On a generalization of the Lucas functions

by

H. C. Williams (Toronto)

1. Introduction. Let \(a, \beta\) be the roots of the equation

\[x^2 - Px + Q = 0,
\]

where \(P, Q\) are coprime integers. The Lucas functions defined on the associated equation (1.1) are given by

\[v_n = a^n + \beta^n,\]

\[u_n = (a^n - \beta^n)/(a - \beta).
\]

We shall call \(\{v_n, u_n\}\) a set of ordinary Lucas functions. These functions and their many properties have been discussed by several authors. The most extensive works are Lucas [7] and Carmichael [2]. Because of the many uses of these functions in Number Theory and Combinatorial Theory, a generalization of them should be of some interest.

We can give an alternative definition of \(\{v_n, u_n\}\) by noting that

\[a = (v_1 + u_1 \delta)/2, \quad \beta = (v_1 - u_1 \delta)/2,
\]

where \(\delta = a - \beta\). Hence,

\[v_n = ((v_1 + u_1 \delta)/2)^n + ((v_1 - u_1 \delta)/2)^n,
\]

\[u_n = \delta^{-1} \{((v_1 + u_1 \delta)/2)^n - ((v_1 - u_1 \delta)/2)^n\},
\]

where \(v_1 = P, u_1 = 1, \delta^2 = \delta = P^2 - 4Q\) and \(P, Q\) are coprime integers. We shall use this definition of the Lucas functions in order to generalize them.

2. Notation and definitions. We denote by \(\mathbb{C}\), the complex field, by \(\mathbb{Z}\), the field of rational integers, and by \(\mathbb{N}\), the set of positive elements of \(\mathbb{Z}\). Let \(q\) be any prime in \(\mathbb{Z}\) and \(\omega = \exp(2\pi i/q)\), where \(i = \sqrt{-1}\). If \(q > 2\), let \(\delta\) be the real \(q\)th root of some nonzero \(\mathbb{A} \in \mathbb{Z}\); if \(q = 2\), let \(\delta = \sqrt{A}\).

Let

\[a_j = \frac{1}{q} \sum_{i=0}^{q-1} U_{ij} \delta^i \omega^{-6i} \quad (j = 0, 1, 2, \ldots, q-1)
\]
be the $q$ roots of
\[ \sum_{k=0}^{q} q^{k-1} (-1)^k Q_k = 0, \]
where $Q_0 = 1$ and $U_{q,k}, U_{1,1}, \ldots, U_{q-1,1} \in \mathbb{Z}$. We define
\[ U_{q,k}^{(q)} = \delta^k \sum_{i=0}^{q-2} a_i^q a_i^q \] 
\[ (k = 0, 1, 2, \ldots, q-1). \]
For $q = 3$ the functions $U_{q,0}^{(q)}, U_{q,1}^{(q)}, U_{q,2}^{(q)}$ were used by Pocklington [10] in the production of an algorithm for finding the cube root of an integer modulo a given prime. Also, if $D = 3$, $U_{q,3} = 3X_1$, $U_{q,3} = 3Y_1$, $U_{q,3} = 3Z_1$, where $D$ is not a perfect cube and $(X_1, Y_1, Z_1)$ is a fundamental solution (see Matthews [8]) of the Diophantine equation
\[ X^3 + DY^3 + D^2Z^3 = 3DXYZ = 1, \]
then any solution of (2.3) is given by $(U_{q,3}^{(q)} / 3, U_{q,3}^{(q)} / 3, U_{q,3}^{(q)} / 3)$ for some integer $n$. These functions are discussed more fully in Williams [14].

In order to simplify our notation, we shall consider $q$ to be an arbitrary but fixed prime of $Z$; this allows us to drop the superscript of $U_{q,k}^{(q)}$.

3. Identities. It may be easily shown that the functions $U_{q,k}$
\[(k = 0, 1, 2, \ldots, q-1),\]
satisfy the following identities:
\[ U_{q,k} = U_{q-1,k} \Delta U_{q-1,k} \Delta U_{q-1,k} \]
\[ U_{q-1,k} U_{q-2,k} \Delta U_{q-2,k} \Delta U_{q-2,k} \]
\[ U_{q-2,k} U_{q-3,k} \Delta U_{q-3,k} \Delta U_{q-3,k} \]
\[ U_{q-3,k} U_{q-4,k} \Delta U_{q-4,k} \Delta U_{q-4,k} \]
\[ \vdots \]
\[ U_{q-1,k} U_{q,k} \Delta U_{q,k} \Delta U_{q,k} \]
\[ = q^{-1} Q_{q} U_{q-1,k} \]
\[ \Delta \]
\[ U_{q-1,k} U_{q-2,k} \Delta U_{q-2,k} \Delta U_{q-2,k} \]
\[ U_{q-2,k} U_{q-3,k} \Delta U_{q-3,k} \Delta U_{q-3,k} \]
\[ U_{q-3,k} U_{q-4,k} \Delta U_{q-4,k} \Delta U_{q-4,k} \]
\[ \vdots \]
\[ U_{q-1,k} U_{q,k} \Delta U_{q,k} \Delta U_{q,k} \]
\[ = Q_{q} U_{q-1,k} \]
\[ \Delta \]
\[ q U_{q,k} = \sum_{k=0}^{q-1} U_{q,k} U_{q-1,k} + \Delta \sum_{k=0}^{q-1} U_{q+k,k} U_{q-k,k} \]
\[ \Delta \]
\[ (\sum_{i=0}^{q-1} U_{q,i} \theta_i^k \theta_i^k)^n = \sum_{i=0}^{q-1} U_{q,i} \theta_i^k \theta_i^k \]
\[ (j = 0, 1, 2, \ldots, q-1), \]
\[ U_{q,j} U_{q,k} = \sum_{k=0}^{q} (-1)^{k+1} Q_{q} U_{q,j+k+k} \]
\[ \sum_{i=0}^{q-1} \theta_i^j x_i = -\log \frac{a_j}{Q_{q}} \quad (j = 0, 1, 2, \ldots, q-2). \]
We have
\[ U_{q,j} = q Q_{q}^{\theta_j} \theta_j y_j(n x_1, n x_2, \ldots, n x_{q-1}), \]
where $y_j$ is the $y_j$ function of Appell [1] and Glaisher [3].
4. The extended Lucas functions of order \( q \). It is clear that the functions \( U_{i,n} (j = 0, 1, 2, \ldots, g-1) \), are generalizations of the Lucas functions. In fact, the identities (3.1), (3.2), (3.3), (3.4), (3.5), (3.8), and (3.10) are completely analogous to the fundamental identities (51), (46), (40), (7), (10), (30), and (5) respectively of Lucas [7]. However, one of the most important properties of the ordinary Lucas functions \( v_n \) and \( w_n \) is that they are both integers for any \( n \in \mathbb{N} \). We shall prove in Theorem 1 that a necessary condition for \( U_{i,n} \in \mathbb{Z} (i = 0, 1, 2, \ldots, q-1) \), and \( n \) any element of \( N \), is that \( Q_i \in \mathbb{Z} (i = 1, 2, \ldots, q) \); but we must first give

