{9} \\
0,1,0,5,0,7,0,8,0,4,0,2 & \quad \text{if } N \equiv 4 \pmod{9} \\
0,1,0,4,0,7 & \quad \text{if } N \equiv 5 \pmod{9} \\
0,1,0,2,0,4,0,8,0,7,0,5 & \quad \text{if } N \equiv 7 \pmod{9} \\
0,1 & \quad \text{if } N \equiv 8 \pmod{9}
\end{align*}
\]

Thus each of the integers 1 and -1 can lie in at most one subsequence \( \{ U_{kn+i} \} \) \( 0 \leq i < k \). Applying Theorem 3 with \( p = 3, r = k \), and \( s = 1 \) gives the result.

**Lemma 6.** If \( \{ U_n \} \) is a non-degenerate Lucas sequence of the first kind satisfying Eq. (1) with \( \Delta = M^2 - 4N < 0 \) and \( M = \pm 3 \), then \( m(1), m(-1) \leq 2 \).

**Proof.** Since \( \Delta < 0 \), \( N > 2 \) and so there is a largest prime divisor \( p \) of \( N \). Suppose \( p^t \mid N \) and let \( d \) be the multiplicative order of \( M \pmod{p^t} \). By Eq. (20), one knows that \( U_n \) can be 1 only if \( n \equiv 1 \pmod{d} \) and \( U_n \) can be -1 only if \( d \) is even and \( n \equiv d/2 + 1 \pmod{d} \).

If \( d = 1 \), then by the definition of \( p^t \) and \( d \), we have \( p^t = 2 \) or 4 and hence \( N = 2 \) or 4. Since \( N > 2 \), we have \( N = 4 \). If \( M = \pm 3 \) and \( N = 4 \), then the sequence \( \{ U_n \} \) reduced modulo 3 (resp. 5) consists of repetitions of the segment \( 0,1,0,2 \pmod{3} \) (resp. \( 0,1, \pm 3, 0, \pm 3,4,0,4, \pm 2,0, \pm 2,1 \pmod{5} \)). Therefore, \( U_n \) can be 1 only if \( n \equiv 1 \pmod{12} \) and it can be -1 only if \( n \equiv 7 \pmod{12} \). Applying Theorem 3 with \( p = 5, r = 3 \), and \( s = 4 \) gives \( m(1), m(-1) \leq 2 \). In particular, we may assume \( d > 1 \).
Since Theorem 3 gives the result in the contrary case, one can also assume that no prime larger than 3 divides $U_d$. By Lemma 1, we know $U_n$ is a multiple of 3 (resp. is even) precisely when $n$ is even (resp. is a multiple of 3). Suppose $2^u \mid d$ and define

$$v = \begin{cases} \ord_3 d & \text{if } N \text{ is odd} \\ 0 & \text{otherwise} \end{cases}$$

and $f = d2^{-u}3^{-v}$.

Since $U_f \mid U_d$ by Lemma 1 and $2, 3 \nmid U_f$, one has $U_f = \pm 1$. If $U_f = 1$, then by the first paragraph of the proof, $d2^{-u}3^{-v} = f \equiv 1 \pmod{d}$ and so $d \mid 2^u3^v$.

If $U_f = -1$, then $d$ is even and $d2^{-u}3^{-v} = f \equiv 1+ d/2 \pmod{d}$ and so again $d \mid 2^u3^v$. Since $2^u3^v \mid d$, one has in all cases that $d = 2^u3^v$.

Suppose $u \geq 2$. Since $U_4 \mid U_d$ by Lemma 1, we know that $U_4$ is divisible by no prime larger than 5. But $U_4 = N(M^2 - 2N) = \pm 3(9 - 2N)$ is clearly odd and exactly divisible by 3. Thus $9 - 2N = \varepsilon$ where $\varepsilon = \pm 1$, and hence $N = (9 - \varepsilon)/2 = 4$ or 5. Now $N = 4$ is impossible since $p^t = 4$ and $d = 2$ in this case. Thus $N = 5$, $M = \pm 3$, and we have $m(1), m(-1) \leq 2$ by Lemma 4.

