ACTA ARITHMETICA
XX (1972)

On a generalization of the Lucas functions

by

H. C. WILLIAMS (Toronto)

1. Introduction. Let α, β be the roots of the equation

$$x^2-Px+Q = 0, \tag{1.1}$$

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

$$v_n = \alpha^n+\beta^n,$$
$$u_n = (\alpha^n-\beta^n)/(\alpha-\beta).$$

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

$$\alpha = (v_1+u_1\delta)/2, \quad \beta = (v_1-u_1\delta)/2,$$

where $\delta = \alpha-\beta$. Hence,

$$v_n = \big((v_1+u_1\delta)/2\big)^n+\big((v_1-u_1\delta)/2\big)^n,$$
$$u_n = \delta^{-1}\{\big((v_1+u_1\delta)/2\big)^n-\big((v_1-u_1\delta)/2\big)^n\},$$

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

$$a_j = \frac{1}{q}\sum_{i=0}^{q-1} U_{i,1}\delta^i\omega^{-ij} \quad (j = 0, 1, 2, \ldots, q-1)$$

be the q roots of

$$\sum_{k=0}^{q} x^{q-k}(-1)^k Q_k = 0, \tag{2.1}$$

where $Q_0 = 1$ and $U_{0,1}, U_{1,1}, \ldots, U_{q-1,1} \in Z$. We define

$$U_{k,n}^{(q)} = \delta^{-k} \sum_{j=0}^{q-1} \alpha_j^n \omega^{kj} \quad (k = 0, 1, 2, \ldots, q-1). \tag{2.2}$$

For $q = 3$ the functions $U_{0,n}^{(3)}, U_{1,n}^{(3)}, U_{2,n}^{(3)}$ 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 $\Delta = D$, $U_{0,1} = 3X_1$, $U_{1,1} = 3Y_1$, $U_{2,1} = 3Z_1$, 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

$$X^3 + DY^3 + D^2Z^3 - 3DXYZ = 1, \tag{2.3}$$

then any solution of (2.3) is given by $(U_{0,n}^{(3)}/3, U_{1,n}^{(3)}/3, U_{2,n}^{(3)}/3)$ 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 $U_{k,n}^{(q)}$.

3. Identities. It may be easily shown that the functions $U_{k,m}$ $(k = 0, 1, 2, \ldots, q-1)$, satisfy the following identities:

$$\begin{vmatrix} U_{j,k} & U_{j-1,k} & U_{j-2,k} & \ldots & U_{0,k} & \Delta U_{q-1,k} & \ldots & \Delta U_{j+1,k} \\ U_{1,m} & U_{0,m} & \Delta U_{q-1,m} & \ldots & \ldots & \ldots & \ldots & \Delta U_{2,m} \\ U_{2,m} & U_{1,m} & U_{0,m} & \ldots & \ldots & \ldots & \ldots & \Delta U_{3,m} \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ U_{q-1,m} & U_{q-2,m} & U_{q-3,m} & \ldots & \ldots & \ldots & \ldots & U_{0,m} \end{vmatrix} = q^{q-1} Q_q^m U_{j,k-m}, \tag{3.1}$$

$$\begin{vmatrix} U_{0,n} & \Delta U_{q-1,n} & \Delta U_{q-2,n} & \ldots & \Delta U_{1,n} \\ U_{1,n} & U_{0,n} & \Delta U_{q-1,n} & \ldots & \Delta U_{2,n} \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ U_{q-1,n} & U_{q-2,n} & U_{q-3,n} & \ldots & U_{0,n} \end{vmatrix} = q^q Q_q^n, \tag{3.2}$$

$$q U_{j,n+m} = \sum_{k=0}^{j} U_{k,n} U_{j-k,m} + \Delta \sum_{k=1}^{q-1-j} U_{j+k,n} U_{q-k,m}, \tag{3.3}$$

$$\Big(\sum_{i=0}^{q-1} U_{i,1} \omega^{ji} \delta^i\Big)^n = q^{n-1} \sum_{i=0}^{q-1} U_{i,n} \omega^{ji} \delta^i \quad (j = 0, 1, 2, \ldots, q-1), \tag{3.4}$$

$$U_{j,n+q} = \sum_{k=1}^{q} (-1)^{k+1} Q_k U_{j,n+q-k}. \tag{3.5}$$

From Newtons Formulas, we obtain

$$\sum_{i=0}^{k-1} (-1)^i Q_i U_{0,k-i} + (-1)^k k Q_k = 0 \tag{3.6}$$

and

$$Q_k = \frac{1}{k!} \begin{vmatrix} U_{0,1} & 1 & 0 & \ldots & 0 \\ U_{0,2} & U_{0,1} & 2 & \ldots & 0 \\ U_{0,3} & U_{0,2} & U_{0,1} & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ U_{0,k} & U_{0,k-1} & U_{0,k-2} & \ldots & U_{0,1} \end{vmatrix}, \tag{3.7}$$

where $k \in N$ and $k \leqslant q$.

If

$$\Delta_n = q \begin{vmatrix} U_{1,n} & U_{1,2n} & \ldots & U_{1,(q-1)n} \\ U_{2,n} & U_{2,2n} & \ldots & U_{2,(q-1)n} \\ \ldots & \ldots & \ldots & \ldots \\ U_{q-1,n} & U_{q-1,2n} & \ldots & U_{q-1,(q-1)n} \end{vmatrix},$$

then

$$\begin{vmatrix} U_{j,(q-1)n+r} & U_{j,(q-2)n+r} & \ldots & U_{j,r} \\ U_{j,qn+r} & U_{j,(q-1)n+r} & \ldots & U_{j,n+r} \\ \ldots & \ldots & \ldots & \ldots \\ U_{j,(2q-2)n+r} & U_{j,(2q-3)n+r} & \ldots & U_{j,(q-1)n+r} \end{vmatrix} = (-1)^{(j+1)(q+1)} q^{-q} Q_q^r \Delta_n^2 \Delta^{q-1-j} \tag{3.8}$$

and

$$\begin{vmatrix} U_{0,r} & U_{1,r} & \ldots & U_{q-1,r} \\ U_{0,n+r} & U_{1,n+r} & \ldots & U_{q-1,n+r} \\ \ldots & \ldots & \ldots & \ldots \\ U_{0,(q-1)n+r} & U_{1,(q-1)n+r} & \ldots & U_{q-1,(q-1)n+r} \end{vmatrix} = Q_q^r \Delta_n. \tag{3.9}$$

Finally, we note that if $x_1, x_2, \ldots, x_{q-1}$ are defined as the roots of the $q-1$ linear equations

$$\sum_{i=1}^{q-1} \omega^{ji} x_i = \frac{1}{q} \log \frac{\alpha_j^q}{Q_q} \quad (j = 0, 1, 2, \ldots, q-2),$$

we have

$$U_{j,n} = q Q_q^{n/q} \delta^{-j} y_j(nx_1, nx_2, \ldots, nx_{q-1}), \tag{3.10}$$

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 $U_{j,n}$ $(j = 0, 1, 2, \ldots, q-1)$, 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), (49), (7), (10), (30), and (5) respectively of Lucas [7]. However, one of the most important properties of the ordinary Lucas functions v_n and u_n is that they are both integers for any $n \in N$. We shall prove in Theorem 1 that a necessary condition for $U_{i,n} \in Z$ $(i = 0, 1, 2, \ldots, q-1)$, and n any element of N, is that $Q_i \in Z$ $(i = 1, 2, \ldots, q)$; but we must first give

LEMMA 1. *Let* $h_i(x) = b_0 + \sum_{j=1}^{q-1} b_j(x\omega^{-i})^j$ $(i = 0, 1, 2, \ldots, q-1)$, *where* $b_k \in Z$ *for* $k = 0, 1, 2, \ldots, q-1$, *and* $x \in \mathscr{C}$; *then, if* $f_r(x) = S_r(h_0(x), h_1(x), \ldots \ldots, h_{q-1}(x))$, *where* $S_r(x_1, x_2, \ldots, x_q)$ *is the* r-*th elementary symmetric function of* $x_1, x_2, \ldots, x_q$, *we have*

$$f_r(x) = \binom{q}{r} b_0^r + \sum_{i=1}^{r-1} a_{i,r} x^{iq},$$

where $a_{i,r} \in Z$ $(r = 1, 2, \ldots, q-1;\ i = 1, 2, \ldots, r-1)$.