**Lemma 1.** Let \( h_i(x) = b_i + \sum_{k=1}^{q-1} h_k(x + i - k)^f (i = 0, 1, 2, \ldots, q-1) \), where \( b_i \in \mathbb{Z} \) for \( k = 0, 1, 2, \ldots, g-1 \), and \( x \in \mathbb{R} \); then, if \( f_i(x) = S_i(h_0(x), h_1(x), \ldots, h_{q-1}(x)), \) where \( S_i(x_1, x_2, \ldots, x_q) \) is the \( r \)-th elementary symmetric function of \( x_1, x_2, \ldots, x_q \), we have

\[
f_i(x) = \left( \frac{q}{2} \right) b_i + \sum_{i=1}^{r-1} a_i x_i^{q-1},
\]

where \( a_i \in \mathbb{Z} (r = 1, 2, \ldots, g-1; i = 1, 2, \ldots, r-1) \).

Proof. This follows easily by observing that \( g_i \) is a symmetric polynomial in \( x^i, x^2, \ldots, x^{q-1} \) and by using the symmetric function theorem.

**Theorem 1.** If \( U_{i,n} \in \mathbb{Z} (i = 0, 1, 2, \ldots, g-1) \), and all \( n \in \mathbb{N} \), then \( Q_i \in \mathbb{Z} (i = 1, 2, \ldots, q) \).

Proof. By Lemma 1, \( g_i Q_i \in \mathbb{Z} (i = 0, 1, 2, \ldots, g) \), and by (3.7), \( i! Q_i \in \mathbb{Z} \); hence, if \( i < g \), \( Q_i \in \mathbb{Z} \). Since \( U_{i,n} \in \mathbb{Z} \) for \( i = 0, 1, 2, \ldots, g-1 \), and \( k = 1, 2, 3, \ldots, g+1 \), it follows from (3.5) that \( g_i Q_k \in \mathbb{Z} \) and \( U_{i,n} Q_k \in \mathbb{Z} \) for \( i = 0, 1, 2, \ldots, g-1 \). If, for some \( i, (1) g_i U_{i,n} Q_i \in \mathbb{Z} \); if \( g_i U_{i,n} \in \mathbb{Z} \), then (by (3.2), we have \( g_i^2 Q_i \in \mathbb{Z} \) and consequently \( Q_i \in \mathbb{Z} \).

We may now define the extended Lucas functions of order \( g \), be chosen such that the expressions (2.2) are rational integers for any \( n \in \mathbb{N} \) and \((1) Q_i, Q_{q-1}, \ldots, Q_1 = 1 \). We call the set of functions \( \{ U_{i,n} \} (i = 0, 1, 2, \ldots, g-1) \), given by (2.2) a set of extended Lucas functions of order \( g \). It is evident that any set of ordinary Lucas functions is a set of extended Lucas functions of order \( 2 \); on the other hand, there are sets of extended Lucas functions of order \( g \) which are not sets of Lucas functions. An example of one of these is given by \( \{ U_{i,n} \}, \) where \( A = 5 \), \( U_{0,1} = 1 \), \( U_{1,1} = 2 \), \( Q_1 = 4 \), and \( Q_2 = -1 \). However, it is not difficult to show that the properties of the extended Lucas functions of order \( 2 \) are the same as the well known properties of the ordinary Lucas functions. For this reason and for the sake of convenience, we shall henceforth consider \( g \) to be an odd prime.

We now obtain the conditions on \( A, U_{i,n} \) \((i = 0, 1, 2, \ldots, g-1) \), which guarantee that \( U_{i,n} \) for \( i = 0, 1, 2, \ldots, g-1 \) are extended Lucas functions. We first require several lemmas.

**5. Preliminary results.**

**Lemma 2.** If \( g_1^2 A, r = (g-1)/2, \) and \( q U_{i,j} \) for \( j = 0, 1, 2, \ldots, r, \) then \( U_{i,j} \in \mathbb{Z} \), \( j = 0, 1, 2, \ldots, r, \), and \( U_{i,j,n} \) for \( j = 0, 1, 2, \ldots, r, \), where \( n \) is any element of \( N \).

**Proof.** This is easily proved from (3.3) by using induction on \( n \).

**Lemma 3.** If the conditions of Lemma 2 are true and \( q \mid n \), where \( n \in \mathbb{N} \), then \( q^2 U_{i,n} \) for \( j = 1, 2, \ldots, r, \) and \( q \mid U_{i,n} \) for \( j = 0, 1, 2, \ldots, r-1 \).

**Proof.** From Lemma 2 and Theorem 1, \( Q_k \in \mathbb{Z} \), and, by (3.6), \( q Q_k \), for \( k = 1, 2, \ldots, g-1 \). This fact, together with (3.5) and Lemma 2, shows that \( q^2 U_{i,n} \) for \( j = 1, 2, \ldots, r, \) and \( q \mid U_{i,n} \) for \( j = 0, 1, 2, \ldots, r-1 \); hence, the lemma is true for \( n = q \). We show that it is true for \( n = kq \) by using (3.3) and induction on \( k \).

