Conspectus materiae tomi XXIX, fasciculi 4

La revue est consacrée à la Théorie des Nombres
The journal publishes papers on the Theory of Numbers
Die Zeitschrift veröffentlicht Arbeiten aus der Zahlentheorie
Журнал посвящен теории чисел

L'adresse de la Rédaction et de l'échange — Address of the Editorial Board and of the exchange — Die Adresse der Schriftleitung und des Austausches — Адрес редакции и книгообмена

ACTA ARITHMETICA

ul. Śniadeckich 8, 00-950 Warszawa

Les auteurs sont priés d'envoyer leurs manuscrits en deux exemplaires
The authors are requested to submit papers in two copies
Die Autoren sind gebeten um Zusendung von 2 Exemplaren jeder Arbeit
Рукописи статей редакция просит предлагать в двух экземплярах

PRINTED IN POLAND

WROCLAWSKA DRUKARNIA NAUKOWA

ACTA ARITHMETICA
XXIX (1976)

A generalization of Lehmer's functions

by

H. C. Williams (Winnipeg, Canada)

1. Introduction. The Lucas functions v_n and u_n are defined by the formulas

$$v_n = a^n + b^n, \quad u_n = (a^n - b^n)/(a-b),$$

where a, b are the zeros of the polynomial $x^2 - Px + Q$ and P, Q are given coprime integers. These functions and their many remarkable properties have been discussed in detail by Lucas [11] and Carmichael [2].

Lehmer [7] extended Lucas' functions by defining the functions

$$V_n = \alpha^n + \beta^n, \quad U_n = (\alpha^n - \beta^n)/(\alpha - \beta),$$

where α, β are the zeros of the polynomial $x^2 - \sqrt{R}x + Q$ and R, Q are given coprime integers. He then put

$$\overline{V}_n = V_n/(\sqrt{R})^i, \quad \overline{U}_n = U_n/(\sqrt{R})^{1-i},$$

where $i \equiv n \pmod 2$ and $0 \leqslant i \leqslant 1$. The functions $\overline{V}_n$ and $\overline{U}_n$ are always integers for any non-negative integer n and they have properties similar to the properties possessed by v_n and u_n.

Generalizations of the Lucas functions have been described by Lucas [11], Poulet (see Lehmer [8]), Pierce [12], Bell [1], Carmichael [3], and more recently by Williams [13]; however, none of these generalizations includes Lehmer's modification of these functions. In this paper we will generalize Lehmer's functions by extending the means by which Lehmer modified the Lucas functions in order to obtain $\overline{V}_n$ and $\overline{U}_n$. We will then show that many of the properties of $\overline{V}_n$ and $\overline{U}_n$ can be deduced as special cases of more general results. By using a special case of these generalized functions, we will show how to extend a result of Williams [14] in order to obtain necessary and sufficient conditions for integers of the forms $2A5^n - 1$ ($A < 5^{n/2}$) and $2A7^n - 1$ ($2A < 7^{n/2}$) to be prime.

2. Definitions. For the purpose of generalizing Lehmer's functions, it is more convenient to consider the four functions $V_{0,n}$, $V_{1,n}$, $U_{0,n}$, $U_{1,n}$. We define these functions by putting

$$V_{0,n} = \overline{V}_n, \quad U_{1,n} = \overline{U}_n, \quad V_{1,n} = 0, \quad U_{0,n} = 0$$

when n is even, and

$$V_{1,n} = \overline{V}_n, \quad U_{0,n} = \overline{U}_n, \quad V_{0,n} = 0, \quad U_{1,n} = 0$$

when n is odd.

It is not difficult to see that if $\delta = \varrho_2 - \varrho_1$, where ϱ_1, ϱ_2 are the zeros of $x^2 - R$, then

$$\delta V_{0,n} = \begin{vmatrix} \alpha_1^n+\beta_1^n & \varrho_1 \\ \alpha_2^n+\beta_2^n & \varrho_2 \end{vmatrix}, \qquad \delta V_{1,n} = \begin{vmatrix} 1 & \alpha_1^n+\beta_1^n \\ 1 & \alpha_2^n+\beta_2^n \end{vmatrix},$$

$$\delta U_{0,n} = \begin{vmatrix} (\alpha_1^n-\beta_1^n)/(\alpha_1-\beta_1) & \varrho_1 \\ (\alpha_2^n-\beta_2^n)/(\alpha_2-\beta_2) & \varrho_2 \end{vmatrix}, \qquad \delta U_{1,n} = \begin{vmatrix} 1 & (\alpha_1^n-\beta_1^n)/(\alpha_1-\beta_1) \\ 1 & (\alpha_2^n-\beta_2^n)/(\alpha_2-\beta_2) \end{vmatrix}.$$

Here α_i, β_i are the zeros of $x^2 - \varrho_i x + Q$ $(i = 1, 2)$. We will now consider a generalization of these $V_{i,n}$, $U_{i,n}$ $(i = 0, 1)$ functions.

Let Q be a given non-zero integer and define the polynomials $v_n(x)$, $u_n(x)$ by the recursive formulas

$$v_{n+1}(x) = x v_n(x) - Q v_{n-1}(x),$$

$$u_{n+1}(x) = x u_n(x) - Q u_{n-1}(x),$$

together with the initial values $v_0(x) = 2$, $v_1(x) = x$, $u_0(x) = 0$, $u_1(x) = 1$. We have $v_n(P) = v_n$ and $u_n(P) = u_n$. We use these polynomials in one variable to define some functions in k variables $x_1, x_2, \ldots, x_k$.

Let

$$\delta(x_1, x_2, \ldots, x_k) = \begin{vmatrix} 1 & x_1 & x_1^2 & \ldots & x_1^{k-1} \\ 1 & x_2 & x_2^2 & \ldots & x_2^{k-1} \\ 1 & x_3 & x_3^2 & \ldots & x_3^{k-1} \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ 1 & x_k & x_k^2 & \ldots & x_k^{k-1} \end{vmatrix}$$

and define for $j = 0, 1, \ldots, k-1$,

$$G_{j,n}(x_1, x_2, \ldots, x_k) = \overline{G}_{j,n}(x_1, x_2, \ldots, x_k)/\delta(x_1, x_2, \ldots, x_k),$$

$$H_{j,n}(x_1, x_2, \ldots, x_k) = \overline{H}_{j,n}(x_1, x_2, \ldots, x_k)/\delta(x_1, x_2, \ldots, x_k),$$

where $\overline{G}_{j,n}(x_1, x_2, \ldots, x_k)$, $\overline{H}_{j,n}(x_1, x_2, \ldots, x_k)$ are the determinants obtained by replacing the $(j+1)$th column of $\delta(x_1, x_2, \ldots, x_k)$ by the columns

$$\begin{pmatrix} u_n(x_1) \\ u_n(x_2) \\ \vdots \\ u_n(x_k) \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} v_n(x_1) \\ v_n(x_2) \\ \vdots \\ v_n(x_k) \end{pmatrix}$$

respectively.

If

$$f(x) = \sum_{i=0}^{k} P_{k-i} x^i (-1)^{k-i}$$

in a monic polynomial with distinct zeros

$$\varrho_1, \varrho_2, \ldots, \varrho_k$$

and integer coefficients P_i $(i = 1, 2, \ldots, k)$ such that

$$(P_1, P_2, \ldots, P_k, Q) = 1,$$

we define the $2k$ functions $V_{j,n}$, $U_{j,n}$ $(j = 0, 1, \ldots, k-1)$ as

$$V_{j,n} = H_{j,n}(\varrho_1, \varrho_2, \ldots, \varrho_k),$$
$$U_{j,n} = G_{j,n}(\varrho_1, \varrho_2, \ldots, \varrho_k) \qquad (j = 0, 1, \ldots, k-1).$$

Also, we put

$$\delta = \delta(\varrho_1, \varrho_2, \ldots, \varrho_k), \qquad \Delta = \delta^2.$$

Since, for any integer $n > 0$, $v_n(x)$, $u_n(x)$ are polynomials with integer coefficients, it is clear that $V_{j,n}$, $U_{j,n}$ $(j = 0, 1, \ldots, k-1)$ are integers.