Proof. This follows easily by observing that f_r is a symmetric polynomial in $x, \omega^{-1}x, \omega^{-2}x, \ldots, \omega^{-q+1}x$ and by using the symmetric function theorem.

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

Proof. By Lemma 1, $q^i Q_i \in Z$ $(i = 0, 1, 2, \ldots, q)$ and by (3.7), $i!\,Q_i \in Z$; hence, if $i < q$, $Q_i \in Z$. Since $U_{i,k} \in Z$ for $i = 0, 1, 2, \ldots, q-1$ and $k = 1, 2, 3, \ldots, q+1$, it follows from (3.5) that $qQ_q \in Z$ and $U_{i,1}Q_q \in Z$ for $i = 0, 1, 2, \ldots, q-1$. If, for some i, [1] $q \nmid U_{i,1}$, $Q_q \in Z$; if $q \mid U_{i,1}$ for $i = 0, 1, 2, \ldots, q-1$, then, by (3.2), we have $q^q \mid q^{q-1}(qQ_q)$ and consequently $Q_q \in Z$.

We may now define the extended Lucas functions of order q.

DEFINITION. Let Δ, $U_{i,1} \in Z$ $(i = 0, 1, 2, \ldots, q-1)$, be chosen such that the expressions (2.2) are rational integers for any $n \in N$ and [1] $(Q_1, Q_2, \ldots, Q_q) = 1$. We call the set of functions $\{U_{i,n};\ i = 0, 1, 2, \ldots, q-1\}$ given by (2.2), a set of *extended Lucas functions of order* q. 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 2 which are not sets of Lucas functions. An example of one of these is given by $\{U_{0,n},\ U_{1,n}\}$, where $\Delta = 5$, $U_{0,1} = 4$, $U_{1,1} = 2$,

(1) If $x, y, z, \ldots$ are rational integers, we write as usual $x \mid y$ for x divides y, $x \nmid y$ for x does not divide y and $(x, y, z, \ldots)$ for the greatest common divisor of $x, y, z, \ldots$

$Q_1 = 4$, 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 q to be an odd prime.

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

5. Preliminary results.

LEMMA 2. *If* $q^2 \mid \Delta$, $r = (q-1)/2$, *and* $q \mid U_{j,1}$ *for* $j = 0, 1, 2, \ldots, r$, *then* $U_{j,n} \in Z$ $(j = 0, 1, 2, \ldots, q-1)$, *and* $q \mid U_{j,n}$ *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* $n \in N$, *then* $q^2 \mid U_{j,n}$ *for* $j = 1, 2, \ldots, r$ *and* $q \mid U_{j,n}$ *for* $j = 0, r+1, r+2, \ldots, q-1$.

Proof. From Lemma 2 and Theorem 1, $Q_k \in Z$ and, by (3.6), $q \mid Q_k$ for $k = 1, 2, \ldots, q-1$. This fact, together with (3.5) and Lemma 2, shows that $q^2 \mid U_{j,q}$ for $j = 1, 2, \ldots, r$ and $q \mid U_{j,q}$ for $j = 0, r+1, \ldots, q-1$; 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* $q \mid U_{j,k}$ *for* $j = 0, 1, 2, \ldots, m$, *where* $m \geqslant r$ *and* $m, n, k \in N$, *then*

$$U_{0,nk} \equiv q(U_{0,k}/q)^n \pmod{q^2},$$

$$U_{m+1,nk} \equiv n(U_{0,k}/q)^{n-1} U_{m+1,k} \pmod{q},$$

$$Q_q \in Z \quad \textit{and} \quad Q_q \equiv U_{0,1}/q \pmod{q}.$$

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

$$U_{0,q} \equiv qQ_q \pmod{q^2};$$

thus,

$$Q_q \equiv U_{0,1}/q \pmod{q}.$$

LEMMA 5. *If* $\Delta = d^q + tq^2$, $U_{j,1} = cd^{q-j-1} + qr_j$ $(j = 0, 1, 2, \ldots, q-1)$ *where* $d, c, t, r_j \in Z$ $(j = 0, 1, 2, \ldots, q-1)$ *and* $q \nmid dc$, *then for any* $n \in N$, $U_{j,n} \in Z$ *and*

$$U_{j,n} \equiv d^{q-j-1}\Big[\Big(c + \sum_{i=0}^{q-1} r_i d^i\Big)^n - \Big(\sum_{i=0}^{q-1} r_i d^i\Big)^n\Big] \pmod{q}$$

for $j = 0, 1, 2, \ldots, q-1$.

Proof. Let $A = \sum_{i=0}^{q-1} r_i d^i$. Suppose that $U_{j,m} = A_m d^{q-j-1} + qR_{j,m}$

$(j = 0, 1, 2, \ldots, q-1)$, where

$$\sum_{j=0}^{q-1} R_{j,m} d^j \equiv A^m \pmod{q} \quad \text{and} \quad A_m \equiv (c+A)^m - A^m \pmod{q}.$$

This supposition is true for $m = 1$. By (3.3)

$$U_{k,m+1} \equiv d^{q-1-k}\Big[(cA_m d^{q-1} + A_m A) + c\sum_{j=0}^{q-1} R_{j,m} d^j\Big] + $$
$$+ q\sum_{j=0}^{k} R_{j,m} r_{k-j} + q d^q \sum_{j=1}^{q-k-1} R_{k+j,m} r_{q-j} +$$
$$+ qctA_m (q-k-1) d^{2(q-1)-k} \pmod{q^2}.$$

Thus,

$$U_{k,m+1} = A_{m+1} d^{q-k-1} + qR_{k,m+1} \qquad (k = 0, 1, 2, \ldots, q-1),$$

where

$$A_{m+1} \equiv (c+A)^{m+1} - A^{m+1} \pmod{q},$$

$$R_{k,m+1} \equiv \sum_{j=0}^{k} R_{j,m} r_{k-j} + d^q \sum_{j=1}^{q-k-1} R_{k+j,m} r_{q-j} +$$
$$+ d^{q-k-1}[ctA_m (q-k-1) d^{q-1} - x] \pmod{q}$$

and

$$x = [(c+A)^{m+1} - A^{m+1} - A_{m+1}]/q.$$

Now

$$\sum_{k=0}^{q-1} R_{k,m+1} d^k \equiv \sum_{k=0}^{q-1} d^k \sum_{j=0}^{k} R_{j,m} r_{k-j} + \sum_{k=q}^{2q-1} d^k \sum_{j=k-q+1}^{q-1} R_{j,m} r_{k-j}$$
$$\equiv \Big(\sum_{k=0}^{q-1} d^k R_{k,m}\Big)\Big(\sum_{k=0}^{q-1} d^k r_k\Big) \equiv A^{m+1} \pmod{q};$$

hence, the lemma follows by induction.

LEMMA 6. *If the conditions of Lemma 5 are true, then* $Q_i \in Z$ *for* $i = 1, 2, \ldots, q$ *and*

$$Q_i \equiv (-1)^{i+1} c\Big(\sum_{j=0}^{q-1} r_j d^j\Big)^{i-1} \pmod{q} \qquad (i < q),$$

$$Q_q \equiv c\Big(\sum_{i=0}^{q-1} r_i d^i\Big)^{q-1} + \sum_{i=0}^{q-1} r_i d^i \pmod{q}.$$

Proof. The first two results follow from Lemma 5, Theorem 1, and (3.6) by using induction on i. The last result follows by using (3.5) to represent $U_{0,q+1}$.