**Lemma 4.** If the conditions of Lemma 2 are true and \( q \mid U_{i,n} \) for \( j = 0, 1, 2, \ldots, m, \) where \( m \geq r \), and \( n \in \mathbb{N} \), then

\[
U_{i,n} = q(U_{i,n}/q)^{m}(\text{mod} q^2),
\]

\[
U_{i,m+n} = n(U_{i,n}/q)^{m}U_{i,m+n} (\text{mod} q^2),
\]

\[
Q_{i} \in \mathbb{Z} \quad \text{and} \quad Q_{i} = \frac{U_{i,n}}{q}(\text{mod} q).
\]

Proof. The first two results follow from (3.3) and Lemma 2 by using induction on \( n \). From (3.5) and Lemma 2, \( Q_k \in \mathbb{Z} \), and

\[
U_{i,n} = qQ_k (\text{mod} q^2);
\]

thus,

\[
Q_{i} = \frac{U_{i,n}}{q}(\text{mod} q).
\]

**Lemma 5.** If \( A = d^2 + q^2 \), \( U_{i,j} = d^{q-1} - q^2 j \) \((j = 0, 1, 2, \ldots, g-1) \), then \( q \mid U_{i,n} \) for \( j = 0, 1, 2, \ldots, g-1 \), and \( q \mid A \).

**Proof.** Let \( A = \sum_{i=0}^{q-1} r_i A_i \). Suppose that \( U_{i,n} = A^q - q^2 R_{i,n} \).
(j = 0, 1, 2, ..., g−1), where
\[ \sum_{j=0}^{g−1} R_{j,m} d^j = A_m^m \pmod{g} \] and \[ A_m = (c + A)^m - A^m \pmod{g}. \]

This supposition is true for \( m = 1 \). By (3.3)
\[ U_{k,m+1} = a_2^{m+1} \left[ (c + A)^m + A \right] + \sum_{j=0}^{g−1} R_{j,m} d^j + q \sum_{j=0}^{g−1} R_{j+1,m} d^{j+1} + q a_2 d^g \quad \] and
\[ + q \sum_{j=0}^{g−1} R_{j,m} d^j. \]

Thus,
\[ U_{k,m+1} = A_{m+1} a_2^{m+1} + \sum_{j=0}^{g−1} R_{j,m} d^j \quad (k = 0, 1, 2, ..., g−1), \]
where
\[ A_{m+1} = (c + A)^{m+1} - A^{m+1} \pmod{g}, \]

\[ R_{j,m} = \sum_{j=0}^{g−1} R_{j,m} d^j + \sum_{j=0}^{g−1} R_{j+1,m} d^{j+1} + \sum_{j=0}^{g−1} R_{j,m} d^j. \]

Thus,
\[ A_{m+1} = (c + A)^{m+1} - A^{m+1} \pmod{g}, \]

\[ R_{j,m} = \sum_{j=0}^{g−1} R_{j,m} d^j + \sum_{j=0}^{g−1} R_{j+1,m} d^{j+1} + \sum_{j=0}^{g−1} R_{j,m} d^j. \]

We also have
\[ U_{k,m} = \sum_{j=0}^{g−1} \left( \sum_{j=0}^{g−1} U_{j,m} d^j \right)^{q−j} = \sum_{j=0}^{g−1} \left( \sum_{j=0}^{g−1} U_{j,m} d^j \right)^{q−j} \pmod{g}. \]

We use the above lemmas to prove two important theorems. We first show what conditions must be placed on \( U_{i,m} \) \((i = 0, 1, 2, ..., g−1)\), and \( A \) in order that \( U_{i,m} \) \((i = 0, 1, 2, ..., g−1)\), be rational integers for any \( n \in N \).

**Theorem 2.** The functions \( U_{i,m} \) for \( i = 0, 1, 2, ..., g−1 \) all be rational integers for any \( n \in N \) if and only if one of the following is true:

(a) \( q \mid U_{i,m} \) \((i = 0, 1, 2, ..., g−1)\),
(b) \( q^2 \mid A \), \( q \mid U_{i,m} \) \((i = 0, 1, 2, ..., r)\),
(c) \( A = 0 \pmod{q^2} \), \( U_{i,m} = \sum_{j=0}^{g−1} d^j \pmod{q^2} \).

Proof. From the preceding lemmas, it is clear that the theorem gives sufficient conditions for \( U_{i,m} \pmod{q} \) \((i = 0, 1, 2, ..., g−1)\). We need only prove the necessity of (i), (ii), or (iii).

**Case 1:** \( d \neq 0 \). Let \( \Delta = d_1 d_2 \cdots d_{g−1} \pmod{q} \), where \( d_1, d_2, ..., d_{g−1} \pmod{q} \), and \( d_1^2 d_2 \cdots d_{g−1} \pmod{q} \) has no square factor in \( Z \). It is evident that this representation of \( d \) is unique. Let
\[ \omega = \sum_{n=1}^{g−1} d_{n−i} i \quad (i = 1, 2, ..., g−1) \]

where \( \omega = \sum_{i=0}^{g−1} d_i \pmod{q} \). We now define \( \gamma_i = \sum_{i=0}^{g−1} d_i \pmod{q} \) for \( i = 1, 2, ..., g−1 \), \( \gamma = \omega \pmod{q} \), and \( \Delta = d \pmod{q} \). Let \( K(\gamma) \) be the algebraic number field formed by adjoining \( \gamma_i \) to \( Z \).

By Theorem 1, \( Q_1, Q_2, ..., Q_{g−1} \pmod{q} \) and \( Q_0 = 1 \); hence
\[ \alpha_0 = \frac{1}{q^{g−1}} \sum_{i=0}^{g−1} U_{i,1} d^i \]
is an algebraic integer in \( K(\gamma) \).
If \( q^i \tau(q^{i-1} - d_q^{i-1}) \), by Westlund [13],

\[
a_q = a_0 + \sum_{i=1}^{q-1} a_{i} \gamma_i,
\]

where \( a_i \in \mathbb{Z} \) (\( i = 0, 1, 2, \ldots, q-1 \)). As a consequence of this, \( q \mid U_{i,q} \gamma_i \) for \( i = 1, 2, \ldots, q-1 \) and \( q \mid U_{q,1} \). If \( q \mid U_{i,1} \) (\( i = 0, 1, 2, \ldots, q-1 \)), we obtain (i). If \( q \mid d_q \gamma_i \) for some \( i \geq 1 \), then \( q \mid d_q \gamma_i \). Since \( U_{1,1} \) is an integer for \( i = 0, 2, 4, \ldots, q-1 \), we have, from (3.3), that \( q \mid U_{i,1} \) for \( i = 0, 1, 2, \ldots, r \). This is case (ii).