If δ_{ij} is the Kronecker delta, we have

$$V_{i,0} = 2\delta_{i,0}, \quad U_{i,0} = 0 \quad (i = 0, 1, \ldots, k-1)$$

and

$$V_{i,1} = \delta_{i,1}, \quad U_{i,1} = \delta_{i+1,1} \quad (i = 0, 1, \ldots, k-1).$$

We will be mainly interested in determining the divisibility properties of the three functions

$$A_n = (U_{0,n}, U_{1,n}, U_{2,n}, \ldots, U_{k-1,n})\,(^1),$$
$$B_n = (V_{0,n}, V_{1,n}, V_{2,n}, \ldots, V_{k-1,n}),$$
$$C_n = (V_{1,n}, V_{2,n}, V_{3,n}, \ldots, V_{k-1,n}).$$

[1] We use the notation $(a, b, c, \ldots, n)$ to denote the greatest common divisor of $a, b, c, \ldots, n$ and $[a, b, c, \ldots, n]$ to denote the least common multiple of $a, b, c, \ldots, n$.

It is not difficult to see that when $f(x) = x^2 - R$, the $V_{0,n}$, $V_{1,n}$, $U_{0,n}$, $U_{1,n}$ functions, are those given at the beginning of this section; thus, in this case, we have

$$A_n = \overline{U}_n \quad \text{and} \quad B_n = \overline{V}_n.$$

In order to investigate the functions $V_{i,n}$, $U_{i,n}$ $(i = 0, 1, \ldots, k-1)$, it will be necessary to use many of the well known properties of the polynomials $v_n(x)$ and $u_n(x)$. We list the results which we will require in Section 3.

3. Some properties of $v_n(x)$ and $u_n(x)$. All the identities satisfied by the functions $v_n(x)$ and $u_n(x)$ which are given in this section can be found in Lucas [11].

$$\begin{aligned} v_{n+m}(x) &= v_m(x)v_n(x) - Q^m v_{n-m}(x), \\ u_{n+m}(x) &= v_m(x)u_n(x) - Q^m u_{n-m}(x); \end{aligned} \tag{3.1}$$

$$\begin{aligned} 2v_{n+m}(x) &= v_n(x)v_m(x) + (x^2-4Q)u_n(x)u_m(x), \\ 2u_{n+m}(x) &= u_n(x)v_m(x) + v_n(x)u_m(x); \end{aligned} \tag{3.2}$$

$$v_n(x) = Q^n v_{-n}(x), \qquad u_n(x) = -Q^n u_{-n}(x); \tag{3.3}$$

$$v_n(x)^2 - (x^2-4Q)u_n(x)^2 = 4Q^n; \tag{3.4}$$

$$\begin{aligned} v_{2n}(x) &= (x^2-4Q)u_n(x)^2 + 2Q^n = v_n(x)^2 - 2Q^n, \\ u_{2n}(x) &= u_n(x)v_n(x); \end{aligned} \tag{3.5}$$

$$u_n^2(x) - u_{n-1}(x)u_{n+1}(x) = Q^{n-1}; \tag{3.6}$$

$$\begin{aligned} v_{nm}(x) &= \sum_{r=0}^{[n/2]} (-1)^r \frac{n}{r}\binom{n-r-1}{r-1} Q^{mr} v_m(x)^{n-2r}, \\ u_{nm}(x) &= \sum_{r=0}^{(n-1)/2} \frac{n}{r}\binom{n-r-1}{r-1} Q^{mr}(x^2-4Q)^{(n-2r-1)/2} u_m(x)^{n-2r} \qquad (n \text{ odd}). \end{aligned} \tag{3.7}$$

Let $y_n(x)$ be the polynomial whose zeros are $2\cos(2j\pi/2n+1)$ $(j = 1, 2, \ldots, n)$; we have

$$y_{n+1}(x) = xy_n(x) - y_{n-1}(x),$$

where

$$y_0(x) = 1, \qquad y_1(x) = x+1$$

and we also have

$$\begin{aligned} v_{m(2n+1)}(x) &= (-1)^n Q^{nm} y_n\big(-v_{2m}(x)/Q^m\big) v_m(x), \\ u_{m(2n+1)}(x) &= Q^{nm} y_n(v_{2m}/Q^m) u_m(x). \end{aligned} \tag{3.8}$$

We also need some results on $v_n(x)$ and $u_n(x)$ modulo a prime p. Using (3.7), it is not difficult to show for an odd prime p that

$$v_{p^n}(x) \equiv x^{p^n}, \qquad u_{p^n}(x) \equiv (x^2-4Q)^{(p^n-1)/2} \pmod p. \tag{3.9}$$

Since

$$v_{2^n}(x) \equiv x^{2^n} \pmod 2,$$

we see that

$$u_{2^n}(x) = \prod_{i=0}^{n-1} v_{2^i}(x) \equiv x^s \pmod 2, \tag{3.10}$$

where

$$s = \sum_{i=1}^{n-1} 2^i.$$

If $2 \nmid Q$ and $s_n(x) = u_{2^n+1}(x)$ then

$$s_{n+1}(x) \equiv x^{2^n} s_n(x) + 1 \pmod 2$$

and

$$u_{2^n+1}(x) \equiv x^{2^n} + \sum_{i=1}^{n} x^{2^n - 2^i} \pmod 2. \tag{3.11}$$

4. Identities satisfied by the $V_{j,n}$ and $U_{j,n}$ functions. Let

$$h_j(x) = x^2 - \varrho_j x + Q$$

and put

$$F(x) = \prod_{j=1}^{k} h_j(x) = \sum_{i=0}^{2k} R_i(-1)^i x^{2k-i}.$$

The R_i $(i = 0, 1, \ldots, 2k)$ are all integers, $R_0 = 1$, $R_{2k} = Q^k$, $R_i \equiv P_i \pmod Q$ $(i = 1, 2, \ldots, k)$, and $R_i \equiv 0 \pmod Q$ $(i = k+1, k+2, \ldots, 2k)$. Since, the $V_{j,n}$ and $U_{j,n}$ functions can be expressed as linear combinations of the zeros of $F(x)$, we see that

$$\begin{aligned} V_{j,n+2k} &= \sum_{i=1}^{2k} (-1)^{i+1} R_i V_{j,n+2k-i}, \\ U_{j,n+2k} &= \sum_{i=1}^{2k} (-1)^{i+1} R_i U_{j,n+2k-i}. \end{aligned} \tag{4.1}$$

If D is the discriminant of $F(x)$, then

$$D = \prod_{i=1}^{k} F'(\alpha_i) \prod_{i=1}^{k} F'(\beta_i)$$

and

$$F'(\alpha_i) = h_i'(\alpha_i) \prod_{j \neq i}^{k} h_j(\alpha_i),$$

where a_i, β_i are the zeros of $h_i(x)$. Hence,

$$D = (-1)^k E\Delta^2 Q^{k(k-1)},$$

where

$$E = f(2\sqrt{Q})f(-2\sqrt{Q}) = \Big(\sum_{j=0}^{[k/2]} 2^{2j}Q^jP_{k-2j}\Big)^2 - Q\Big(\sum_{j=0}^{[k-1/2]} 2^{2j+1}Q^jP_{k-2j-1}\Big)^2.$$

From the definition of the functions $V_{j,n}$ and $U_{j,n}$ it is evident that

$$\text{(4.2)}\qquad \begin{aligned} \sum_{j=0}^{k-1} V_{j,n}\varrho_i^j &= v_n(\varrho_i) \quad (i = 1, 2, \ldots, k), \\ \sum_{j=0}^{k-1} U_{j,n}\varrho_i^j &= u_n(\varrho_i) \quad (i = 1, 2, \ldots, k). \end{aligned}$$

Thus, any identity involving $v_n(x)$ or $u_n(x)$ can be converted into an identity involving the $V_{j,n}$ or $U_{j,n}$ functions by substituting the above expressions and eliminating the ϱ_i's. Since $\Delta \neq 0$, we can always eliminate these ϱ_i's. We give below several identities which will be useful in obtaining the properties of A_n, B_n and C_n, which are given in subsequent sections. In order to derive these identities we make use of the k auxiliary functions $Z_{j,n}$ $(j = 0, 1, \ldots, k-1)$, which are defined by the equations

$$\varrho_i^n = \sum_{j=0}^{k-1} Z_{j,n}\varrho_i^j \quad (i = 1, 2, \ldots, k).$$