LEMMA 7. *If* $q \mid U_{i,1}$ *for* $i = 0, 1, 2, \ldots, q-1$, *then, for any* $n \in N$, $U_{i,n} \in Z$ *and* $q \mid U_{i,n}$ $(i = 0, 1, 2, \ldots, q-1)$ *also* $Q_i \in Z$ *and* $q \mid Q_i$ $(i = 1, 2, 3, \ldots, q-1)$. *Finally* $Q_q \in Z$ *and*

$$Q_q^n \equiv \sum_{i=0}^{q-1} (U_{i,n}/q) \Delta^i \pmod{q}.$$

Proof. The first result follows on using (3.3) and induction on n. By Theorem 1, $Q_i \in Z$ for $i = 1, 2, 3, \ldots, q$. From (3.6), $q \mid Q_i$ for $i = 1, 2, \ldots, q-1$ and by (3.5) and (3.3)

$$U_{0,qn} \equiv qQ_q^n \pmod{q^2}.$$

We also have

$$U_{0,qn} = \sum_{i=0}^{q-1}\Big(\sum_{j=0}^{q-1} (U_{j,n}/q)\,\delta^j \omega^{-ij}\Big)^q \equiv q\sum_{i=0}^{q-1} (U_{i,n}/q)^q \Delta^i \pmod{q^2}.$$

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

THEOREM 2. *The functions* $U_{i,n}$ *for* $i = 0, 1, 2, \ldots, q-1$ *will all be rational integers for any* $n \in N$ *if and only if one of the following is true:*

(i) $q \mid U_{i,1}$ $(i = 0, 1, 2, \ldots, q-1)$,

(ii) $q^2 \mid \Delta$, $q \mid U_{i,1}$ $(i = 0, 1, 2, \ldots, r)$,

(iii) $\Delta \equiv d^q \pmod{q^2}$, $U_{i,1} \equiv cd^{q-i-1} \pmod{q}$, *where* $q \nmid cd$.

Proof. From the preceding lemmas, it is clear that the theorem gives sufficient conditions for $U_{i,n} \in Z$ $(i = 0, 1, 2, \ldots, q-1)$. We need only prove the necessity of (i), (ii), or (iii).

Case 1: $\delta \notin Z$. Let $\Delta = d_1 d_2^2 d_3^3 \ldots d_{q-1}^{q-1} d_q^q$, where $d_1, d_2, \ldots, d_q \in Z$ and $d_1 d_2 d_3 \ldots d_{q-1}$ has no square factor in Z. It is evident that this representation of Δ is unique. Let

$$g_i = \prod_{s=1}^{q} d_s^{(si-i_s)/q} \qquad (i = 1, 2, \ldots, q-1)$$

where $i_s \equiv si \pmod{q}$ and $0 \leqslant i_s < q$. We now define $\gamma_i = \delta^i/(g_i d_q^{i-1})$ for $i = 1, 2, \ldots, q-1$, $e = d_1 d_2^2 \ldots d_{q-2}^{q-2}$, and $d = ed_q$. Let $K(\gamma_1)$ be the algebraic number field formed by adjoining γ_1 to Z.

By Theorem 1, $Q_1, Q_2, \ldots, Q_q \in Z$ and $Q_0 = 1$; hence

$$\alpha_0 = \frac{1}{q}\sum_{i=0}^{q-1} U_{i,1}\delta^i$$

is an algebraic integer in $K(\gamma_1)$.

If $q^2 \nmid (e^{q-1} - d_{q-1}^{q-1})$, by Westlund [13],

$$a_0 = x_0 + \sum_{i=1}^{q-1} x_i \gamma_i,$$

where $x_i \in Z$ $(i = 0, 1, 2, \ldots, q-1)$. As a consequence of this, $q \mid U_{i,1} g_i d_q$ for $i = 1, 2, \ldots, q-1$ and $q \mid U_{0,1}$. If $q \mid U_{i,1}$ $(i = 0, 1, 2, \ldots, q-1)$, we obtain (i). If $q \mid d_q g_i$ for some $i \geq 1$, then $q^2 \mid \Delta$. Since $U_{i,2}$ 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 $q^2 \mid (e^{q-1} - d_{q-1}^{q-1})$, then $\Delta \equiv d^q \pmod{q^2}$ and (Westlund [13])

$$a_0 = x_0 \varepsilon + \sum_{i=1}^{q-1} x_i \gamma_i,$$

where $x_i \in Z$ $(i = 0, 1, 2, \ldots, q-1)$ and $q\varepsilon = 1 + \sum_{i=1}^{q-1} \gamma_1^i e^{q-1-i}$. Since

$$U_{0,1} + \sum_{i=1}^{q-1} U_{i,1} g_i d_q^i \gamma_i = x_0 + \sum_{i=1}^{q-1} (g_i e^{q-i-1} x_0 + q x_i) \gamma_i,$$

we have

$$U_{0,1} = x_0,$$

$$U_{i,1} g_i d_q^i \equiv g_i e^{q-1-i} x_0 \pmod{q},$$

for $i = 1, 2, \ldots, q-1$. If $q \mid U_{0,1}$, then $q \mid U_{i,1}$ $(i = 0, 1, 2, \ldots, q-1)$ or $q^2 \mid \Delta$ and $q \mid U_{i,1}$ $(i = 0, 1, 2, \ldots, r)$. Since $(e, d_{q-1}) = 1$, $q \nmid e$, $q \nmid d_{q-1}$, and $q \nmid g_i$ for $i = 1, 2, \ldots, q-1$. Thus, if $q \nmid U_{0,1} d_q$,

$$U_{i,1} \equiv c d^{q-i-1} \pmod{q},$$

where $q \nmid cd$.

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

$$a_{q-1} = \frac{1}{q} \sum_{i=0}^{q-1} U_{i,1} d_q^i \omega^i, \quad \text{where} \quad d_q \in Z,$$

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

$$a_{q-1} = \sum_{i=0}^{q-2} x_i \omega^i, \quad \text{where} \quad x_i \in Z \quad (i = 0, 1, 2, \ldots, q-2)$$

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

$$U_{i,1} d_q^i \equiv U_{q-1,1} d_q^{q-1} \pmod{q}.$$

If $q \mid d_q$, $q^2 \mid \Delta$ and we have case (ii). If $q \nmid d_q$ and $q \mid U_{q-1,1}$, then $q \mid U_{i,1}$ $(i = 0, 1, 2, \ldots, q-1)$; this is case (i). Finally, if $q \nmid U_{q-1} d_q$,

$$U_{i,1} \equiv c d^{q-1-i} \pmod{q} \quad (i = 0, 1, 2, \ldots, q-1),$$

$$\Delta \equiv d^q \pmod{q^2}, \quad \text{and} \quad q \nmid cd.$$

The conditions on $U_{i,1}$ $(i = 0, 1, 2, \ldots, q-1)$ and Δ which guarantee that $(Q_1, Q_2, Q_3, \ldots, Q_q) = 1$ are given in

THEOREM 3. *If $q \mid U_{i,1}$ for $i = 0, 1, 2, \ldots, q-1$, $(Q_1, Q_2, \ldots, Q_q) = 1$ if and only if $(U_{0,1}, U_{1,1}, U_{2,1}, \ldots, U_{q-1,1}) = q$, $(\Delta, U_{0,1}) = 1$, and $q^2 \nmid \sum_{i=0}^{q-1} U_{i,1} \Delta^i$ or $(U_{0,1}, U_{1,1}, U_{2,1}, \ldots, U_{q-1,1}) = q$, $(\Delta, U_{0,1}) = q$, and $q^2 \nmid U_{0,1}$.*

If $q^2 \mid \Delta$, $q \mid U_{i,1}$ for $i = 0, 1, 2, \ldots, r$, and $q \nmid U_{k,1}$ for some k, then $(Q_1, Q_2, \ldots, Q_q) = 1$ if and only if $(\Delta, U_{0,1}) = q$ and $(U_{0,1}, U_{1,1}, \ldots, U_{q-1,1}) = 1$.