If \( q^i \mid (q^{i-1} - d_q^{i-1}) \), then \( \Delta = \Phi(q^{i-1}) \) (mod \( q^i \)) and (Westlund [13])

\[
a_q = a_0 + \sum_{i=1}^{q-1} a_{i} \gamma_i,
\]

where \( a_i \in \mathbb{Z} \) (\( i = 0, 1, 2, \ldots, q-1 \)) and \( a_0 = 1 + \sum_{i=1}^{q-1} a_{i} \gamma_i \). Since

\[
U_{i,1} + \sum_{i=1}^{q-1} U_{i,1} \gamma_i = a_0 + \sum_{i=1}^{q-1} (g_i q^{i-1} a_0 + q \gamma_i),
\]

we have

\[
U_{i,1} = a_0,
\]

\[
U_{i,1} \gamma_i = q \Phi(q^{i-1}) a_0 \quad \text{(mod \( q^i \))}
\]

for \( i = 1, 2, \ldots, q-1 \). If \( q \mid U_{1,1} \), then \( q \mid U_{i,1} \) (\( i = 0, 1, 2, \ldots, q-1 \)) or \( q \mid \Delta \) and \( q \mid U_{1,1} \). Since \( a_i \gamma_i = 1 \), \( g \tau \gamma_i = g_i \), and \( q \tau \gamma_i \) for \( i = 1, 2, \ldots, q-1 \). Thus, if \( q \tau U_{1,1} \gamma_i \),

\[
U_{i,1} = q \Phi(q^{i-1}) \quad \text{(mod \( q^i \))},
\]

where \( q \tau \gamma_i \).

Case 2: \( \delta \in \mathbb{Z} \). Let \( K(\omega) \) be the algebraic number field formed by adjoining \( \omega \) to \( \mathbb{Z} \). Then

\[
a_{q-1} = \frac{1}{q} \sum_{i=1}^{q-1} U_{i,1} \omega_i,
\]

is an algebraic integer in \( K(\omega) \) and

\[
a_{q-1} = \sum_{i=1}^{q-1} \omega_i \gamma_i, \quad \text{where} \quad a_i \in \mathbb{Z} \quad (i = 0, 1, 2, \ldots, q-2)
\]

(see, for example, Leveque [6]). Since \( \sum_{i=1}^{q-1} \omega_i = 0 \), we have

\[
U_{i,1} \omega_i = U_{q-1,1} \omega_i \quad \text{(mod \( q^i \))},
\]

we have

\[
a_0 = 0 \quad \text{(mod \( P_i \))} \quad (i = 1, 2, \ldots, k).
\]

Thus, \( a_0 = 0 \) (mod \( P_i \)) or \( a_k = p \), where \( k \in \mathbb{Z} \). It follows that \( p \mid U_{1,1} \), \( U_{1,1} \), \( U_{q-1,1} \). If \( p \tau \Delta \) and \( \delta \tau \mathbb{Z} \), we use a similar argument on \( a_{q-1} \) in \( K(\omega) \).
We assume throughout the remaining portion of this paper that the symbol $U_{n, n}$ represents an extended Lucas function of order $q$ and that $\pi \in U_{n}$.

6. Properties of the extended Lucas functions. We shall demonstrate a great many properties of the functions $U_{n, n}$, which are similar to properties possessed by the ordinary Lucas functions $v_n$ and $v_{n+1}$. In fact, we shall produce analogues of Carmichael's Theorems I, II, III, VI, VII, X, XII, XIII, in Theorems 6, 5, 4, 9, 11, 12, 13, 14 respectively. We deal with divisibility of $(U_{n, n}, U_{n, n+1}, U_{n, n+2}, \ldots, U_{n, q-1})$ by $q$ in

**Theorem 4.** Let $n$ be any element of $N$. If $q | (U_{n, 1}, U_{n, 2}, U_{n, 3}, \ldots, U_{n, q-1})$, then $q | (U_{n, 1}, U_{n, 2}, U_{n, 3}, \ldots, U_{n, q-1})$ if and only if $q | (U_{n, 1}, U_{n, 2}, U_{n, 3}, \ldots, U_{n, q-1})$.

**Proof.** These results follow easily from the preceding lemmas, it should be noted that in the case of the last result $q | (U_{n, 1}, U_{n, 2}, U_{n, 3}, \ldots, U_{n, q-1})$.

**Lemma 8.** If $q | (U_{n, 1}, U_{n, 2}, U_{n, 3}, \ldots, U_{n, q-1})$ or $q | (U_{n, 1}, U_{n, 2}, U_{n, 3}, \ldots, U_{n, q-1})$, then $q | (U_{n, 1}, U_{n, 2}, U_{n, 3}, \ldots, U_{n, q-1})$.

**Proof.** Suppose $q | (U_{n, 1}, U_{n, 2}, U_{n, 3}, \ldots, U_{n, q-1})$ and $q | (U_{n, 1}, U_{n, 2}, U_{n, 3}, \ldots, U_{n, q-1})$. By Theorem 4, $q | (U_{n, 1}, U_{n, 2}, U_{n, 3}, \ldots, U_{n, q-1})$, as required.

We may now prove the important

**Theorem 5.** For any $n \in N$, $(U_{n, 1}, U_{n, 2}, U_{n, 3}, \ldots, U_{n, q-1})$ if and only if $q | (U_{n, 1}, U_{n, 2}, U_{n, 3}, \ldots, U_{n, q-1})$.

**Proof.** Let $p$ be any prime. If $p | U_{n, 1}$, then $q | U_{n, 1}$, hence $(U_{n, 1}, U_{n, 2}, U_{n, 3}, \ldots, U_{n, q-1})$ if and only if $q | (U_{n, 1}, U_{n, 2}, U_{n, 3}, \ldots, U_{n, q-1})$.