It should be noted here that

$$Z_{i,j} = \delta_{ij} \quad (0 \leqslant j < k),$$
$$Z_{i,k} = (-1)^{k-i+1}P_{k-i},$$

and

$$\text{(4.3)}\qquad Z_{j,n+k} = \sum_{i=1}^{k} P_i(-1)^{i+1}Z_{j,n+k-i}.$$

From (3.2), we deduce the identities

$$\text{(4.4)}\qquad \begin{aligned} 2V_{h,n+m} &= \sum_{i=0}^{k-1}\sum_{j=0}^{k-1}(V_{i,n}V_{j,m}Z_{h,i+j} - 4Q\,U_{i,n}U_{j,m}Z_{h,i+j} + \\ &\qquad + U_{i,n}U_{j,m}Z_{h,i+j+2}), \\ 2U_{h,n+m} &= \sum_{i=0}^{k-1}\sum_{j=0}^{k-1}(V_{i,n}U_{j,m} + V_{j,m}U_{i,n})Z_{h,i+j} \quad (h = 0, 1, \ldots, k-1), \end{aligned}$$

and from (3.3) we easily see that

$$\text{(4.5)}\qquad Q^nV_{j,-n} = V_{j,n}, \qquad -Q^nU_{j,-n} = U_{j,n}.$$

Putting $m = -m$ in (4.4) and using (4.5), we can produce formulas for $V_{h,n-m}$ and $U_{h,n-m}$.

By (3.1) we have

$$\text{(4.6)}\qquad \begin{aligned} V_{h,n+m} &= \sum_{i=0}^{k-1}\sum_{j=0}^{k-1} V_{j,m}V_{i,n}Z_{h,i+j} - Q^mV_{h,n-m}, \\ U_{h,n+m} &= \sum_{i=0}^{k-1}\sum_{j=0}^{k-1} V_{j,m}U_{i,n}Z_{h,i+j} - Q^mU_{h,n-m}. \end{aligned}$$

Putting $m = 1$ and using the values of $U_{j,1}$, $V_{j,1}$ and $Z_{j,k}$, we have

$$\text{(4.7)}\qquad \begin{aligned} V_{0,n+1} &= (-1)^{k+1}P_kV_{k-1,n} - Q\,V_{0,n-1}, \\ V_{h,n+1} &= V_{h-1,n} + (-1)^{k-h+1}P_{k-h}V_{k-1,n} - Q\,V_{h,n-1} \quad (h > 0). \end{aligned}$$

Putting $n = m$ in (4.6) we get

$$\text{(4.8)}\qquad \begin{aligned} V_{h,2n} &= \sum_{i=0}^{k-1}\sum_{j=0}^{k-1} V_{i,n}V_{j,n}Z_{h,i+j} - 2\delta_{h,0}Q^n, \\ U_{h,2n} &= \sum_{i=0}^{k-1}\sum_{j=0}^{k-1} V_{j,n}U_{i,n}Z_{h,i+j} \quad (h = 0, 1, \ldots, k-1). \end{aligned}$$

We can obtain another formula for $V_{h,2n}$ by using (3.5)

$$\text{(4.9)}\qquad V_{h,2n} = \sum_{i=0}^{k-1}\sum_{j=0}^{k-1} U_{i,n}U_{j,n}(Z_{h,i+j+2} - 4QZ_{h,i+j}) + 2\delta_{h,0}Q^n.$$

From the relation (3.6) we obtain the rather simple result

$$\text{(4.10)}\qquad V_{h,n} = U_{h,n+1} - QU_{h,n-1}.$$

We deduce the identity

$$\text{(4.11)}\qquad \sum_{i=0}^{k-1}\sum_{j=0}^{k-1}(V_{j,n}V_{i,n}Z_{h,i+j} + 4Q\,U_{j,n}U_{i,n}Z_{h,i+j} - U_{j,n}U_{i,n}Z_{h,i+j+2}) = 4\delta_{h,0}Q^n$$

from the formula (3.4).

For a given $f(x)$ define the polynomial functions in k variables $Y_{i,n}(x_0, x_1, \ldots, x_{k-1})$ $(i = 0, 1, \ldots, k-1)$ by the equations

$$y_n\Big(\sum_{i=0}^{k-1} x_i\varrho_j^i\Big) = \sum_{i=0}^{k-1} Y_{i,n}(x_0, x_1, \ldots, x_{k-1})\varrho_j^i \quad (j = 1, 2, \ldots, k).$$

We have

$$Y_{i,0}(x_0, x_1, \ldots, x_{k-1}) = \delta_{i,0}, \qquad Y_{i,1}(x_0, x_1, \ldots, x_{k-1}) = x_i + \delta_{i,0}$$

and

$$Y_{h,n+1}(x_0, x_1, \ldots, x_{k-1})$$
$$= \sum_{i=0}^{k-1} \sum_{j=0}^{k-1} x_j Y_{i,n}(x_0, x_2, \ldots, x_{k-1}) Z_{h,i+j} - Y_{h,n-1}(x_1, x_2, \ldots, x_{k-1}).$$

Also

$$Y_{0,n}(2, 0, 0, \ldots, 0) = y_n(2) = 2n+1.$$

Referring to (3.8), we derive the identities

$$V_{h,(2n+1)m} = (-1)^n Q^{nm} \sum_{i=0}^{k-1} \sum_{j=0}^{k-1} Y_{i,n}(-V_{0,2m}/Q^m, -V_{1,2m}/Q^m, \ldots,$$
$$-V_{k-1,2m}/Q^m) V_{j,m} Z_{h,i+j}, \tag{4.12}$$
$$U_{h,(2n+1)m} = Q^{nm} \sum_{i=0}^{k-1} \sum_{j=0}^{k-1} Y_{i,n}(V_{0,2m}/Q^m, V_{1,2m}/Q^m, \ldots, V_{k-1,2m}/Q^m) U_{j,m} Z_{h,i+j}.$$

By using (3.7), we are also able to deduce the identities

$$V_{h,nm} = \sum_{r=0}^{[n/2]} (-1)^r \frac{n}{r} \binom{n-r-1}{r-1} Q^{mr} \sum \frac{(n-2r)!}{i_0!\, i_1! \ldots i_{k-1}!} Z_{h,\sigma} \prod_{j=0}^{k-1} V_{j,m}^{i_j},$$
$$U_{h,nm} = \sum_{r=0}^{(n-1)/2} \frac{n}{r} \binom{n-r-1}{r-1} Q^{mr} \sum_{s=0}^{(n-2r-1)/2} \binom{(n-2r-1)/2}{s} (-4Q)^{(n-2r-2s-1)/2} \times \tag{4.13}$$
$$\times \sum \frac{(n-2r)!}{i_0!\, i_1! \ldots i_{k-1}!} Z_{h,\sigma+2s} \prod_{j=0}^{k-1} U_{j,m}^{i_j} \quad (n \text{ odd}),$$

where the last sum in each formula is taken over all sets of non-negative integers $\{i_0, i_1, \ldots, i_{k-1}\}$ such that

$$\sum_{j=0}^{k-1} i_j = n-2r \quad \text{and} \quad \sigma = \sum_{j=0}^{k-1} j i_j.$$

5. Preliminary results on A_n, B_n, and C_n. The functions $\overline{U}_n$ and $\overline{V}_n$ have some remarkable divisibility properties. We will show in the following sections that these properties are also possessed by the more general functions A_n and B_n. We will also show that C_n has some interesting divisibility properties.

Throughout the following sections we will use the symbol n to denote a positive integer. We define

$$D_n = (Z_{k-1,n}, Z_{k-1,n+1}, Z_{k-1,n+2}, \ldots, Z_{k-1,n+k-1}),$$

where $Z_{k-1,m}$ is defined in Section 4.

Lemma 5.1. *If p is a prime and $p \mid D_n$, then $p \mid (P_1, P_2, \ldots, P_k)$.*

Proof. Let $p \mid D_n$. Since $Z_{i,n} = \delta_{i,j}$ for $n < k$, it follows that $n \geqslant k$. From (4.3) we have

$$Z_{k-1,n+k-j} = \sum_{i=1}^{k} P_i (-1)^{i+1} Z_{k-1,n+k-i-j}.$$

Putting $j = 1$, we see that $p \mid P_k Z_{k-1,n-1}$. If $p \nmid Z_{k-1,n-1}$, then $p \mid P_k$ and if $j = 2$,

$$0 \equiv Z_{k-1,n+k-2} \equiv (-1)^k P_{k-1} Z_{k-1,n-1} \pmod{p};$$

thus, $p \mid P_{k-1}$. Putting $j = 3, 4, \ldots, k$ and repeating this argument, we deduce that $p \mid P_{k-2}$, $p \mid P_{k-3}, \ldots, p \mid P_1$; that is, $p \mid (P_1, P_2, \ldots, P_k)$.