If $\Delta \equiv d^q \pmod{q^2}$ and $U_{i,1} \equiv c d^{q-1-i} \pmod{q}$, for $i = 0, 1, 2, \ldots, q-1$ and $q \nmid cd$, $(Q_1, Q_2, \ldots, Q_q) = 1$ if and only if $(\Delta, U_{0,1}) = (U_{0,1}, U_{1,1}, U_{2,1}, \ldots, U_{q-1,1}) = 1$.

Proof. Since the proofs of these three results are similar, we shall prove the first only.

Let p $(\neq q)$ be a prime. If $p \mid (U_{0,1}, U_{1,1}, \ldots, U_{q-1,1})$ or $p \mid (U_{0,1}, \Delta)$, by Lemma 1, $p \mid q^i Q_i$ for $i = 1, 2, \ldots, q$. Thus, if $(Q_1, Q_2, \ldots, Q_q) = 1$, we have $(U_{0,1}, U_{1,1}, \ldots, U_{q-1,1}) = q^\nu$ and $(U_{0,1}, \Delta) = q^\mu$. If μ or $\nu \geq 2$, by Lemma 7, $q \mid (Q_1, Q_2, \ldots, Q_q)$; hence, if $(Q_1, Q_2, \ldots, Q_q) = 1$, $(U_{0,1}, U_{1,1}, \ldots$ $\ldots, U_{q-1,1}) = q$ and $(U_{0,1}, \Delta) \mid q$. If, further, $(U_{0,1}, \Delta) = 1$, $q^2 \nmid \sum_{i=0}^{q-1} U_{i,1} \Delta^i$; or, if $(U_{0,1}, \Delta) = q$, $q^2 \nmid U_{0,1}$.

Suppose $p \mid (Q_1, Q_2, \ldots, Q_q)$. If $p \mid \Delta$, then $p \mid (U_{0,1}, \Delta)$. If $p \nmid \Delta$ and $\delta \notin Z$, let $K[\gamma_1]$ be the ring of algebraic integers in $K(\gamma_1)$ and let $P = [p]$ be the ideal generated in $K[\gamma_1]$ by p. Since $p \neq q$, p does not divide the discriminant of $K(\gamma_1)$; consequently, $P = P_1 P_2 \ldots P_k$, where the P_i are distinct prime ideals in $K[\gamma_1]$.

Since

$$a_0^q = \sum_{i=1}^{q} (-1)^{i+1} Q_i a_0^{q-i},$$

we have

$$a_0 \equiv 0 \pmod{P_i} \quad (i = 1, 2, \ldots, k).$$

Thus, $a_0 \equiv 0 \pmod{P}$ or $a_0 = pI$, where $I \in K[\gamma_1]$. It follows that $p \mid (U_{0,1}, U_{1,1}, \ldots, U_{q-1,1})$. If $p \nmid \Delta$ and $\delta \in Z$, we use a similar argument on a_{q-1} in $K(\omega)$.

We assume throughout the remaining portion of this paper that the symbol $U_{i,n}$ represents an extended Lucas function of order q and that $n \in N$.

6. Properties of the extended Lucas functions. We shall demonstrate a great many properties of the functions $U_{i,n}$, which are similar to properties possessed by the ordinary Lucas functions v_n and u_n. 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 $(U_{0,n}, U_{1,n}, U_{2,n}, \ldots, U_{q-1,n})$ by q in

THEOREM 4. *Let n be any element of N. If $q \mid Q_1$, $q \nmid Q_q$, and $q \mid (U_{0,1}, U_{1,1}, \ldots, U_{q-1,1})$, then $q \mid (U_{0,n}, U_{1,n}, \ldots, U_{q-1,n})$.*

If $q \mid Q_1$, $q \nmid Q_q$ and $q \nmid U_{i,1}$ for some $i > r$, then $q \mid (U_{0,n}, U_{1,n}, \ldots, U_{q-1,n})$ if and only if $q \mid n$.

If $q \nmid Q_1$ and $q \mid Q_q$, then $q \nmid (U_{0,n}, U_{1,n}, \ldots, U_{q-1,n})$.

If $q \nmid Q_1$ and $q \nmid Q_q$, then $q \mid (U_{0,n}, U_{1,n}, \ldots, U_{q-1,n})$ if and only if $t \mid n$, where t is the least positive integer such that $q \mid U_{0,t}$.

Proof. These results follow easily from the preceding lemmas. It should be noted that in the case of the last result $t \mid q-1$.

LEMMA 8. *If $q \mid (U_{0,n}, U_{1,n}, \ldots, U_{q-1,n})$ or $q \mid (U_{0,n}, \Delta)$ then $q \nmid Q_q$.*

Proof. Suppose $q \mid (U_{0,n}, U_{1,n}, \ldots, U_{q-1,n})$ and $q \mid Q_q$. By Theorem 4, $q \mid Q_1$; and, by Lemmas 7 and 3, $q \mid (Q_1, Q_2, \ldots, Q_{q-1})$; this is not possible. Suppose $q \mid (U_{0,n}, \Delta)$ and $q \mid Q_q$. By (3.3), we see that $q \mid (U_{0,1}, \Delta)$, which, under the assumption that $q \mid Q_q$, is also impossible.

We may now prove the important

THEOREM 5. *For any $n \in N$, $(U_{0,n}, \Delta) \mid q$ and $(U_{0,n}, U_{1,n}, U_{2,n}, \ldots, U_{q-1,n}) \mid q$.*

Proof. Let p be any prime. If $p \mid U_{0,n}$ and $p \mid \Delta$, by (3.3), $p \mid U_{0,1}$; hence $(\Delta, U_{0,n}) = q^{\nu}$. If $\nu > 1$, by Lemmas 3, 4 and 7, $q \mid Q_q$; this is contrary to Lemma 8.

Let p $(\neq q)$ be a prime and suppose $p \mid (U_{0,n}, U_{1,n}, \ldots, U_{q-1,n})$. Then, if $\delta \notin Z$ and P is the ideal generated by p in $K[\gamma_1]$, we see that by (3.4),

$$q a_0^n \equiv 0 \pmod{P}.$$

Since $p \nmid q\Delta$, we have $p \mid (U_{0,1}, U_{1,1}, \ldots, U_{q-1,1})$, which is impossible. If $\delta \in Z$, we may apply the same sort of argument to a_{q-1} in $K[\omega]$. Hence, $(U_{0,n}, U_{1,n}, \ldots, U_{q-1,n}) = q^{\nu}$. If $\nu > 1$, by (3.2), $q \mid Q_q$; by Lemma 8, this is impossible.

Up to this point, we have dealt completely with the possible divisors of $(U_{0,n}, U_{1,n}, \ldots, U_{q-1,n})$. We now concern ourselves with the divisors of the following functions. We define, for any $n \in N$,

$$D_{i,n} = (U_{0,n}, U_{1,n}, U_{2,n}, \ldots, U_{i-1,n}, U_{i+1,n}, \ldots, U_{q-1,n})$$

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

$$D_{0,n} = (U_{1,n}, U_{2,n}, U_{3,n}, \ldots, U_{q-1,n}).$$

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

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

Proof. Let $p \mid (D_{i,n}, Q_q)$. By (3.2), $p \mid \Delta^i U_{i,n}^q$. If $p \mid U_{i,n}$, $p \mid (U_{i,n}, D_{i,n})$ and $p = q$. But, if $p = q$, $p \mid Q_q$; this is impossible. If $p \mid \Delta$, $p \mid (\Delta, U_{0,n})$; hence, $p = q$. This too is impossible.