Let $p (\not| q)$ be a prime and suppose $p | (U_{n, 1}, U_{n, 2}, U_{n, 3}, \ldots, U_{n, q-1})$. Then, if $q | (U_{n, 1}, U_{n, 2}, U_{n, 3}, \ldots, U_{n, q-1})$, we see that by (3.4),

$$q^2 \equiv 0 \pmod{p}.$$  

Since $q \not| p$, we have $p | (U_{n, 1}, U_{n, 2}, U_{n, 3}, \ldots, U_{n, q-1})$, which is impossible. If $q \not| p$, we may apply the same sort of argument to $a_{q-1}$ in $K[\alpha]$. Hence, $(U_{n, 1}, U_{n, 2}, U_{n, 3}, \ldots, U_{n, q-1}) = q^r$. If $q > 1$, by (3.4), $q | (U_{n, 1}, U_{n, 2}, U_{n, 3}, \ldots, U_{n, q-1})$, this is impossible.

Up to this point, we have dealt completely with the possible divisors of $(U_{n, 1}, U_{n, 2}, \ldots, U_{n, q-1})$. We now concern ourselves with the divisors of the following functions. We define, for any $n \in N$,

$$D_{n, q} = (U_{n, 1}, U_{n, 2}, U_{n, 3}, \ldots, U_{n, q-1}, U_{n+1, 1}, U_{n+1, 2}, \ldots, U_{n+1, q-1}).$$

where $i = 1, 2, 3, \ldots, q-1$ and

$$D_{n, q} = (U_{n, 1}, U_{n, 2}, U_{n, 3}, \ldots, U_{n, q-1}).$$

In the theorems that follow we obtain some of the many remarkable properties of these $D$ functions.

**Theorem 6.** For $i = 0, 1, 2, \ldots, q-1$, $(D_{n, q}, o_i) = 1$.

**Proof.** Let $q | (D_{n, q}, o_i)$. By (3.2), $p | (D_{n, q}, o_i)$. If $p | (D_{n, q}, o_i)$, then $p | (D_{n, q}, o_i)$ and $p = q$. But, if $p = q$, then $q | (D_{n, q}, o_i)$, and $p = q$. This too is impossible.

**Theorem 7.** If $m \not| 2, \ldots, q-1$, then $m | (D_{n, q}, o_i)$.

**Proof.** The theorem is true for $1 = 1$; suppose it is true for $1 = a$.

From (3.3)

$$q | (U_{n, 1}, U_{n, 2}, U_{n, 3}, \ldots, U_{n, q-1})$$

where $i = 1, 2, 3, \ldots, q-1$ and

$$D_{n, q} = (U_{n, 1}, U_{n, 2}, U_{n, 3}, \ldots, U_{n, q-1}).$$

In the theorems that follow we obtain some of the many remarkable properties of these $D$ functions.

**Theorem 8.** For $i = 0, 1, 2, \ldots, q-1$, $(D_{n, q}, o_i) = 1$.

**Proof.** Let $q | (D_{n, q}, o_i)$. By (3.2), $p | (D_{n, q}, o_i)$. If $p | (D_{n, q}, o_i)$, then $p | (D_{n, q}, o_i)$ and $p = q$. But, if $p = q$, then $q | (D_{n, q}, o_i)$, and $p = q$. This too is impossible.

**Theorem 9.** If $m \not| 2, \ldots, q-1$, then $m | (D_{n, q}, o_i)$.

**Proof.** The theorem is true for $1 = 1$; suppose it is true for $1 = a$.

From (3.3)

$$q | (U_{n, 1}, U_{n, 2}, U_{n, 3}, \ldots, U_{n, q-1})$$

where $i = 1, 2, 3, \ldots, q-1$ and

$$D_{n, q} = (U_{n, 1}, U_{n, 2}, U_{n, 3}, \ldots, U_{n, q-1}).$$

In the theorems that follow we obtain some of the many remarkable properties of these $D$ functions.

**Theorem 10.** For $i = 0, 1, 2, \ldots, q-1$, $(D_{n, q}, o_i) = 1$.

**Proof.** Let $q | (D_{n, q}, o_i)$. By (3.2), $p | (D_{n, q}, o_i)$. If $p | (D_{n, q}, o_i)$, then $p | (D_{n, q}, o_i)$ and $p = q$. But, if $p = q$, then $q | (D_{n, q}, o_i)$, and $p = q$. This too is impossible.
THEOREM 8. Let \( m \mid Z \) and \( n \mid Z \). If \((1) q \mid m, (2) q \not\mid U_{\lambda,n}, (3) k = 0, 1 \pmod{q}\), and \( m \mid D_{i,n} \), then \( m \mid qD_{i,n} \) for \( i = k \pmod{q} \) and \( 0 \leq i < q - 1 \). If \((1), (2), (3)\) are not all true and \( m \mid D_{i,n} \), then \( m \mid D_{i,n} \).

Proof. Let \( k = qu + v \), where \( v < q \). We shall prove this theorem by induction on \( v \). Let \( v = 1 \). From (3.3),

\[
qU_{h,n} = \sum_{i=1}^{h-1} U_{i,n} U_{h-i,n} + A \sum_{i=1}^{q-1-h} U_{i+h,n} U_{q-i,n}.
\]

Now \( m \mid D_{h,n} \) and \( m \mid D_{i,n} \); thus, \( q \mid m, \) \( m \mid D_{i,n} \). If \( q \not\mid m, q \mid U_{h,n} \) and \( qm \mid U_{h,n} \) for \( h \neq j \). The theorem is true for \( v = 1 \). Suppose it is true for \( v = u < q - 1 \); then

\[
qU_{h,(k+1)v} = \sum_{i=1}^{h} U_{i,n} U_{h-i,n} + A \sum_{i=1}^{q-1-h} U_{i+h,n} U_{q-i,n}.
\]

By the induction hypothesis, \((1), (2), (3)\) are all true, then \( q \mid A \), which implies \( q \mid A \mid A \)

Hence, \( m \mid D_{h,n} \), where \( k = (w+1)j \). If \( k = 0, 1 \pmod{q} \) and \( m \mid D_{h,n} \), where \( h \neq j \), then \( q \mid U_{i,n} \); by Lemma 4, this is impossible.

By Theorem 7, we see that in the sequence \( D_{i,n}, D_{i+1,n}, \ldots, D_{n,n} \), \( m \mid D_{h,n} \) if \( k, j \). Such a sequence is called a divisibility sequence. Some properties of these sequences have been discussed by Lehmer [4], [5], Pierce [9], and Ward [19].