If $p \mid Z_{k-1,n-1}$, then $p \mid D_{n-1}$ and we can apply the above argument again. We must finally conclude that $p \mid (P_1, P_2, \ldots, P_k)$ or $p \mid Z_{k-1,k-1}$. Since $Z_{k-1,k-1} = 1$, the lemma is proved.

Theorem 5.1. $(A_n, B_n) = 1, 2$.

Proof. From (4.11) it is clear that if $p^2 \mid (A_n, B_n)$ when $p = 2$ or if $p \mid (A_n, B_n)$ when p is an odd prime, then $p \mid Q$. From (4.4), we also see that $p \mid U_{k-1,n+m}$ for $m = 0, 1, \ldots$ By definition of $U_{k-1,n}$, we have

$$U_{k-1,j} = \delta_{k-1,j-1} \quad (-k < j \leqslant k);$$

thus, if $p \mid Q$, it follows from (4.1) and (4.3) that

$$U_{k-1,n+m} \equiv Z_{k-1,n+m-1} \pmod{p}.$$

Hence, if $(A_n, B_n) \neq 1, 2$, there exists a prime p such that $p \mid D_{n-1}$ and $p \mid Q$; but, by Lemma 5.1, this means that $p \mid (P_1, P_2, \ldots, P_k, Q)$, which is impossible.

Corollary 5.1.1. *If $2 \mid Q$, then $2 \nmid (A_n, B_n)$.*

Proof. If $2 \mid Q$ and $2 \mid (A_n, B_n)$, then $2 \mid D_{n-1}$ and $2 \mid (P_1, P_2, \ldots, P_k, Q)$.

Corollary 5.1.2. $(A_n, B_n, Q) = 1$.

We are now able to present several simple properties of A_n, B_n and C_n. We do this by giving the following sequence of lemmas.

Lemma 5.2. $(A_n, C_n, Q) = 1$.

Proof. If p is a prime and $p \mid (A_n, C_n, Q)$, then it follows from (4.11) that $p \mid V_{0,n}$ and consequently that $p \mid (A_n, B_n, Q)$.

LEMMA 5.3. $B_n | A_{2n}$, $A_n | C_{2n}$.

Proof. The first result follows from (4.8) and the second from (4.9).

LEMMA 5.4. *$A_n | A_{mn}$, $C_n | C_{mn}$, $B_n | B_{(2m+1)n}$, where m is any positive integer.*

Proof. The results follow by using formulas (4.6) and mathematical induction.

LEMMA 5.5. $(B_n, Q) = (A_n, Q) = 1$.

Proof. If $m | B_n$, then $m | A_{2n}$ and $m | (C_{4m}, A_{4m})$; thus, $m \nmid Q$. The proof that $(A_n, Q) = 1$ is similar.

LEMMA 5.6. *If $2 | A_n$, then $2 | B_n$.*

Proof. From (4.6), we see that if $2 | A_n$,

$$U_{h,n+1} \equiv Q\, U_{h,n-1} (\operatorname{mod} 2) \qquad (h = 0, 1, \ldots, k-1).$$

Putting this result together with (4.10), it is clear that

$$V_{h,n} \equiv 0 (\operatorname{mod} 2) \qquad (h = 0, 1, \ldots, k-1).$$

We give below three lemmas which describe the divisibility of A_n, B_n, and C_n by powers of 2.

LEMMA 5.7. *If $2^\lambda \| B_n$ $(\lambda \geqslant 1)$, then $2^\lambda \| B_{(2m+1)n}$ and $2 \| B_{2n}$.*

Proof. Using (4.8), we have

$$V_{0,2n} \equiv -2Q^n (\operatorname{mod} 2^{2\lambda}).$$

Since $2 \nmid Q$, $2 \| B_{2n}$. Using (4.13), we see that

$$V_{h,(2m+1)n} \equiv (-1)^m (2m+1) Q^{mn} V_{h,n} (\operatorname{mod} 2^{\lambda+2});$$

hence, $2^\lambda \| B_{(2m+1)n}$.

LEMMA 5.8. *If $2 | C_m$, then $4 | C_{2m}$. If $2 | B_m$ and $4 | C_m$, then $16 | C_{2m}$. If $2 | B_m$, $2^\lambda \| C_m$ $(\lambda > 2)$, then $2^{\lambda+2} \| C_{2m}$. If $2 \nmid B_m$, $2^\lambda \| C_m$ $(\lambda > 1)$, then $2^{\lambda+1} \| C_{2m}$.*

Proof. Follows from the fact that if $2^\lambda | C_m$, we have from (4.8) that

$$V_{h,2m} \equiv 2 V_{h,m} V_{0,m} (\operatorname{mod} 2^{2\lambda}) \qquad (h > 0).$$

LEMMA 5.9. *If $2^\lambda | A_m$, then $2^{\lambda+1} | A_{2m}$. If $4 | C_m$ and $2^\lambda \| A_m$ $(\lambda > 1)$, then $2^{\lambda+1} \| A_{2m}$.*

Proof. Follows from (4.8) by a method similar to that used for proving Lemma 5.8.

COROLLARY. *If $4 | C_m$ and $2^\lambda \| A_m$ $(\lambda > 1)$, then $2^{\lambda+\alpha} \| A_{2^\alpha m}$.*

6. Further properties of A_n, B_n, and C_n. We begin this section with the following

DEFINITION. If A_ω is the first term of the sequence

$$A_1, A_2, \ldots, A_n, \ldots$$

in which the integer m appears as a factor, we call $\omega = \omega(m)$ the *rank of apparition* of m.

In the next two sections we will investigate the properties of $\omega(m)$ and the numbers analogous to ω for the functions B_n and C_n. The most important result concerning ω is that of Theorem 6.2; however, we must first give

LEMMA 6.1. *Let m be an integer and let $\omega = \omega(m)$. If $m | A_{q\omega+r}$ $(0 \leqslant r < \omega,\ q > 0)$, then $m | A_{q\omega-r}$.*

Proof. Putting $n = q\omega$, $m = r$ in (4.6), we get

$$U_{h,\omega q+r} = \sum_{i=0}^{k-1} \sum_{j=0}^{k-1} V_{i,r} U_{i,\omega q} - Q^r U_{q\omega-r}.$$

Since $(m, Q) = 1$ and $m | A_{\omega q}$, we see that if $m | A_{q\omega+r}$, then $m | A_{q\omega-r}$.

THEOREM 6.1. *Let $\omega = \omega(m)$. If $m | A_n$, then $\omega | n$.*

Proof. Suppose $\omega \nmid n$; then $n = q\omega + r$ $(0 < r < \omega,\ q > 0)$. From the preceding lemma we see that

$$A_{(q-1)\omega+\omega-r} \equiv 0 (\operatorname{mod} m).$$

If $q = 1$, we have $m | A_{\omega-r}$; if $q > 1$, we apply the lemma again and get

$$A_{(q-2)\omega+r} \equiv 0 (\operatorname{mod} m).$$

We continue this process until we ultimately have either $m | A_r$ or $m | A_{\omega-r}$. Since $0 < r < \omega$, neither of these results can be true by definition of ω; hence $\omega | n$.

COROLLARY 6.1.1. $(A_m, A_n) = A_{(m,n)}$.

We wish at this point to investigate a function which is similar to $\omega(m)$.

DEFINITION. Let B_σ be the first term of the sequence

$$B_1, B_2, \ldots, B_n, \ldots$$

in which an integer m occurs as a factor. The value of the function $\sigma(m)$ is defined to be σ.

In the next two results we give some properties of $\sigma(m)$ and its relation to $\omega(m)$.