THEOREM 7. *If $m \in Z$, $l \in N$ and $m \mid D_{0,n}$, then $m \mid D_{0,ln}$.*

Proof. The theorem is true for $l = 1$; suppose it is true for $l = s$. From (3.3)

$$qU_{j,(s+1)n} = \sum_{k=0}^{j} U_{k,ns} U_{j-k,s} + \Delta \sum_{k=1}^{q-j-1} U_{j+k,ns} U_{q-k,s}.$$

If $q \nmid m$, $m \mid U_{j,(s+1)n}$ for $j = 1, 2, \ldots, q-1$. If $q \mid m$, from (3.2), $q \mid U_{0,n}$ and, by Theorem 4, $q \mid U_{0,sn}$; therefore, $qm \mid qU_{j,(s+1)n}$ for $j = 1, 2, \ldots, q-1$. The theorem follows by induction.

We obtain a more general result than Theorem 7 in Theorem 8; however, we must first prove

LEMMA 9. *If $m \in Z$ and $m \mid D_{i,n}$, then $m \mid D_{0,qn}$.*

Proof. By the preceding theorem, we may assume $i \neq 0$. From (3.4), we get

$$q^{q-1} U_{j,qn} = \sum \binom{q}{i_0\, i_1 \ldots i_{q-1}} \Delta^{\frac{1}{q}\left(\sum_{k=0}^{q-1} k i_k - j\right)} \prod_{k=0}^{q-1} U_{k,n}^{i_k}, \tag{6.1}$$

where the sum is taken over all possible sets $\{i_0, i_1, i_2, \ldots, i_{q-1}\}$ of non-negative integers such that $\sum_{k=0}^{q-1} i_k = q$ and $\sum_{k=0}^{q-1} k i_k \equiv j \pmod{q}$. Let $\{h_{j0}, h_{j1}, h_{j2}, \ldots, h_{jq-1}\}$ be any such set and let $m = q^{\nu} m'$, where $(m', q) = 1$. If $j > 0$, it is clear that $m' \mid \prod_{k=0}^{q-1} U_{k,n}^{h_{jk}}$; hence $m' \mid U_{j,qn}$ for $j > 0$.

If $\nu > 1$, we see that either $q \mid (U_{0,n}, D_{0,n})$ or $q \mid U_{l,n}$ for $l = 0, 1, 2, \ldots, r$ and $q^2 \mid \Delta$. In the first case, we have

$$q^{\nu(q-h_{ji})+h_{ji}} \,\Big|\, \prod_{k=0}^{q-1} U_{k,n}^{h_{jk}},$$

where $h_{ji} \leqslant q-1$, for $j > 0$. Since $\nu(q-h_{ji}) + h_{ji} \geqslant q+\nu-1$, when $\nu \geqslant 1$ and $h_{ji} \leqslant q-1$, from (6.1) we have $q^{\nu} \mid U_{j,qn}$ for $j > 0$. In the second case, since $i \neq 0$, and $(\Delta, U_{0,n}) \mid q$, $\nu = 1$. By Lemma 3, $q \mid U_{j,qn}$ for $j \geqslant 0$. Thus, $q^{\nu} m' \mid D_{0,qn}$.

THEOREM 8. *Let* $m \in Z$ *and* $k \in N$. *If* (1) $q|m$, (2) $q \nmid U_{j,n}$, (3) $k \equiv 0, 1 \pmod q$, *and* $m|D_{j,n}$, *then* $m|qD_{i,kn}$ *and* $m \nmid D_{i,kn}$, *where* $i \equiv kj \pmod q$ *and* $0 \leqslant i \leqslant q-1$. *If* (1), (2), (3) *are not all true and* $m|D_{j,n}$, *then* $m|D_{i,kn}$.

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

$$qU_{h,kn} = \sum_{l=0}^{h} U_{l,qun}U_{h-l,n} + \Delta \sum_{l=1}^{q-1-h} U_{l+h,qun}U_{q-l,n}.$$

Now $m|D_{0,qun}$ and $m|D_{j,n}$; thus, if $q \nmid m$, $m|D_{j,kn}$. If $q|m$, $q|U_{0,qun}$ and $qm|qU_{h,kn}$ for $h \neq j$. The theorem is true for $v = 1$. Suppose it is true for $v = w < q-1$; then

$$qU_{h,(k+1)n} = \sum_{l=0}^{h} U_{l,kn}U_{h-l,n} + \Delta \sum_{l=1}^{q-1-h} U_{l+h,kn}U_{q-l,n}.$$

By the induction hypothesis, if (1), (2), (3) are not all true, $m|D_{i,kn}$, where $i \equiv wj \pmod q$ and $0 \leqslant i \leqslant q-1$. Suppose $q \nmid m$. If $i+j < q$, $m|U_{h,kn}$ for $h \neq i+j$; if $i+j \geqslant q$, $m|U_{h,kn}$ for $h \neq i+j-q$. If $q|m$, we have $qm|qU_{h,kn}$ for $h \neq i+j$, when $i+j < q$ and $qm|qU_{h,kn}$ for $h \neq i+j-q$, when $i+j \geqslant q$. Thus, $m|D_{h,kn}$, where $h \equiv i+j \equiv (w+1)j \pmod q$.

If (1), (2), (3) are all true, then $q^2|\Delta$, which implies that $\left(\dfrac{m}{q}, q\right) = 1$. Hence, $\dfrac{m}{q}\Big| D_{h,kn}$, where $h \equiv (w+1)j \pmod q$. If $k \equiv 0, 1 \pmod q$ and $m|D_{h,kn}$, where $h \neq j$, then $q|U_{j,kn}$; by Lemma 4, this is impossible.

By Theorem 7, we see that, in the sequence $D_{0,1}, D_{0,2}, \ldots, D_{0,n}, \ldots$, we have $D_{0,k}|D_{0,j}$ if $k|j$. Such a sequence is called a *divisibility sequence*. Some properties of these sequences are given in Ward [11]. Other types of divisibility sequences have been discussed by Lehmer [4], [5], Pierce [9], and Ward [12]. 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 theorems; however, we shall first introduce a

DEFINITION. For any fixed $m \in Z$ let D_{i,ϱ_i} 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 $\varrho_i = 0$. We call $\varrho = \varrho_0$ the rank of apparition of m.

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

THEOREM 9. *If* $m|D_{0,n}$, *then* ϱ *exists and* $\varrho|n$.

Proof. Clearly ϱ exists and $\varrho \leqslant n$. Suppose $n = u\varrho+v$, where $0 < v < \varrho$. From (3.3),

$$qU_{i,n} = \sum_{k=0}^{i} U_{k,u\varrho}U_{i-k,v} + \Delta \sum_{k=1}^{q-1-i} U_{i+k,u\varrho}U_{q-k,v}.$$

By Theorem 6, $m|D_{0,u\varrho}$; hence, $m|U_{0,u\varrho}U_{i,v}$ for $i = 1, 2, \ldots, q-1$. If $q \nmid m$, $m|D_{0,v}$. If $q|m$, $q|Q_1$ and $q|D_{0,1}$, then $q|(U_{0,v}, D_{0,v})$; if $q|m$, $q|Q_1$, and $q \nmid D_{0,1}$, $q|n$, $q|\varrho$ and $q|v$ and $q|(U_{0,v}, D_{0,v})$; finally, if $q|m$ and $q \nmid Q_1$, then $t|n$, $t|\varrho$ and $t|v$ and $q|(U_{0,v}, D_{0,v})$. When $q|(U_{0,v}, D_{0,v})$, we have $qm|U_{0,u\varrho}U_{i,v}$ for $i = 1, 2, \ldots, q-1$; hence, $m|D_{0,v}$. If $\varrho \nmid n$, we can find a $v < \varrho$ such that $m|D_{0,v}$, this contradicts the definition of ϱ.