Theorem 8 shows that the behaviour of the sequence

\[
D_{i,1}, D_{i,2}, \ldots, D_{i,n}, \ldots
\]

for \( i \neq 0 \), is somewhat more complicated. We shall investigate these sequences more fully in the following theorem; however, we shall first introduce a

DEFINITION. For any fixed \( m \mid Z \) let \( D_{h,n} \) be the first term of the sequence \( D_{i,1}, D_{i,2}, \ldots, D_{i,n}, \ldots \) in which \( m \) occurs as a factor. If \( m \) does not occur as a factor in the above sequence, we define \( \ell \mid 0 \). We call \( q \) the rank of apparition of \( m \).

It is clear that \( \ell \) is a function of \( m \) and may be written as \( \ell(m) \); however, there is no doubt as to what the argument is, it is more convenient to omit it.

THEOREM 9. If \( m \mid D_{h,n} \), then \( q \) exists and \( q \mid n \).

Proof. Clearly \( q \exists n \) exists and \( q \leq n \). Suppose \( n = uq + v \), where \( 0 < v < q \). From (3.3),

\[
qU_{h,n} = \sum_{i=1}^{h} U_{i,n} U_{h-i,n} + A \sum_{i=1}^{q-1-h} U_{i+h,n} U_{q-i,n}.
\]

By Theorem 6, \( m \mid D_{h,n} \) and \( m \mid U_{h,n} \); hence, \( m \mid U_{h-n} U_{h-i,n} \) for \( i = 1, 2, \ldots, q-1 \). If \( q \not\mid m, q \mid D_{h,n} \). If \( q \not\mid m, q \mid U_{h-n} \) and \( q \mid D_{h,n} \), then \( q \mid U_{h-n} U_{h-i,n} \); if \( q \mid m, q \mid U_{h-n} \) and \( q \mid D_{h,n} \), finally, if \( q \mid m \) and \( q \mid D_{h,n} \), then \( q \mid U_{h-n} \) and \( q \mid U_{h-n} \). When \( q \mid U_{h-n} U_{h-i,n} \), we have \( q \mid U_{h-n} U_{h-i,n} \); if \( i = 1, 2, \ldots, q-1 \); hence, \( m \mid D_{h,n} \).

If \( q \mid U_{h,n} \), we can find \( v < q \) such that \( m \mid D_{h,n} \); this contradicts the definition of \( q \).

COROLLARY 1. If \( n = (m,n) \), then \( m \not\mid D_{h,n} \) for \( m \mid n \).

Proof. Let \( L = (D_{h,n}, D_{n,n}) \); clearly \( D_{h,n} \mid L \). Let \( q \mid L \) be the rank of apparition of \( L \). We see that \( q \mid m \) and \( q \mid n \) or that \( q \mid v \); thus, \( L \mid D_{h,n} \), which, since \( D_{h,n} \mid L \), implies that \( L = D_{h,n} \).

THEOREM 10. Let \( m \mid D_{h,n} \). Then \( q \exists n \) exists and \( m \mid D_{h,n} \) if \( k = n \pmod{q} \).

Proof. Clearly \( q \exists n \) exists if \( m \mid D_{h,n} \); in fact \( q \mid n \). Since the theorem is true for \( j = 0 \), we may assume \( j \neq 0 \).

If \( h < n \) and \( n = k \pmod{q} \), then \( n = v + k \), where \( v \in N \). From (3.3),

\[
qU_{h,n} = \sum_{i=1}^{h} U_{i,n} U_{h-i,n} + A \sum_{i=1}^{q-1-h} U_{i+h,n} U_{q-i,n}.
\]

hence, \( U_{i,n} U_{h-i,n} = 0 \pmod{m} \) for \( h \neq j \). If \( q \not\mid m \), we have \( m \mid D_{h,n} \).

Case 1: \( q \mid D_{h-n} \). In this case \( q \mid U_{h-n} \) for \( i = 0, 1, 2, \ldots, q-1 \); thus, \( q \mid U_{i,n} U_{h-i,n} \) for \( h \neq j \) and consequently \( m \mid D_{h,n} \).

Case 2: \( q \mid D_{h-n} \). Hence, \( q \mid U_{i,n} U_{h-i,n} \) for \( i = 0, 1, 2, \ldots, q-1 \). This brings us back to case 1.

If \( h > n \) and \( n = k \pmod{q} \), we have \( k = qu + h \) for some \( u \in N \). Also

\[
qU_{h,n} = \sum_{i=1}^{h} U_{i,n} U_{h-i,n} + A \sum_{i=1}^{q-1-h} U_{i+n} U_{h-i,n}.
\]

With the same sort of argument used above, we can easily show that, if \( q \mid m, q \mid U_{h,n} \) for \( h \neq j \) and if \( q \mid m, q \mid U_{h,n} \) for \( h \neq j \).
Suppose $m \mid D_{k, m}, m \mid D_{k, m}, m \mid q$ and $k \equiv n (mod q)$. Since $q \equiv k \equiv q \equiv gn$, we may allow $k' = qk \equiv qn'$, where $k', n' \equiv N$. Since $j \neq 0$, and $m \mid qk$, it is clear that $k', n' \neq 0 (mod q)$. Choose $a, b \equiv N$ such that $n' = k' (mod q)$ and $ax = y (mod q)$, where $0 \leq x \leq q - 1$. Since $k' \equiv n' (mod q)$, we have $i \neq j$. If $q \mid m$, then $m \mid D_{k, m}$, which implies that $m \mid D_{k, m}$. This is impossible if $m \mid q$. If $q \mid m$ and $q \mid U_{k, m}$, we also have $m \mid D_{k, m}$.

Finally, if $q \mid m$ and $q \mid U_{k, m}$, we have $m \mid qD_{k, m}$. Since $q^2 \mid m, m \equiv q, 1$; this too is a contradiction.

We are now able to prove a generalization of Corollary 9.1 in

**Theorem 11.** Let $n = (m, n)$, $m' = m/n$, $n' = n/n$. Suppose $j' \equiv km' (mod q)$ and $m' \equiv j (mod q)$, where $0 \leq j \leq q - 1$. If $q \mid D_{j', m}, q \mid D_{k, m', D_{j', m}}, q \mid D_{k, m}$, then $q \mid D_{j', m}, q \mid D_{k, m}$.