LEMMA 6.2. *Let $\omega = \omega(m)$. If $2 | \omega$ and $m | B_{g\omega/2}$, where g is an odd positive integer, then $m | B_{\omega/2}$.*

Proof. Let $g = 2h+1$. From (4.4) and (4.6) we have

$$0 \equiv V_{j,g\omega/2} \equiv -Q^{\omega/2} V_{j,h\omega-\omega/2} (\operatorname{mod} m);$$

thus, $m | B_{(g-2)\omega/2}$. We repeat this process until we have $m | B_{\omega/2}$.

THEOREM 6.2. *Let m (>2) be an integer. If $\sigma\,(=\sigma(m))$ and $\omega\,(=\omega(m))$ exist for m, then $\omega=2\sigma$. Also, if $m\,|\,B_n$, then $\sigma\,|\,n$ and n/σ is odd.*

Proof. If $m\,|\,A_\sigma$, then $m\,|\,B_{2\sigma}$, $\omega\,|\,2\sigma$, and we put $2\sigma=g\omega$. If g were even, we would have $m\,|\,(A_\sigma,B_\sigma)=2$, which is not possible; thus, g is odd, ω is even and $m\,|\,B_{g\omega/2}$. By Lemma 6.2, $m\,|\,B_{\omega/2}$, consequently $\sigma\leqslant\omega/2$. Hence, $\omega=2\sigma$.

If $m\,|\,B_n$, then $m\,|\,A_{2n}$, $\omega\,|\,2n$, and $\sigma\,|\,n$. If n/σ were even, we would have $m\,|\,B_{\omega(n/2\sigma)}$ and $m\,|\,A_{\omega(n/2\sigma)}$, which is impossible, consequently n/σ is odd.

The behaviour of the sequence $\{C_n\}$ is not as simple as that of $\{A_n\}$ and $\{B_n\}$. We give two results concerning this sequence in Lemma 6.3 and Theorem 6.3.

LEMMA 6.3. *If $(m,Q)=1$, $\omega=\omega(m)$, and $m\,|\,C_n$, then $m\,|\,C_{2\omega a+bn}$, where a, b are any integers such that $2\omega a+bn\geqslant 0$.*

Proof. From (4.4) and (4.5), we see that there exists a non-negative integer g such that

$$2Q^g V_{h,2a\omega+bn}=\sum_{i=0}^{k-1}\sum_{j=0}^{k-1}(V_{i,2c\omega}V_{j,dn}Z_{h,i+j}\mp 4QU_{i,2c\omega}U_{j,dn}Z_{h,i+j}\pm \pm U_{i,2c\omega}U_{j,dn}Z_{h,i+j+2}),$$

where $c=|a|$ and $d=|b|$. Since $m\,|\,A_\omega$ and $m\,|\,C_n$, we see that $m\,|\,A_{2c\omega}$, $m\,|\,C_{2c\omega}$, $m\,|\,C_{dn}$. If m is odd, we have

$$2V_{h,2a\omega+bn}\equiv 0\ (\mathrm{mod}\ m)\qquad (h>0);$$

hence, $m\,|\,C_{2\omega a+bn}$.

If m is even, $2m\,|\,A_{2c\omega}$, $2m\,|\,C_{2c\omega}$, $2\,|\,V_{0,2c\omega}$; hence,

$$2V_{h,2a\omega+bn}\equiv 0\ (\mathrm{mod}\ 2m)\qquad (h>0)$$

and $m\,|\,C_{2a\omega+bn}$.

DEFINITION. Let m be an integer such that $(m,Q)=1$. Let C_{τ_0} be the first term of the sequence

$$(*)\qquad C_1,C_2,\ldots,C_n,\ldots$$

in which m occurs as a factor. We define the increasing sequence of integers

$$\tau_0,\tau_1,\ldots,\tau_j,\ldots$$

by saying that C_{τ_j} is the first term of the sequence $(*)$ such that $m\,|\,C_{\tau_j}$ and $\tau_i\nmid\tau_j$ $(i=0,1,\ldots,j-1)$. We call these τ_j's the *orders of apparition* of m.

THEOREM 6.3. *If $(m,Q)=1$ and τ_j is any order of apparition of m, then $\tau_j\,|\,2\omega$, where ω is the rank of apparition of m.*

Proof. We select a, b such that $2a\omega+b\tau_j=d$, where $d=(2\omega,\tau_j)$. If $d=\tau_j$, then $\tau_j\,|\,2\omega$. If $d\neq\tau_j$, then $d<\tau_j$ and since (Lemma 6.3) $m\,|\,C_d$, we must have $d=s\tau_i$ $(i<j)$. Since $d\,|\,\tau_j$, this is impossible by definition of τ_j.

We end this section with a theorem describing those members of the sequences $\{A_n\}$, $\{B_n\}$ and $\{C_n\}$, which are divisible by odd prime powers.

THEOREM 6.4. *Let p be an odd prime, m an integer such that $p\nmid m$, λ $(\geqslant 1)$ an integer. If $p^\lambda\,\|\,A_n$, then $p^{\lambda+\alpha}\,\|\,A_{p^\alpha nm}$; if $p^\lambda\,\|\,B_n$, then $p^{\lambda+\alpha}\,\|\,B_{p^\alpha nm}$; and if $p^\lambda\,|\,C_n$ then $p^{\lambda+\alpha}\,|\,C_{p^\alpha n}$.*

Proof. Let $\{i_0,i_1,\ldots,i_{k-1}\}$ be any set of k non-negative integers such that

$$\sum_{j=0}^{k-1}i_j=p-2r,$$

for a fixed integral value of $r\leqslant(p-1)/2$. Since

$$\prod_{j=0}^{k-1}U_{j,n}^{i_j}\equiv 0\ (\mathrm{mod}\ p^{3\lambda})\quad (r\neq(p-1)/2)\equiv 0\ (\mathrm{mod}\ p^{(p-2r)\lambda})$$

when $p^\lambda\,|\,A_n$, we see by the second formula of (4.13) that

$$U_{h,pn}\equiv\frac{p}{(p-1)/2}\binom{p-(p-1)/2-1}{(p-1)/2-1}Q^{n(p-1)/2}\sum_{i=0}^{k-1}Z_{h,i}U_{i,n}\ (\mathrm{mod}\ p^{3\lambda})$$
$$\equiv pQ^{n(p-1)/2}U_{h,n}\ (\mathrm{mod}\ p^{\lambda+2}).$$

Thus, if $p^\lambda\,\|\,A_n$, then $p^{\lambda+1}\,\|\,A_{pn}$ and by induction $p^{\lambda+\alpha}\,\|\,A_{p^\alpha n}$. If $p^{\lambda+\alpha+1}\,|\,A_{p^\alpha nm}$, then $p^{\lambda+\alpha+1}\,|\,(A_{p^{\alpha+1}n},A_{p^\alpha nm})$ or $p^{\lambda+\alpha+1}\,|\,A_{p^\alpha n}$ which is not so. The proof of the other statements of the theorem is similar to that given above.

The results in Theorem 6.4 and Lemmas 5.7, 5.8 and 5.9 are called collectively the *Laws of Repetition for A_n, B_n, and C_n*.

7. The Law of Apparition. We have not yet shown (apart from direct calculation) how the value of $\omega(m)$ may be determined for any given m, Q and f; indeed, we have not shown under what conditions $\omega(m)$ even exists. In this section we give those values of m for which $\omega(m)$ exists and we give a function Φ of m, Q, f such that when $\omega(m)$ exists, $\omega(m)\,|\,\Phi(m)$. We first define $\Phi(m)$ for a fixed Q and f.

DEFINITION. If Q and f of Section 2 are fixed we define the function Φ in the following manner.

(i) Let p be any prime.
If $p\,|\,\Delta$, let

$$F(x)\equiv\prod_{i=1}^{\varkappa}\psi_i(x)^{e_i}\ (\mathrm{mod}\ p)$$

be the Schönemann decomposition of $F(x)$ into irreducible functions ψ_i $(i=1,2,\ldots,\varkappa)$ modulo p. Let the degree of ψ_i be μ_i and $e=\max(e_1,e_2,\ldots,e_\varkappa)$. If μ is an integer such that $p^\mu \leqslant e < p^{\mu+1}$, we define

$$\Phi(p)=p^{\mu+1}[p^{\mu_1}-1,\, p^{\mu_2}-1,\,\ldots,\, p^{\mu_k}-1].$$

If $p\nmid\Delta$, let

$$f(x)\equiv\prod_{i=1}^{\lambda}\varphi_i(x)\ (\mathrm{mod}\,p)$$

where the φ_i are irreducible modulo p and the degree of φ_i is ν_i. If $\varepsilon_i=(E_i|p)$, where $E_i=\varphi_i(2\sqrt{Q})\varphi_i(-2\sqrt{Q})$ and $(E_i|p)$ is the Kronecker symbol, we define

$$\Phi(p)=[p^{\nu_1}-\varepsilon_1,\, p^{\nu_2}-\varepsilon_2,\,\ldots,\, p^{\nu_\lambda}-\varepsilon_\lambda].$$

(ii) $\Phi(p^n)=p^{n-1}\Phi(p)$, where p is a prime.