COROLLARY 9.1. *If* $\nu = (m, n)$, *where* $m, n \in N$, *then*

$$D_{0,\nu} = (D_{0,m}, D_{0,n}).$$

Proof. Let $L = (D_{0,m}, D_{0,n})$; clearly $D_{0,\nu}|L$. Let ϱ be the rank of apparition of L. We see that $\varrho|m$ and $\varrho|n$ or that $\varrho|\nu$; thus, $L|D_{0,\nu}$, which, since $D_{0,\nu}|L$, implies that $L = D_{0,\nu}$.

THEOREM 10. *Let* $m|D_{j,n}$. *Then* ϱ *exists and* $m|D_{j,k}$ *if* $k \equiv n \pmod \varrho$. *If* $m|D_{j,k}$ *and* $m \nmid q$, *then* $n \equiv k \pmod \varrho$.

Proof. Clearly ϱ exists if $m|D_{j,n}$; in fact $\varrho|qn$. Since the theorem is true for $j = 0$, we may assume $j \neq 0$.

If $k < n$ and $n \equiv k \pmod \varrho$, then $n = \varrho u+k$, where $u \in N$. From (3.3),

$$qU_{h,n} = \sum_{i=0}^{h} U_{i,\varrho u}U_{h-i,k} + \Delta \sum_{i=1}^{q-h-1} U_{i+h,\varrho u}U_{q-i,k};$$

hence, $U_{0,\varrho u}U_{h,k} \equiv 0 \pmod m$ for $h \neq j$. If $q \nmid m$, we have, $m|D_{j,k}$. If $q|m$, we have three possible cases.

Case 1: $q|Q_1$, $q \nmid Q_q$, $q|D_{0,1}$. In this case $q|U_{i,k}$ for $i = 0, 1, 2, \ldots$ $\ldots, q-1$; thus, $qm|U_{0,\varrho u}U_{h,k}$ for $h \neq j$ and consequently $m|D_{j,k}$.

Case 2: $q|Q_1$, $q \nmid Q_q$, $q \nmid D_{0,1}$. Here, $q^2|\Delta$, $q^2 \nmid m$ and $q|\varrho$; hence, by Lemma 3, $qm|U_{i,\varrho u}$ for $1 \leqslant i \leqslant r$ and $q|U_{i,k}$ for $0 \leqslant i \leqslant r$. We see once again that $qm|U_{0,\varrho u}U_{h,k}$ for $h \neq j$.

Case 3: $q \nmid Q_1$. Since $t|n$ and $t|\varrho$, $t|k$ and $q|U_{i,k}$ for $i = 0, 1, 2, \ldots$ $\ldots, q-1$. This brings us back to case 1.

If $k > n$ and $n \equiv k \pmod p$, we have $k = \varrho u+n$ for some $u \in N$. Also

$$qU_{h,k} = \sum_{i=0}^{h} U_{i,\varrho u}U_{h-i,n} + \Delta \sum_{i=1}^{q-h-1} U_{i+h,\varrho u}U_{q-i,n}.$$

With the same sort of argument used above, we can easily show that, if $q \nmid m$, $m|qU_{h,k}$ for $h \neq j$ and if $q|m$, $qm|qU_{h,k}$ for $h \neq j$.

Suppose $m\,|\,D_{j,n}$, $m\,|\,D_{j,k}$, $m \nmid q$ and $k \not\equiv n \pmod{\varrho}$. Since $\varrho\,|\,qk$ and $\varrho\,|\,qn$, we may allow $k' = qk/\varrho$ and $n' = qn/\varrho$, where $k', n' \in N$. Since $j \neq 0$, and $m \nmid q$, it is clear that $k', n' \not\equiv 0 \pmod{q}$. Choose x, $i \in N$ such that $n'x \equiv k' \pmod{q}$ and $xj \equiv i \pmod{q}$, where $0 \leqslant i \leqslant q-1$. Since $k' \not\equiv n' \pmod{q}$, we have $i \neq j$. If $q \nmid m$, then $m\,|\,D_{i,xn}$, which implies that $m\,|\,D_{i,k}$. This is impossible if $m \nmid q$. If $q\,|\,m$ and $q\,|\,U_{j,n}$, we also have $m\,|\,D_{i,xn}$. Finally, if $q\,|\,m$ and $q \nmid U_{j,n}$, we have $m\,|\,qD_{i,xn}$. Since $q^2 \nmid m$, $\dfrac{m}{q} \neq q, 1$; this too is a contradiction.

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

THEOREM 11. *Let* $\nu = (m, n)$, $m' = m/\nu$, $n' = n/\nu$. *Suppose* $jn' \equiv km' \pmod{q}$ *and* $m'l \equiv j \pmod{q}$, *where* $0 \leqslant l \leqslant q-1$.

If $q\,|\,(D_{l,\nu}, D_{k,n}, D_{j,m})$ *or* $q \nmid D_{l,\nu}$ *and* $q \nmid (D_{j,m}, D_{k,n})$, $D_{l,\nu} = (D_{k,n}, D_{j,m})$.

If $q \nmid D_{l,\nu}$ *and* $q\,|\,(D_{j,m}, D_{k,n})$, $qD_{l,\nu} = (D_{k,n}, D_{j,m})$.

If $q\,|\,D_{l,\nu}$ *and* $q \nmid (D_{j,m}, D_{k,n})$, $D_{l,\nu} = q(D_{j,m}, D_{k,n})$.

On the other hand, if $jn' \not\equiv km' \pmod{q}$, *then* $(D_{j,m}, D_{k,n})\,|\,q$.

Proof. The theorem is true if $j = k = 0$, we shall assume that $j \neq 0$. Let $jn' \equiv km' \pmod{q}$, $L = (D_{k,n}, D_{j,m})$, ϱ be the rank of apparition of L, and $m^* m' \equiv 1 \pmod{q}$, where $m^* \in N$. Since $\varrho\,|\,qm$ and $\varrho\,|\,qn$, we have $\varrho\,|\,q\nu$.

If $q \nmid L$, $L\,|\,D_{l,m^*m}$. Since $m^*m = \nu m'm^* \equiv \nu \pmod{q\nu}$, we see, by Theorem 10, that $L\,|\,D_{l,\nu}$. If $q \nmid D_{l,\nu}$, $D_{l,\nu}\,|\,L$; if $q\,|\,D_{l,\nu}$, $D_{l,\nu}\,|\,qL$. Hence, if $q \nmid L$ and $q \nmid D_{l,\nu}$, $L = D_{l,\nu}$; if $q\,|\,D_{l,\nu}$ and $q \nmid L$, $qL = D_{l,\nu}$.

If $q\,|\,L$, $(L/q)\,|\,D_{l,m^*m}$ and $(L/q)\,|\,D_{l,\nu}$. If $q \nmid D_{l,\nu}$, $D_{l,\nu}\,|\,L$; thus, $L = qD_{l,\nu}$. If $q\,|\,D_{l,\nu}$, then $D_{l,\nu}\,|\,qL$, when $q^2\,|\,\Delta$ and $D_{l,\nu}\,|\,L$ when $q^2 \nmid \Delta$. When $q^2 \nmid \Delta$, $L\,|\,D_{l,\nu}$ and $L = D_{l,\nu}$. When $q^2\,|\,\Delta$, $L\,|\,qD_{l,\nu}$; since $q^2 \nmid L$ and $q^2 \nmid D_{l,\nu}$, we have $L = D_{l,\nu}$.

Let $jn' \not\equiv km' \pmod{q}$ and $L = (D_{k,n}, D_{j,m})$. Since q cannot divide both of n' and m' we shall assume $q \nmid n'$. Let $i, h \in Z$ such that $n'i \equiv k \pmod{q}$ and $h \equiv m'i \pmod{q}$, where $0 \leqslant i, h \leqslant q-1$. If $q \nmid L$ or if $q\,|\,L$ and $q^2 \nmid \Delta$, we have $L\,|\,D_{i,\nu}$ and $L\,|\,D_{h,m}$, where $h \neq j$; hence, $L\,|\,q$. If $q\,|\,L$ and $q^2\,|\,\Delta$, then, since $L\,|\,D_{j,m}$, where $j \neq 0$, $q^2 \nmid L$; thus, $L\,|\,qD_{h,m}$ and $L\,|\,q$.