If $q \mid D_{j', m}, q \mid D_{k, m}$, then $q \mid D_{j', m}, q \mid D_{k, m}$.

If $q \mid D_{j', m}, q \mid D_{k, m}$, then $q \mid D_{j', m}, q \mid D_{k, m}$.

The proof of the theorem is true if $j = k = 0$, we shall assume that $j \neq 0$.

Let $j' \equiv km' (mod q)$ and $L = (D_{j', m}, D_{k, m})$, the rank of appearance of $L$, and $m^* = m (mod q)$. Since $q \mid m$ and $q \mid n$, we have $q \mid m^*$.

If $q \mid L$, $L = (D_{j', m}, D_{k, m})$, since $m^* = m (mod q)$, we see, by Theorem 10, that $L = D_{j', m}, D_{k, m}$, if $q \mid D_{j', m}, D_{k, m}, q \mid L$. Hence, if $q \mid L$ and $q \mid D_{j', m}, D_{k, m} = D_{j', m}$, if $q \mid D_{j', m}$ and $q \mid L$, $L = D_{j', m}$.

If $q \mid L = L(q)/D_{j', m}, D_{k, m} = L(q)/D_{j', m}$, if $q \mid D_{j', m}, D_{k, m}, L = D_{j', m}$. If $q \mid D_{j', m}, D_{k, m}, L = D_{j', m}$, if $q \mid D_{j', m}, D_{k, m}, L = D_{j', m}$, then $q \mid D_{j', m}, D_{k, m}, L = D_{j', m}$, if $q \mid D_{j', m}, D_{k, m}, L = D_{j', m}$, when $q^2 \mid L$, $L \mid D_{j', m}, D_{k, m}$, since $q^2 \mid L$, $L \mid D_{j', m}, D_{k, m}$, when $q^2 \mid L$, we have $L = D_{j', m}$.

Let $j' \equiv km' (mod q)$ and $L = (D_{j', m}, D_{k, m})$. Since $q$ cannot divide both of $n'$ and $m^*$ we shall assume $q \equiv nm, q \equiv m'. Let i, h \equiv (k (mod q)) and $h = m' (mod q), where 0 \leq i, h \leq q - 1$. If $q \mid L$ or if $q \mid L$ and $q \mid D_{j', m}, D_{k, m}$, we have $L = D_{j', m}, D_{k, m}$, if $q \mid L$, $L = D_{j', m}$, if $q \mid D_{j', m}$ and $q \mid L$, $L = D_{j', m}$, then, since $L = (D_{j', m}, D_{k, m})$, $j = q^2 \mid L$; thus, $L \mid qD_{j', m}$ and $L \mid q$.

7. The laws of repetition and appearance. So far we have only defined the rank of appearance $q$ of an integer $m \mid e$ without saying anything about its existence or what it is if it should exist. We shall answer these questions in the following theorems.

**Theorem 12 (The Law of Repetition).** If $q > 0$, $p \neq q, 2$ and $p$ is the highest power of a prime $p$ contained in $D_{k, m}$, then the highest power of $p$ contained in $D_{k, m}$, which is a contradiction. Hence, $q^{p^2}$ is the highest power of $q$ dividing $D_{k, m}$.

**Corollary 13.1.** If $n, n \equiv (mod q), D_{k, m}, D_{k, m}, D_{k, m}) = m$.

**Theorem 13 (The Law of Appearance).** Let $p$ be a prime such that $p \mid Q_{Q, j}$ then if $p \mid D_{k, m}$.

\[q^{p^2 - 1} U_{k, m} = \sum_{1}^{p} q^{p^2 (k - 1)} \prod_{k=0}^{p^2 (k - 1)} U_{k, m}^{p^2 - 1},\]
If \( p \mid A, D_{0,p^m} = 0 \pmod{p} \), where \( m \) is the least positive integer such that \( p^m > q \).

Proof. From (3.4) and the fact that \( p \left( i \frac{p^k}{i} \right) \), when no \( i \equiv p^k \), we have
\[
(7.2) \quad q^{p^k - 1} U_{i,p^k} = A^q U_{i,p^k} (\pmod{p}),
\]
where \( i p^k = j (\pmod{q}), 0 \leq i < q-1, \) and \( q_i = (ip^k - j)/q \).

Case 1: \( p \not\mid A, p \equiv 1 \pmod{q} \). Let \( n \) be the index to which \( p \) belongs \( \pmod{q} \); then, by (7.2)
\[
U_{i,p^n} = U_{i,1} (\pmod{p}),
\]
for \( j = 0, 1, 2, \ldots, q-1 \). From (3.1) and (3.2), we have \( U_{i,p^n - 1} \equiv q (\pmod{p}) \) and \( p \mid D_{0,p^n - 1} \).

Case 2: \( p \mid A, p \equiv 1 \pmod{q} \). By (7.2)
\[
U_{i,p^n} = U_{i,1} (\pmod{p}),
\]
thus \( U_{i,p^n - 1} \equiv q (\pmod{p}) \) and \( p \mid D_{0,p^n - 1} \).

Case 3: \( p \mid A, p \equiv 1 \pmod{q} \). Let \( A^{(p^n - 1)/q} \equiv 1 \pmod{p} \); then \( \sum_{k=0}^{q-1} f_k \equiv 0 \pmod{p} \). By (3.3)
\[
q^{p^k - 1} \sum_{i=0}^{q-1} U_{i,a}^\delta = \prod_{\delta = 0}^{q-1} U_{i,a}^\delta (\pmod{p}),
\]
and by (7.2)
\[
U_{i,p^k} = f_i U_{i,1} (\pmod{p}).
\]

Let \( P \) be the ideal generated by \( p \) in \( K(\gamma_1) \). Thus, in \( K(\gamma_1) \),
\[
q^{p^k - 1} \sum_{i=0}^{q-1} U_{i,a}^\delta = \prod_{\delta = 0}^{q-1} f_i U_{i,a}^\delta (\pmod{P}).
\]

By (3.2),
\[
q^{p^k - 1} (U_{i,a} - qQ \delta) = q^{p^k - 1} \sum_{i=0}^{q-1} U_{i,a}^\delta = 0 (\pmod{P}).
\]
This implies that
\[
U_{i,a} = qQ \delta (\pmod{p}) \quad \text{and} \quad p \mid D_{0,a}.
\]

Case 4: \( p \mid A \). Let \( a \) be the least element of \( N \) such that \( p^a > q \).