Suppose $d = 2$. Since $N^2 = 9 \equiv 1 \pmod{p^t}$, we have $p^t \mid 8$ and so $N = 4$ or 8 as $N > 2$. The case $N = 4$ having already been treated, we may assume $N = 8$ and $M = \pm 3$. The sequence $\{U_n\}$ reduced modulo 4 consists of 0 followed by repetitions of the segment 1, $\pm 3 \pmod{4}$. Since $3\mid U_{2n}$ for all $n \geq 0$ by Lemma 1, it follows that $m(-1) = 0$. By Eq. (22) with $r = 2$ and $V_2 = M^2 - 2N = -7$, one has

$$U_{2n+1} \equiv V_2 U_{2n-1} \equiv \ldots \equiv V_2^{n-1} U_3 = (-7)^{n-1} \pmod{N^2}$$

for $n > 0$. Since $-7$ has multiplicative order 8 modulo $N^2 = 64$, it follows that $U_{2n+1}$ can be 1 only if $n = 0$ or $n \equiv 1 \pmod{8}$. In particular, in
order to prove $m(1) \leq 2$ it suffices to show that the subsequence $\{U_{8n+3}\}$ is of multiplicity one. Using Eq. (12), one obtains

$$U_4 = M(M^2 - 2N) = \pm 21 \equiv 0 \pmod{7}, \quad U_3 = M^2 - N = 1,$$

$$U_7 = U_4^2 - NU_3^2 \equiv -N \pmod{7^2},$$

$$1 + NU_7 \equiv 1 - N^2 = -63 \equiv 5 \pmod{7^2},$$

$$U_{11} - U_3 = (U_4 U_8 - NU_3 U_7) - U_3 \equiv -U_3 (1 + NU_7) \not\equiv 0 \pmod{7^2}.$$

Applying Theorem 1 with $p = 7, q = 8, i = 3$, and $K = 1$, one sees that $\{U_{8n+3}\}$ is indeed of multiplicity one.

The above cases exhaust that in which $d = 2^{u_3}v$ is a power of 2. By the definition of $v$, we may assume $N$ is odd and $3 \mid d$. If $6 \mid d$, then by the first paragraph of the proof, both 1 and -1 can each occur in at most one subsequence $\{U_{6n+1}\}, 0 \leq i < 6$. By Lemma 4, it follows that $m(1), m(-1) \leq 2$. If $9 \mid d$, then $U_9 \mid U_d$ by Lemma 1, and so $U_9$ is divisible by no prime larger than 3. By Eqs. (7,8), one has

$$U_9 = U_3 (\beta_1^6 + \beta_1^3 \beta_2^3 + \beta_2^6) = U_3 (V_3^2 - N^3).$$

Also $V_3 = M(M^2 - 3N) = \pm 3 \pmod{9 - 3N}$ implies that $V_3^2 - N^3$ is neither even nor divisible by 3. Therefore $V_3^2 - N^3 = \epsilon$ where $\epsilon = \pm 1$. This is a special case of the Catalan equation; by theorems of Lebesgue [5] and Chao Kuo [2], the only solutions are

$$V_3 = \pm 3, \quad N = 2, \quad \epsilon = 1$$

or $V_3 = \pm 1, 0$.

Since $N$ is odd, it follows that $V_3 = 0$ and $N = \pm 1$ contrary to the assumption that $\Delta = M^2 - 4N < 0$. 

28
The remaining case is \( d = 3 \). Since \( N \) is odd, \( \pm 27 = M^3 \equiv 1 \pmod{p^t} \) and so \( N = p^t = 13 \) if \( M = 3 \), and \( N = p^t = 7 \) if \( M = -3 \). If \( M = 3 \) and \( N = 13 \) then \( m(1), m(-1) \leq 2 \) by Lemma 4. If \( M = -3 \) and \( N = 7 \), then Lemma 4 shows that \( m(-1) = 0 \) and \( \{U_{6n+1}\} \) contains at most two occurrences of 1. By the first paragraph of the proof and the assumption that \( d = 3, -1 \) does not occur in \( \{U_n\} \) and 1 does not occur in \( \{U_{6n-1}\} \). Thus \( m(1) \leq 2 \) and the proof of the lemma is complete.