7. The laws of repetition and apparition. So far we have only defined the rank of apparition ϱ of an integer $m \in Z$ 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 for* $\nu > 0$, $p^\nu \neq q, 2$ *and* p^ν *is the highest power of a prime* p *contained in* $D_{0,m}$, *then the highest power of* p *contained in* $D_{0,m\mu p^a}$, *where* $(\mu, p) = 1$, *is* $p^{a+\nu}$. *If* $p^\nu = q, 2$ *and* $(\mu, p) = 1$, $D_{0,m\mu p^a}$ *contains the factor* p^{a+1} *and* $p^2 \nmid D_{0,\mu m}$.

Proof. By (3.4),

$$q^{p-1} U_{j,mp} = \sum \binom{p}{i_0, i_1 i_2 \ldots i_{q-1}} \Delta^{\frac{1}{q}\left(\sum\limits_{k=0}^{q-1} k i_k - j\right)} \prod_{k=0}^{q-1} U_{k,m}^{i_k}, \tag{7.1}$$

where the sum is taken over all sets $\{i_0, i_1, i_2, \ldots, i_{q-1}\}$ whose elements are non-negative integers and such that $\sum\limits_{k=0}^{q-1} i_k = p$, $\sum\limits_{k=0}^{q-1} k i_k \equiv j \pmod{q}$. Let $\{h_{j0}, h_{j1}, \ldots, h_{jq-1}\}$ be such a set and suppose $p \neq q$. If $j > 0$, $p\,\Big|\binom{p}{h_{j0} h_{j1} \ldots h_{jq-1}}$ unless h_{jk} is p for some k and the rest are zero. Hence,

$$q^{p-1} U_{j,mp} \equiv p U_{0,m}^{p-1} U_{j,m} \pmod{p^{\nu+2}}$$

for $j = 1, 2, \ldots, q-1$ and $p\nu \geqslant \nu+2$; i.e. $p^\nu > 2$. Since $p \nmid U_{0,m}$, we have $p^{\nu+1}\,|\,D_{0,mp}$ and $p^{\nu+2} \nmid D_{0,mp}$. By induction, the highest power of p contained in D_{mp^a} is $p^{a+\nu}$. Also, since $(\mu, p) = 1$, by Corollary 9.1, $p^{a+\nu+1} \nmid D_{m\mu p^a}$. If $p^\nu = 2$, it is clear that $4\,|\,D_{0,2m}$; hence, by the first part of the theorem, $2^{a+1}\,|\,D_{0,m\mu 2^a}$ and $4 \nmid D_{0,\mu m}$ for odd μ.

Suppose $p = q$. If we put $p = q$ in (7.1), we see that if $q^\nu\,|\,D_{0,m}$, we have $q\,\Big|\binom{q}{h_{j0} h_{j1} \ldots h_{jq-1}}$ and $q^{h_{j0}+\nu(q-h_{j0})}$ divides $\prod\limits_{k=0}^{q-1} U_{k,m}^{h_{jk}}$ for $j > 0$. Since $h_{j0} < q$ for $j > 0$,

$$1 + h_{j0} + \nu(q - h_{j0}) > \nu + q - 1;$$

thus, $q^{\nu+1}\,|\,D_{0,qm}$. By induction, $q^{a+\nu}\,|\,D_{0,q^a m}$. If $\nu > 1$ and $q^{\nu+2}\,|\,D_{0,qm}$, we have $q^{q+1+\nu}$ as a divisor of the right hand side of (7.1) whenever $j > 0$. Since

$$h_{j0} + \nu(q - h_{j0}) + 1 \geqslant q + 1 + \nu,$$

when $h_{j0} < q-1$, we obtain

$$U_{0,m}^{q-1} U_{j,m} \equiv 0 \pmod{q^{q+\nu}}$$

for $j = 1, 2, \ldots, q-1$. Now $q^2 \nmid U_{0,m}$; therefore, $q^{\nu+1}\,|\,D_{0,m}$, which is a contradiction. Hence, $q^{\nu+a}$ is the highest power of q dividing $D_{0,q^a m}$ if q^ν $(\nu > 1)$ is the highest power of q dividing $D_{0,m}$.

COROLLARY 12.1. *If* $m, n \in N$, $(D_{0,mn}/D_{0,n}, D_{0,n})\,|\,m$.

THEOREM 13 (THE LAW OF APPARITION). *Let* p *be a prime such that* $p \nmid qQ_q$; *then if* $p \nmid \Delta$,

$$D_{0,p^n-1} \equiv 0 \pmod{p},$$

when $p \not\equiv 1 \pmod{q}$ *and* n *is the index to which* p *belongs* $\pmod{q}$;

$$D_{0,p-1} \equiv 0 \pmod{p},$$

when $p \equiv 1 \pmod{q}$ *and* $\Delta^{(p-1)/q} \equiv 1 \pmod{p}$;

$$D_{0,a} \equiv 0 \pmod{p},$$

when $p \equiv 1 \pmod{q}$, $\Delta^{(p-1)/q} \not\equiv 1 \pmod{p}$, *and* $a = (p^q-1)/(p-1)$.

If $p \mid \Delta$, $D_{0,p^m} \equiv 0 \pmod p$, where m is the least positive integer such that $p^m > q$.

Proof. From (3.4) and the fact that $p \mid \binom{p^k}{i_0 i_1 \ldots i_{q-1}}$, when no $i_j = p^k$, we have

$$q^{p^{k}-1} U_{j,p^k} \equiv \Delta^{g_j} U_{i,1}^{p^k} \pmod p, \tag{7.2}$$

where $ip^k \equiv j \pmod q$, $0 \leqslant i \leqslant q-1$, and $g_j = (ip^k - j)/q$.

Case 1: $p \nmid \Delta$, $p \not\equiv 1 \pmod q$. Let n be the index to which p belongs $(\bmod q)$; then, by (7.2)

$$U_{j,p^n} \equiv U_{j,1} \pmod p,$$

for $j = 0, 1, 2, \ldots, q-1$. From (3.1) and (3.2), we have $U_{0,p^n-1} \equiv q \pmod p$ and $p \mid D_{0,p^n-1}$.

Case 2: $p \nmid \Delta$, $p \equiv 1 \pmod q$, $\Delta^{(p-1)/q} \equiv 1 \pmod p$. By (7.2)

$$U_{j,p} \equiv U_{j,1} \pmod p;$$

thus $U_{0,p-1} \equiv q \pmod p$ and $p \mid D_{0,p-1}$.

Case 3: $p \nmid \Delta$, $p \equiv 1 \pmod q$, $\Delta^{(p-1)/q} \not\equiv 1 \pmod p$. Let $\Delta^{(p-1)/q} \equiv f \pmod p$; then $\sum_{k=0}^{q-1} f^k \equiv 0 \pmod p$. By (3.5)

$$q^{q-1} \sum_{j=0}^{q-1} U_{j,a} \delta^j = \prod_{k=0}^{q-1} \sum_{j=0}^{q-1} U_{j,p^k} \delta^j$$

and by (7.2)

$$U_{j,p^k} \equiv f^{kj} U_{j,1} \pmod p.$$

Let P be the ideal generated by p in $K[\gamma_1]$. Thus, in $K[\gamma_1]$,

$$q^{q-1} \sum_{j=0}^{q-1} U_{j,a} \delta^j \equiv \prod_{k=0}^{q-1} \sum_{j=0}^{q-1} f^{kj} U_{j,1} \delta^j \pmod P$$

$$\equiv \begin{vmatrix} U_{0,1} & \delta^{q-1} U_{q-1,1} & \delta^{q-2} U_{q-2,1} & \ldots & \delta U_{1,1} \\ \delta U_{1,1} & U_{0,1} & \delta^{q-1} U_{q-1,1} & \ldots & \delta^2 U_{2,1} \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ \delta^{q-1} U_{q-1,1} & \delta^{q-2} U_{q-2,1} & \delta^{q-3} U_{q-3,1} & \ldots & U_{0,1} \end{vmatrix} \pmod P.$$

By (3.2),

$$q^{q-1}(U_{0,a} - qQ_q) + q^{q-1} \sum_{j=1}^{q-1} U_{j,a} \delta^j \equiv 0 \pmod P.$$

This implies that

$$U_{0,a} \equiv qQ_q \pmod p \quad \text{and} \quad p \mid D_{0,a}.$$

Case 4: $p \mid \Delta$. Let m be the least element of N such that $p^m > q$. By (7.2), $U_{0,p^n} \equiv U_{0,1} \pmod p$ and $p \mid D_{0,p^m}$.