(iii) $\Phi(mn)=[\Phi(m),\Phi(n)]$ when m and n are integers such that $(m,n)=1$.

THEOREM 7.1 (The Law of Apparition). *If p is any prime such that $p\nmid Q$, then $\omega(p)$ exists and $\omega(p)\,|\,\Phi(p)$.*

Proof. If $p\,|\,\Delta$, the theorem follows from (4.1) and general results of Engstrom [5].

If $p\nmid\Delta$, consider $f(x)$ to be a polynomial in the (finite) Galois Field $\mathrm{GF}(p)$ and let $K=\mathrm{GF}(p^\nu)$, where $\nu=[\nu_1,\nu_2,\ldots,\nu_\lambda]$, be the field which contains all the roots of $f(x)=0$. Let these roots be denoted by ϱ_{ij} $(i=1,2,\ldots,\lambda;\ j=1,2,\ldots,\nu_i)$, where, for a fixed value of i, ϱ_{ij} $(j=1,2,\ldots,\nu_i)$ are all the roots of $\varphi_i(x)=0$. Since φ_i is irreducible in $\mathrm{GF}(p)$, we have

$$\varrho_{ij}=\varrho_{i1}^{p^{j-1}}\quad\text{and}\quad \varrho_{ij}^{p^{\nu_i}}=\varrho_{ij}$$

in K.

If we put

$$\delta^*=\delta(\varrho_{11},\varrho_{12},\ldots,\varrho_{1\nu_1},\varrho_{21},\ldots,\varrho_{2\nu_2},\ldots,\varrho_{\lambda\nu_\lambda}),$$

$$V_{j,n}^*=H_{j,n}(\varrho_{11},\varrho_{12},\ldots,\varrho_{1\nu_1},\varrho_{21},\ldots,\varrho_{2\nu_2},\ldots,\varrho_{\lambda\nu_\lambda}),$$

$$U_{j,n}^*=G_{j,n}(\varrho_{11},\varrho_{12},\ldots,\varrho_{1\nu_1},\varrho_{21},\ldots,\varrho_{2\nu_2},\ldots,\varrho_{\lambda\nu_\lambda}),$$

then $V_{j,n}^*,\,U_{j,n}^*\in\mathrm{GF}(p)$ and $V_{j,n}\equiv V_{j,n}^*(\mathrm{mod}\,p)$, $U_{j,n}\equiv U_{j,n}^*(\mathrm{mod}\,p)$.

Case 1: p an odd prime. Using (3.9) we see that in K

$$u_{p^{\nu_i}}(\varrho_{ij})=(\varrho_{ij}^2-4Q)^{(p^{\nu_i}-1)/2}=\prod_{a=0}^{\nu_i-1}(\varrho_{ij}^{2p^a}-4Q)^{(p-1)/2}$$

$$=\Big\{\prod_{j=1}^{\nu_i}(\varrho_{ij}^2-4Q)\Big\}^{(p-1)/2}=E_i^{(p-1)/2}$$

Now if

$$\varphi_i(x)=\sum_{j=0}^{\nu_i}a_{ij}x^{\nu_i-j},\tag{7.1}$$

we have

$$E_i=\Big(\sum_{j=0}^{[\nu_i/2]}a_{\nu_i-2j}2^{2j}Q^j\Big)^2-Q\Big(\sum_{j=0}^{[(\nu_i-1)/2]}a_{\nu_i-2j-1}2^{2j+1}Q^j\Big)^2;$$

hence, $E_i\equiv 1,\ 0\,(\mathrm{mod}\,4)$ and $E_i^{(p-1)/2}\equiv(E_i|p)\equiv\varepsilon_i=0,\ -1,\ 1$. We also have

$$v_{p^{\nu_i}}(\varrho_{ij})=\varrho_{ij}^{p^{\nu_i}}=\varrho_{ij}.$$

From (3.2), we see that if $\varepsilon_i\neq 0$, $Q^{\varepsilon_i}u_{p^{\nu_i}-\varepsilon_i}(\varrho_{ij})=0$; thus, since $u_{nm}(x)=u_n(x)g_{mn}(x)$, where $g_{mn}(x)$ is a polynomial with integer coefficients we have $u_\Phi(\varrho_{ij})=0$ for all i,j and consequently $U_{j,\Phi}\equiv 0\,(\mathrm{mod}\,p)$ $(j=0,1,\ldots,k-1)$.

Case 2: $p=2$. Assuming that $\varphi_i(x)$ is given by (7.1); we deduce from (3.10) that

$$u_{2^{\nu_i}}(\varrho_{ij})=\prod_{h=0}^{\nu_i-1}\varrho_{ij}^{2^h}=a_{i\nu_i}.$$

From (3.11) we find that

$$u_{2^{\nu_i}+1}(\varrho_{ij})=\varrho_{ij}^{2^{\nu_i}}+\sum_{h=1}^{\nu_i}\varrho_{ij}^{2^{\nu_i}-2^h}=\varrho_{ij}+\varrho_{ij}\Big(\sum_{h=1}^{\nu_i}\varrho_{ij}^{-2^h}\Big)$$

$$=\varrho_{ij}(1+a_{i,\nu_i-1})\qquad(a_{i\nu_i}\neq 0).$$

Also

$$u_{2^{\nu_i}-1}(\varrho_{ij})=\varrho_{ij}(a_{i,\nu_i-1})\qquad(a_{i\nu_i}\neq 0).$$

Now

$$E_i\equiv a_{i\nu_i}^2-4a_{i,\nu_i-1}^2\ (\mathrm{mod}\,8);$$

thus, $2\,|\,a_{i\nu_i}$ if and only if $2\,|\,E_i$. If $2\nmid E_i$, $2\,|\,a_{i,\nu_i-1}$, if and only if $E_i\equiv 1\,(\mathrm{mod}\,8)$ and $2\nmid a_{i,\nu_i-1}$ if and only if $E_i\equiv 5\,(\mathrm{mod}\,8)$. We have shown that

$$u_{2^{\nu_i}-\varepsilon_i}(\varrho_{ij})=0$$

where $\varepsilon_i=(E_i|2)$. It follows that $p\,|\,A_\Phi$.

COROLLARY 7.1. *$\omega(m)$ exists if and only if $(m,Q)=1$. If $(m,Q)=1$, $\omega(m)\,|\,\Phi(m)$.*

It should be noted that this result is not as precise as that of Lehmer [7] for his functions $\overline{V}_n$ and $\overline{U}_n$.

In the case of an odd prime p $(p \nmid DQ)$ we can be somewhat more precise than we were in Theorem 7.1. We put $\Phi_i = \Phi/(p^{\nu_i} - \varepsilon_i)$ and $\eta = (Q\,|\,p)$, where $(Q\,|\,p)$ is the Legendre symbol.

THEOREM 7.2. *If p is an odd prime and $(p, DQ) = 1$, then $\omega(p)\,|\,\Phi(p)/2$ if and only if one of the following is true*

1) $\eta = 1$,

2) $\eta = -1, 2\,|\,\nu_i\Phi_i$ $(i = 1, 2, \ldots, \lambda)$.

Proof. We use the same symbols that were used in Theorem 7.1. Since in K

$$\sum_{h=0}^{k-1} U_{h,n}^{*}\varrho_{ij}^{h} = u_n(\varrho_{ij}) \qquad (i = 1, 2, \ldots, \lambda;\ j = 1, 2, \ldots, \nu_i)$$

and $p \nmid \Delta\ (= \delta^{*2})$, we see that $p\,|\,A_n$ if and only if $u_n(\varrho_{ij}) = 0$ $(i = 1, 2, \ldots, \lambda;$ $j = 1, 2, \ldots, \nu_i)$.