By (7.3), \( U_{a,p^n} = U_{a,1} (\pmod{p}) \) and \( p \mid D_{0,a} \).

We are able now to discuss the rank of apparition of an arbitrary \( m \in N \).

Definition. For the extended Lucas functions of order \( q \) defined on \( U_{i,1} \) \( (i = 0, 1, 2, \ldots, q-1) \) and \( A \), we define the function \( \Phi : N \rightarrow N+ + \{0 \} \) in the following fashion. If \( p \) is a prime,
\[
\Phi(p) = 0 \quad \text{when} \quad p \mid Q, \quad \Phi(p) = p^k \quad \text{when} \quad p \not\mid Q, \quad p \mid A \quad \text{and} \quad k \text{ is the least integer such that} \quad p^k > q, \quad \Phi(p) = q-1 \quad \text{when} \quad p \not\mid Q \quad \text{and} \quad p \not\mid A, \quad \Phi(p) = p^{q-1} \quad \text{when} \quad p \mid qQ \quad \text{and} \quad p \mid A(\pmod{q}), \quad \Phi(p) = (p^{q-1} - 1)/(p-1) \quad \text{when} \quad p \not\mid qQ \quad \text{and} \quad p \not\mid A(\pmod{q}) \quad \text{and} \quad A^{(p^{q-1} - 1)/q} \equiv 1 (\pmod{p}), \quad \Phi(p) = p^{q-1} \Phi(p) \quad \text{for any prime} \quad p.
\]

If \( m \) is prime, \( m = \prod_{i=0}^{r} p_i^a_i \), where \( p_i \) are distinct primes. We define \( \Phi(m) \) be the least common multiple of \( \Phi(p_i^{a_i}) = \Phi(p_i^{a_i+1}) \), \( \Phi(p_i^{a_i+2}) \), \( \ldots \).

Theorem 14. Let \( m \in N \). If we denote \( \Phi(m) \) by \( \Phi \), we have \( D_{0,a} = 0 (\pmod{m}) \).

Corollary 14.1. If \( (m, Q) = 1 \), the rank of apparition \( e \) of \( m \) exists and \( q \mid \Phi \).

It is interesting to note that the \( D_{0,a} \) functions do not seem to increase as quickly as the Lucas functions. This means that they are more easily factored. For example, if \( q = 3, A = 9, U_{1,1} = 3, U_{1,2} = 3, U_{2,1} = 9, \) we evaluate \( D_{0,3,A} = 17 \times 45367 \). Now \( D_{0,120} = 309, D_{0,125} = 9 \) and \( D_{0,126} = 9 \); hence, \( 9 \times 103 \times D_{0,126} = 188191 \), we notice that if \( p \) is a prime divisor of \( 188191 \), \( p = 1+306k \) or \( p = 1+306k \). This implies that \( p = \pm 1, \pm 35 (\pmod{306}) \). The only numbers of these forms less than the square root of \( 188191 \) are \( 271, 305, 307, 341 \). The third of these numbers is found to be a divisor of \( 188191 \) and we have \( D_{0,306} = 9 \times 103 \times 307 \times 613 \).

We close with a theorem similar to a fundamental theorem of Lucas (777, p. 302), which was used by him in the testing of large integers for primality.

Theorem 15. If \( M \in N \), \( M, 2qD_{0,1} = 1 \) and the rank of apparition \( M \) is either \( M^{p-1} - 1 \) or \( (M^2 - 1)/(M-1) \) or \( (M^2 - 1)/q(M-1) \), then \( M \) is a prime.
Proof. Suppose \( M \) is composite and that \( M = \prod_{i=1}^{r} p_i^{a_i} \), where the \( p_i \) are distinct primes. Clearly \( p_i \nmid qAq_i \); therefore \( q \mid \Phi(p_i) \) and \( \Phi(M) \mid J \), where

\[
J = q \prod_{i=1}^{r} p_i^{a_i-1} \frac{\Phi(p_i)}{q^i}.
\]

Now

\[
\frac{J}{M^{a_i-1}} = q \prod_{i=1}^{r} \frac{p_i^{a_i-1}}{p_i^{a_i-1}} \frac{\Phi(p_i)}{qp_i^{a_i-1}} \leq q \prod_{i=1}^{r} \left( 1 + \frac{1}{p_i} + \frac{1}{p_i^2} + \cdots + \frac{1}{p_i^{a_i-1}} \right) \leq q \prod_{i=1}^{r} \frac{p_i}{q(p_i-1)}.
\]

If \( n = 1 \), we have \( a_i \geq 2 \) and therefore

\[
\frac{J}{M^{a_i-1}} \leq \frac{1}{p_i-1} \leq \frac{1}{2}.
\]

If \( n \geq 2 \),

\[
\frac{J}{M^{a_i-1}} \leq \frac{1}{q} \left( \frac{p_1}{p_1-1} \right) \left( \frac{p_2}{p_2-1} \right) \leq \frac{1}{3} \frac{2}{4} = \frac{1}{2}.
\]

Since \( M > 2 \),

\[
J < M^{a_i-1} - 1 < (M^2 - 1)/(M - 1).
\]

But \( M \mid D_{\alpha} \); hence, \( M \) is prime if the rank of apparition of \( M \) is \( M^{a_i-1} - 1 \) or \( (M^2 - 1)/(M - 1) \).

If the rank of apparition of \( M \) is \( (M^2 - 1)/(M - 1)q \), then

\[
J = s(M^2 - 1)/(M - 1)q, \quad \text{where} \quad s < q.
\]

But \( q \mid J \) and \( q^2 \nmid (M^2 - 1)/(M - 1) \); thus, \( M \) is a prime.

References


[9] T. A. Pierce, The numerical factors of the arithmetical forms \( \prod_n (1 + a_n^m) \), Ann. of Math. 18 (1916), pp. 53–64.


Received on 8. 6. 1979