The next result contains the first two theorems stated in the introduction.

**Theorem 4.** Let \( \{U_n\} \) be a Lucas sequence of the first kind satisfying Eq. (1) with \( \Delta = M^2 - 4N < 0 \). The multiplicity of \( \{U_n\} \) is at most two except when \( M = 1, N = 3,5 \) or \( M = \pm 1, N = 2 \). More precisely, if \( c > 1 \) is a positive integer, then \( m(c) + m(-c) \leq 2 \), and the same inequality holds with \( c = 1 \) except possibly in the following cases.

(a) \( M = \pm 1 \) and \( N = 2, 3, 5 \).

(b) \( M \neq \pm 1, N \equiv 2 \pmod{48} \), and for every odd prime divisor \( p_1 \) of \( N \) (resp. \( p_2 \) of \( M \)), the multiplicative order \( d_1 \) of \( M \pmod{p_1} \) (resp. \( d_2 \) of \( -N \pmod{p_2} \)) satisfies \( 2^3 \nmid d_1 \) (resp. \( 2^2 \nmid d_2 \)). In this case, \( U_1 = 1 \) is the only occurrence of 1, every occurrence of -1 lies in the subsequence \( \{U_{8n+5}\} \), and every odd prime divisor \( p_1 \) of \( N \) (resp. \( p_2 \) of \( M \)) satisfies \( p_1 \equiv 1 \pmod{8} \) (resp. \( p_2 \equiv 1 \pmod{4} \)).

**Proof.** Let \( \{V_n\} \) be the Lucas sequence of the second kind which satisfies the same recurrence relation as does \( \{U_n\} \). One cannot have \( U_m = 0 \) for any \( m > 0 \) since this would imply by Lemma 1 that \( \{U_n\} \) has an infinity of zeros contrary to the non-degeneracy of \( \{U_n\}, [4] \). Let \( \epsilon \) be any non-zero integer occurring in \( \{U_n\}, \) and \( f \) be the least positive integer with \( \epsilon \mid U_f \). By Lemma 1, \( U_f \equiv \pm \epsilon \).
and all occurrences of $c$ and $-c$ lie in the subsequence $\{U_{fn}\}$. In particular, $m(U_f)$ (resp. $m(-U_f)$) is equal to the number of times 1 (resp. -1) occurs in the sequence $b_n = U_{fn}/U_f$. By Eq. (22), $\{b_n\}$ is a Lucas sequence of the first kind satisfying the recurrence relation

$$b_{n+2} = V_f b_{n+1} - N_f b_n, \quad b_0 = 0, \quad b_1 = 1.$$  

Further, if $c \neq \pm 1$, then $f > 1$ and hence $N_f \not\equiv 2, 3, 5 \pmod{4}$. Therefore, we are reduced to showing that $m(1), m(-1) \leq 2$ except in case (a) above, that $m(1) + m(-1) \leq 2$ except in cases (a) and (b), and that the assertions of case (b) hold.

To show that $m(1), m(-1) \leq 2$ except when $M = \pm 1$, $N = 2, 3, 5$ it suffices in the case where $M$ is a multiple of a prime greater than 3 (resp. $9 | N$, $M = \pm 3$, $M = \pm 1$) to apply Theorem 3 (resp. Lemma 5, Lemma 6, Corollary 3). In case $M = \pm 1$, $N \not\equiv 2, 3, 5$, one obtains the stronger assertion $m(1) + m(-1) \leq 2$. This leaves the case where $M$ is even; here Theorem 3 applied with $p = 2$ and $q = 4$ shows the multiplicity of the subsequence $\{U_{4n+1}\}$ is at most 2, and therefore $m(1) + m(-1) \leq 2$ by Corollary 1 (i,ii). In particular, $\{U_n\}$ has multiplicity at most 2 unless $M = \pm 1$, $N = 2, 3, 5$.