From the results of Theorem 7.1, we determine that

$$v_{p^{\nu_i} - \varepsilon_i}(\varrho_{ij}) = 2Q^{\gamma_i} \qquad (\gamma_i = (1-\varepsilon_i)/2).$$

Hence, by induction we have

$$v_{n(p^{\nu_i} - \varepsilon_i)} = 2Q^{n\gamma_i}$$

and consequently

$$v_{\Phi}(\varrho_{ij}) = 2Q^{\gamma_i\Phi_i}.$$

Now if $\varepsilon_i = -1$,

$$\frac{p^{\nu_i} - \varepsilon_i}{2} = \begin{cases} (p+1)/2 + m(p-1) & \text{when } \nu_i \text{ is odd,} \\ (p+1)/2 + (2m+1)(p-1)/2 & \text{when } \nu_i \text{ is even,} \end{cases}$$

where m is an integer. Hence

$$Q^{(p^{\nu_i} - \varepsilon_i)/2} \equiv \eta^{\nu_i} Q \pmod{p}$$

and

$$v_{\Phi}(\varrho_{ij}) = 2\eta^{\nu_i\Phi_i} Q^{\Phi/2}$$

when $\varepsilon_i = -1$.

If $\varepsilon_i = +1$, $v_{\Phi}(\varrho_{ij}) = 2$, and

$$Q^{\Phi/2} \equiv \eta^{\nu_i\Phi_i} \pmod{p}.$$

From (3.5) we see that

$$v_{\Phi/2}(\varrho_{ij})^2 = 2Q^{\gamma_i\Phi/2}(1 + \eta^{\nu_i\Phi_i}).$$

Since

$$0 = u_{\Phi}(\varrho_{ij}) = u_{\Phi/2}(\varrho_{ij})\,v_{\Phi/2}(\varrho_{ij})$$

and

$$v_{\Phi/2}(\varrho_{ij})^2 - (\varrho_{ij}^2 - 4Q)\,u_{\Phi/2}(\varrho_{ij})^2 = 4Q^{\Phi/2},$$

we see that

$$u_{\Phi/2}(\varrho_{ij}) = 0 \qquad (i = 1, 2, \ldots, \lambda;\ j = 1, 2, \ldots, \nu_i)$$

if and only if $1 + \eta^{\nu_i\Phi_i} \neq 0$ $(i = 1, 2, \ldots, \lambda)$.

COROLLARY 7.2.1. *If p is a prime and $(p, 2DQ) = 1$, then $\sigma(p)$ exists if and only if $\eta = -1$, $2 \nmid \nu_i$ $(i = 1, 2, \ldots, \lambda)$ and $\varepsilon_1 = \varepsilon_2 = \ldots = \varepsilon_\lambda$.*

Proof. $p\,|\,B_{\Phi/2}$ if and only if in K

$$v_{\Phi/2}(\varrho_{ij}) = 0 \qquad (i = 1, 2, \ldots, \lambda;\ j = 1, 2, \ldots, \nu_i).$$

Also $1 + \eta^{\gamma_i\Phi_i} = 0$ $(i = 1, 2, \ldots, \lambda)$ if and only if $\eta = -1$, $2 \nmid \nu_i$ $(i = 1, 2, \ldots, \lambda)$ and $\varepsilon_1 = \varepsilon_2 = \ldots = \varepsilon_\lambda$.

8. Tests for primality. One of the most interesting features of Lucas' functions and Lehmer's functions is that they can be used to test integers for primality. In this section we show that the generalized functions may also be used to test the primality of certain integers. In Theorem 8.1 we give a result analogous to that of Lucas ([11], p. 302); however, we require a preliminary lemma.

LEMMA 8.1. *If p is an odd prime and $(p, QD) = 1$, then $\Phi(p) \leqslant 1 + p^k$.*

Proof.

$$\Phi(p) = 2\,[(p^{\nu_1} - \varepsilon_1)/2, (p^{\nu_2} - \varepsilon_2)/2, \ldots, (p^{\nu_\lambda} - \varepsilon_\lambda)/2] \leqslant 2\prod_{i=1}^{\lambda}(p^{\nu_i} + 1)/2.$$

Since, for $\lambda = 1$, we have

$$p^k + 1 = 2\prod_{i=1}^{\lambda}(p^{\nu_i} + 1)/2$$

and, for $\lambda > 1$,

$$p^{-k}\prod_{i=1}^{\lambda}(p^{\nu_i} + 1) = \prod_{i=1}^{\lambda}(1 + p^{-\nu_i}) \leqslant (4/3)^{\lambda} < 2^{\lambda-1},$$

the lemma follows.

THEOREM 8.1. *If $(N, 2DQ) = 1$ and the rank of apparition of N is $N^k \pm 1$, then N is a prime.*

Proof. Suppose N is composite and $\omega(N) = N^k \pm 1$. We have

$$N = \prod_{i=1}^{n} p_i^{\alpha_i},$$

where the p_i are distinct primes. If we put

$$J = 2\prod_{i=1}^{n} p_i^{\alpha_i - 1}\Phi(p_i)/2,$$

we see that $\Phi(N)\,|\,J$. Since

$$J/N^k \leqslant 2^{n-1}\prod_{i=1}^{n}\Phi(p_i)/p_i^k,$$

we have

$$J/N^k \leqslant 2\prod_{i=1}^{n}(1+p_i^{-k})/2.$$

If $n \geqslant 2$, then $N > 5$ and

$$J/N^k < (1+1/3)(1+1/5)/2 = 4/5.$$

If $n = 1$, then $\alpha_1 \geqslant 2$ and

$$J/N^k \leqslant (1+p^{-k})/p^k < 4/9.$$

Thus, if N is composite, there exists an integer J such that $J < \omega(N)$ and $\Phi(N)\,|\,J$. Since $\omega(N)\,|\,\Phi(N)$, N must be prime.

With this result it is not difficult (Lehmer [7]) to prove

THEOREM 8.2. *If $(N, 2DQ) = 1$, $m = N^k \pm 1$, $N\,|\,A_m$, and for each prime divisor r_i of m, $A_{m_i} \not\equiv 0 \pmod N$, where $m_i = m/r_i$, then N is a prime.*

We can also give some results which limit the possible prime divisors of an integer N.

THEOREM 8.3. *Let $(N, 2DQ) = 1$ and $N\,|\,C_m$ (or A_m). If r is a prime divisor of m and $N \nmid C_{m/r}$ (or $A_{m/r}$), then the prime divisors of N which do not divide both N and $C_{m/r}$ (or $A_{m/r}$) must satisfy the congruence*

$$p^s \equiv \pm 1 \pmod{r^a},$$

where $r^a \| m$ and s is some integer such that $1 \leqslant s \leqslant k$.

Proof. Let p be a prime such that $p\,|\,N$ and $p \nmid (N, C_{m/r})$. There exists an order of apparition τ of p such that $\tau\,|\,m$ and $\tau \nmid m/r$; hence, $r^a\,|\,\tau$. Since $\tau\,|\,2\omega$, $\omega\,|\,\Phi(p)$, and

$$\Phi(p) = [p^{\nu_1}-\varepsilon_1, p^{\nu_2}-\varepsilon_2, \ldots, p^{\nu_\lambda}-\varepsilon_\lambda],$$

where $|\varepsilon_i| = 1$ and $\nu_i \leqslant k$, we see that for some j

$$p^{\nu_j} \equiv \varepsilon_j \pmod{r^a}.$$

The proof of this theorem for the function A_m is similar to that given above.

A frequently useful means of determining when $N\,|\,A_{tr}$ and $(N, A_t) = 1$ is given in

LEMMA 8.2. *If r is an odd prime, $s = (r-1)/2$, $(N, 2rQ) = 1$, $MQ \equiv 1 \pmod N$, and*

$$Y_{i,s}(M^tV_{0,2t}, M^tV_{1,2t}, \ldots, M^tV_{k-1,2t}) \equiv 0 \pmod N \quad (i = 0, 1, \ldots, k-1),$$

then

$$N\,|\,A_{rt} \quad \text{and} \quad (N, A_t) = 1.$$

Proof. From (4.12), it follows that $N\,|\,A_{rt}$. If p is a prime such that $p\,|\,(N, A_t)$, then by using (4.9), we obtain the results

$$V_{h,2t} \equiv 2\delta_{0,h}Q^t \pmod p \quad (h = 0, 1, \ldots, k-1).$$

Since $p\,|\,N$ and $N\,|\,Y_{0,s}(M^tV_{0,2t}, M^tV_{1,2t}, \ldots, M^tV_{k-1,2t})$, we must have

$$Y_{0,s}(2, 0, 0, \ldots, 0) = 2s+1 = r \equiv 0 \pmod p.$$

Since $(N, r) = 1$, this is impossible; thus, $(N, A_t) = 1$.