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 Δ, we define the function $\Phi: N \to N + \{0\}$ in the following fashion. If p is a prime,

$\Phi(p) = 0$ when $p \mid Q_q$,

$\Phi(p) = p^k$ when $p \nmid Q_p$, $p \mid \Delta$ and k is the least integer such that $p^k > q$,

$\Phi(q) = q-1$ when $q \nmid Q_q$ and $q \nmid \Delta$,

$\Phi(p) = p^k - 1$ when $p \nmid qQ_q\Delta$, $p \not\equiv 1 \pmod q$, and k is the index to which p belongs $(\bmod q)$,

$\Phi(p) = p-1$, when $p \nmid qQ_q$, $p \equiv 1 \pmod q$ and $\Delta^{(p-1)/q} \equiv 1 \pmod p$,

$\Phi(p) = (p^q - 1)/(p-1)$, when $p \nmid qQ_q\Delta$, $p \equiv 1 \pmod q$ and $\Delta^{(p-1)/q} \not\equiv 1 \pmod p$.

$\Phi(p^n) = p^{n-1}\Phi(p)$ for any prime p.

If m is composite, $m = \prod_{i=0}^{\nu} p_i^{a_i}$, where the p_i are distinct primes. We define $\Phi(m)$ to be the least common multiple of $\Phi(p_1^{a_1}), \Phi(p_2^{a_2}), \ldots, \Phi(p_\nu^{a_\nu})$.

Theorem 14. *Let $m \in N$. If we denote $\Phi(m)$ by Φ, we have $D_{0,\Phi} \equiv 0 \pmod m$.*

Corollary 14.1. *If $(m, Q_q) = 1$, the rank of apparition ϱ of m exists and $\varrho \mid \Phi$.*

It is interesting to note that the $D_{0,n}$ functions do not seem to increase as quickly as the Lucas functions. This means that they are more easily factored. For example, if $q = 3$, $\Delta = 9$, $U_{0,1} = 3$, $U_{1,1} = 3$, $U_{2,1} = 9$, we evaluate $D_{0,306} = 174453057$. Now $D_{0,102} = 309$, $D_{0,153} = 9$ and $D_{0,18} = 9$; hence, $9 \cdot 103 \mid D_{0,306}$. To factor $D_{0,306}/(9 \cdot 103) = 188191$, we notice that if p is a prime divisor of 188191, $p = 1 + 306k$, or $p^2 = 1 + 306k$. This implies that $p \equiv \pm 1$, $\pm 35 \pmod{306}$. 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 $D_{0,306} = 9 \cdot 103 \cdot 307 \cdot 613$.

We close with a theorem similar to a fundamental theorem of Lucas ([7], 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 of M is either $M^{q-1} - 1$ or $(M^q - 1)/(M-1)$ or $(M^q - 1)/[q(M-1)]$, then M is a prime.*

Proof. Suppose M is composite and that $M = \prod_{i=1}^{\nu} p_i^{a_i}$, where the p_i are distinct primes. Clearly $p_i \nmid q\Delta Q_q$; therefore $q \mid \Phi(p_i)$ and $\Phi(M) \mid J$, where

$$J = q\prod_{i=1}^{\nu} p_i^{a_i-1}\left(\Phi(p_i)/q\right).$$

Now

$$J/M^{q-1} = q\prod_{i=1}^{\nu} \frac{p_i^{a_i-1}}{p_i^{(q-1)(a_i-1)}}\,\frac{\Phi(p_i)}{qp_i^{q-1}}$$

$$\leqslant q\prod_{i=1}^{\nu} p_i^{(2-q)(a_i-1)}\frac{1}{q}\left(1+\frac{1}{p_i}+\frac{1}{p_i^2}+\ldots+\frac{1}{p_i^{q-1}}\right)$$

$$< q\prod_{i=1}^{\nu} p_i^{(2-q)(a_i-1)}\frac{p_i}{q(p_i-1)}.$$

If $\nu = 1$, we have $a_i \geqslant 2$ and therefore

$$\frac{J}{M^{q-1}} < \frac{1}{p_1-1} \leqslant \frac{1}{2}.$$

If $\nu \geqslant 2$,

$$\frac{J}{M^{q-1}} < \frac{1}{q}\left(\frac{p_1}{p_1-1}\right)\left(\frac{p_2}{p_2-1}\right) \leqslant \frac{1}{3}\cdot\frac{3}{2}\cdot\frac{5}{4} = \frac{5}{8}.$$

Since $M > 2$,

$$J < M^{q-1}-1 < (M^q-1)/(M-1).$$

But $M \mid D_{0,J}$; hence, M is prime if the rank of apparition of M is $M^{q-1}-1$ or $(M^q-1)/(M-1)$.

If the rank of apparition of M is $(M^q-1)/[(M-1)q]$, then

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

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

References

[1] M. Appell, *Sur certaines functions analogues aux functions circulaires*, C. R. Acad. Sci. (Paris), 84 (1877), pp. 1378–1380.

[2] R. D. Carmichael, *On the numerical factors of the arithmetic forms* $a^n \pm \beta^n$, Ann. of Math. 15 (1913–1914), pp. 30–70.

[3] J. W. L. Glaisher, *On a special form of determinant and on certain functions of n variables analogous to the sine and cosine*, Quart. Journ. Pure Appl. Math. 16 (1879), pp. 15–33.

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

[5] — *Factorization of certain cyclotomic functions*, ibid, 34 (1933), pp. 461–479.

[6] W. J. Leveque, *Topics in Number Theory*, Reading, Mass., 1958, Vol. II, pp. 87.

[7] Edouard Lucas, *Théorie des fonctions numériques simplement périodiques*, Amer. Journ. Math. 1 (1878), pp. 184–240, 289–321.

[8] G. B. Matthews, *On the arithmetic theory of the form* $x^3+ny^3+n^2z^3-3nxyz$, Proc. London Math. Soc. 21 (1891), pp. 280–287.

[9] T. A. Pierce, *The numerical factors of the arithmetic forms* $\prod^{n}(1\pm a_i^m)$, Ann. of Math. 18 (1916), pp. 53–64.

[10] H. C. Pocklington, *The direct solution of the quadratic and cubic binomial congruences with prime moduli*, Proc. Cambridge Phil. Soc. 42 (1917), pp. 57–59.

[11] Morgan Ward, *A note on divisibility sequences*, Bull. Amer. Math. Soc. 42 (1936), pp. 843–845.

[12] — *Memoir on elliptic divisibility sequences*, Amer. Journ. Math. 70 (1948), pp. 31–74.

[13] Jacob Westlund, *On the fundamental number of the algebraic number field* $k(\sqrt[p]{m})$, Trans. Amer. Math. Soc. 11 (1910), pp. 388–392.

[14] H. C. Williams, *A Generalization of the Lucas Functions*, unpublished Ph. D. thesis, University of Waterloo, Waterloo, Ontario, 1969.

Received on 8. 6. 1970 (93)