Suppose that both $M$ and $N$ are odd and $M \neq \pm 1$. By Lemma 4, all occurrences of 1 and -1 lie in the subsequences $\{U_{6n-1}\}$ and $\{U_{6n+1}\}$. Further, one has by Eqs. (19,12) that

$$U_6 = M(M^2 - N)(M^2 - 3N) \equiv M(1-N)(1+N) \equiv 0 \pmod{8}$$

$$8 | N^6 - 1, \quad 2 | U_3, \quad 3 \nmid U_4, \quad \text{and}$$

$$U_7 = U_4^2 - NU_3^2 \equiv 1 \pmod{4}.$$
Therefore, Proposition 2 (i,ii) applied with $p = 2$, $d = 6$ shows that either $m(1)$, $m(-1) \leq 1$ or else $m(-1) = 0$; and so $m(1) + m(-1) \leq 2$.

If $4|N$ and $M \neq \pm 1$, then $1$ and $-1$ cannot occur in $\{U_{2n}\}$ by Lemma 1 and $U_{2n+1} \equiv 1 \pmod{4}$ by Eq. (20). Hence $m(-1) = 0$ and so $m(1) + m(-1) \leq 2$.

Having treated the above cases, we may assume that $M \neq \pm 1$, $N \equiv 2 \pmod{4}$ and hence that $1$ and $-1$ do not occur in $\{U_{2n}\}$. By Eq. (22) with $r = 2$ and $s = 1$, one has

$$U_{2n+1} \equiv V_2 U_{2n-1} \equiv \ldots \equiv V_2^{n-1} U_3 = (M^2 - 2N)^{n-1} (M^2 - N) \equiv 3 \pmod{4}$$

for $n \geq 1$. Therefore $U_1 = 1$ is the only occurrence of $1$ in $\{U_n\}$. With $p_1$ and $d_1$ as in the statement, Eq. (21) shows that $U_n$ can be $-1$ only when $d_1$ and $d_2$ are even, $n \equiv 1 + d_1/2 \pmod{d_1}$, and $n \equiv 1 + d_2 \pmod{2 d_2}$.

Since $2 | |N$ and $M$ is odd, $V_2 = M^2 - 2N \equiv 5 \pmod{8}$. Therefore $V_2$ is divisible by an odd prime $p$, and we have $p \neq U_4 = U_2 V_2$ and $p \nmid M$. By Theorem 2 (ii) applied with $d = 4$, it follows that $-1$ occurs at most once in the subsequence $\{U_{4n+3}\}$. Similarly, if $U_3 = M^2 - N$ is divisible by an odd prime $p$, then the same result applied with $d = 3$ and $p$ shows that $-1$ occurs at most once in the subsequence $\{U_{3n-1}\}$.

Suppose that $3 | M$. With $p_2 = 3$ and $d_2 = 1$ or $2$ depending on whether or not $N \equiv 2 \pmod{3}$, we see that $m(-1) = 0$ if $N \equiv 2 \pmod{3}$, and that $-1$ occurs only in the subsequence $\{U_{4n+3}\}$ if $N \equiv 1 \pmod{3}$. Therefore $m(-1) \leq 1$ and $m(1) + m(-1) \leq 2$.

Suppose that $3 | N$. With $p_1 = 3$ and $d_1 = 1$ or $2$ depending on whether or not $M \equiv 1 \pmod{3}$, we see that $m(-1) = 0$ since $-1$ does not occur in $\{U_{2n}\}$.

Suppose that $3 | M$ and $3 | N-1$. Then $3 | U_3$ and so $-1$ occurs at most once.
in \( \{U_{3n-1}\} \). By Eqs. (12,14),

\[
U_{6n+1} \equiv U_7^n = (U_4^{2} - NU_3^2)^n \equiv (U_4^{2})^n \equiv 1 \pmod{3}.
\]

By Lemma 4, it follows that \( m(-1) \leq 1 \), and so \( m(1) + m(-1) \leq 2 \).

The remaining case is \( 3 \nmid M \) and \( N \equiv 2 \pmod{3} \). Let \( p_1 \) and \( d_1 \) be as in the statement. By the criterion of the fifth paragraph of the proof, all occurrences of \(-1\) in \( \{U_n\} \) lie in the following subsequences.

- none if \( d_1 \) or \( d_2 \) is odd
- \( \{U_{2n}\} \) if \( 2 \mid d_1 \)
- \( \{U_{4n+3}\} \) if \( 4 \mid d_1 \) or \( 2 \mid d_2 \)
- \( \{U_{8n+5}\} \) if \( 8 \mid d_1 \) or \( 4 \mid d_2 \)
- \( \{U_{8n+1}\} \) if \( 16 \mid d_1 \) or \( 8 \mid d_2 \).

In the first three cases, \( m(-1) \leq 1 \) and so \( m(1) + m(-1) \leq 2 \). In the fifth case, \( m(-1) = 0 \) and hence \( m(1) + m(-1) = 1 \) since by Eqs. (14,12) and the fact that \( 3 \nmid U_4 \), one has

\[
U_{8n+1} \equiv U_9^n = (U_5^{2} - NU_4^2)^n \equiv U_5^{2n} \equiv 1 \pmod{3}.
\]

Finally, in the fourth case, \( p_1 \equiv 1 \pmod{8} \) and \( p_2 \equiv 1 \pmod{4} \) since \( d_1 \mid p_1 - 1 \) and \( d_2 \mid p_2 - 1 \). In particular, since \( N \) is positive, \( 2 \mid N \), and \( 3 \mid N-2 \), we have \( N \equiv 2 \pmod{48} \). This completes the proof of the Theorem.
6. Open questions.

In view of Theorem 4, it is natural to make the following conjecture.

Conjecture 1. If \( \{U_n\} \) is a non-degenerate Lucas sequence of the first kind satisfying Eq. (1) with either \( M \neq \pm 1 \) or \( N \equiv 2, 3, 5 \), then \( m(1) + m(-1) \leq 2 \).

Using Theorem 2 (ii) and Theorem 4, it is straightforward to check by considering the various possibilities of \( M(\mod 5) \) and \( M(\mod 7) \) that the following is true.

Proposition 4. If \( \{U_n\} \) is a non-degenerate Lucas sequence of the first kind satisfying Eq. (1) with \( M \neq \pm 1 \) and either \( N \equiv \pm 1 (\mod 5) \) or \( N \equiv 6 (\mod 7) \), then \(-1\) occurs at most once in \( \{U_n\} \).

Applying this result and Theorem 4 to check the various values of \( N \equiv 2 (\mod 48) \), one obtains

Corollary 5. The above conjecture is true for all \( N \leq 1200 \) with the possible exception of \( N = 578 \).

Conjecture 2. If \( \{U_n\} \) is a non-degenerate Lucas sequence of the first kind, then with the possible exception of finitely many integers \( c \), one has

\[
m(c) + m(-c) \leq 1\.
\]

F. Beukers has announced to the author progress on both of the above conjectures.
REFERENCES.

1. R. Alter, K.K. Kubota, The diophantine equation \( x^2 + 11 = 3^n \) and a related sequence, J. Number Theory, 7 (1975), 5-10.

2. Chao Ko, On the diophantine equation \( x^2 = y^n + 1 \), \( xy \neq 0 \), Scientia Sinica (Notes), 14 (1964), 457-60.


8. W. Ljunggren, Some remarks on the diophantine equations \( x^2 - Dy^4 = 1 \) and \( x^4 - Dy^2 = 1 \), J. London Math. Soc., 41 (1966), 542-44.