This lemma allows us to deduce a result concerning the values of $U_{i,rt} \pmod N$ when we know only the values of $M^tV_{i,2t} \pmod N$ $(i = 0, 1, \ldots, k-1)$. When $(N, P_kQ) = 1$, we can calculate $M^nV_{i,2n} \pmod N$ for any $n > 0$ in approximately $O(\log n)$ operations. We will not need to calculate any values of the U's in order to do this.

We let S, M be integers such that

$$QM \equiv (-1)^{k+1}P_kS \equiv 1 \pmod N$$

and define

$$W_{h,n} = \begin{cases} S^2M^{n/2}V_{h,n} & (n \text{ even}), \\ SM^{(n+1)/2}V_{h,n} & (n \text{ odd}). \end{cases}$$

From (4.7) we have

$$W_{k-1,2m+1} \equiv W_{0,2(m+\ )} + W_{0,2m},$$

$$\text{(8.1)} \quad W_{h-1,2m+1} \equiv (-1)^{k+1}P_k(W_{h,2m+2}+W_{h,2m}) + (-1)^{k-h}P_{k-h}W_{k-1,2m+1}$$
$$(h = 1, 2, \ldots, k-1) \quad \pmod N,$$

and from (4.8) we have

$$\text{(8.2)} \quad \left.\begin{aligned} W_{h,2m} &\equiv Q\sum_{i=0}^{k-1}\sum_{j=0}^{k-1}W_{i,m}W_{j,m}Z_{h,i+j} - 2\delta_{h,0}S^2 \quad (m \text{ odd}) \\ W_{h,2m} &\equiv P_k^2\sum_{i=0}^{k-1}\sum_{j=0}^{k-1}W_{i,m}W_{j,m}Z_{h,i+j} - 2\delta_{h,0}S^2 \quad (m \text{ even}) \end{aligned}\right\} \pmod N.$$

Using (8.1) and (8.2), we can find $W_{i,n} \pmod N$ by employing a power algorithm technique similar to that of Lehmer [9]. This algorithm will determine $W_{i,n} \pmod N$ in $O(\log n)$ operations.

If $N = 2Ar^n-1$, where r is an odd prime, we are able to obtain some results which can be used to strengthen Theorem 8.3 when $k = 2$ and $k = 3$.

LEMMA 8.3. *Let $N = 2Ar^n-1$, where r is an odd prime and $A < r^{n/2}$. If any prime divisor of N must satisfy one of the congruences*

$$x \equiv \pm 1 \pmod{r^n},$$
$$x^2 \equiv -1 \pmod{r^n},$$

then N is a prime or the square of a prime.

Proof. Let p be any prime divisor of N. If $p \equiv \pm 1 \pmod{r^n}$, then

$$p = 2mr^n \pm 1 \qquad (m \geqslant 1).$$

Let x_1, x_2 be the two roots of

$$x^2 \equiv -1 \pmod{r^n}$$

such that $0 < x_1, x_2 < r^n$. Clearly $x_1+x_2 = r^n$. If $p^2 \equiv -1 \pmod{r^n}$, we have

$$p = x_i + hr^n \qquad (i = 1 \text{ or } 2,\ h \geqslant 0),$$
$$p^2 = -1+2jr^n \qquad (j \geqslant 1).$$

If N is not a prime or the square of a prime, then $N = pqN_1$ or $N = p^3N_2$, where p, q are distinct primes and N_1, N_2 are positive integers. Since $p^3 \geqslant (2r^n-1)^{3/2} > N$ and $(2r^n \pm 1)(2r^n-1)^{1/2} > N$, we must have $N = pqN_1$, where $p = x_i + h_1 r^n$ and $q = x_j + h_2 r^n$. If $i = j$, we have $h_1 \neq h_2$ and $h_1 \equiv h_2 \pmod 2$; thus,

$$pq > (2r^n-1)^{1/2}\{(2r^n-1)^{1/2}+2r^n\} > N.$$

Since $i \neq j$, r^n is odd, and $x_j = r^n - x_i$, h_1 and h_2 can not both be zero; consequently,

$$pq \geqslant x_i(2r^n - x_i) \qquad (h_1 = 0,\ h_2 = 1) \qquad \text{or}$$
$$pq \geqslant (x_i + r^n)(r^n - x_i) \qquad (h_1 = 1,\ h_2 = 0).$$

If $h_1, h_2 > 0$, it is clear that $pq > N$. In both of the above formulas for pq, we have $pq \equiv -x_i^2 \equiv 1 \pmod{r^n}$; consequently, $pq \neq N$. Thus, there exists a prime s such that $s \mid N_1$, and $s > (2r^n-1)^{1/2}$. Since $spq > N$, it follows that N must be a prime or the square of a prime.

LEMMA 8.4. *Let $N = 2Ar^n-1$, where r is an odd prime and $2A < r^{n/2}$. If any prime factor of N must satisfy one of the congruences*

$$x^s \equiv \pm 1 \pmod{r^n} \qquad (s = 1, 2, 3),$$

then N is a prime or the square of a prime.

Proof. Let p be any prime factor of N. If $p^2-1 \equiv 0 \pmod{r^n}$, then $p = 2mr^n \pm 1$. If $p^2+1 \equiv 0 \pmod{r^n}$, then $p > (2r^n-1)^{1/2}$. Let x_1, x_2 be the two roots of

$$(1) \qquad x^2 - x + 1 \equiv 0 \pmod{r^n}$$

such that

$$0 < x_1, x_2 < r^n$$

and let x_3, x_4 be the two roots of

$$(2) \qquad x^2 + x + 1 \equiv 0 \pmod{r^n}$$

such that

$$0 < x_3, x_4 < r^n.$$

Thus, if $p^2 \not\equiv \pm 1 \pmod{r^n}$, we have

$$p = x_i + hr^n \qquad (i = 1, 2, 3, \text{ or } 4,\ h \geqslant 0).$$

It should be noted here that

$$x_1 + x_2 = r^n + 1, \qquad x_3 + x_4 = r^n - 1,$$
$$x_3 = x_2 - 1, \qquad x_4 = x_1 - 1, \qquad x_1, x_2 > r^{n/2}, \qquad x_3, x_4 > r^{n/2} - 1.$$

If $N = pqsN_1$, where p, q, s are distinct primes, then, since $p, q, s \geqslant [r^{n/2}]$, we have

$$N \geqslant [r^{n/2}]([r^{n/2}]+2)([r^{n/2}]+4) > ([r^{n/2}]+1)^3 > r^{3n/2} > N.$$

If $N = p^3N_2$ and p does not satisfy (2), then $p \geqslant [r^{n/2}]+1$ and $N \geqslant ([r^{n/2}]+1)^3 > N$. If $N = p^3N_2$ and p satisfies (2), then $N_2 = 1$; for, if $N_2 \neq 1$, then $N_2 \geqslant 3$, and $N \geqslant 3p^3 > 3(r^{n/2}-1)^3 > N$. On the other hand, if $N = p^3$, then $p^3 \equiv -1 \pmod{r^n}$; but, since p satisfies (2), $p^3 \equiv 1 \pmod{r^n}$; thus, $N \not\equiv p^3N_2$.

If $N = pq^2N_3$, it follows that $N_3 = 1$. If q does not satisfy (2),

$$N \geqslant [r^{n/2}]([r^{n/2}]+2)^2 > ([r^{n/2}]+1)^3 > N.$$

If q satisfies (2), then, since $pq^2 \equiv -1 \pmod{r^n}$, we have

$$p \equiv -q \pmod{r^n}, \qquad p \geqslant 2r^n - q, \qquad \text{and} \qquad pq^2 > N.$$

We have shown that $N = p$, p^2 or pq; it remains to show that $N \neq pq$. If $N = pq$ and $p^2 \equiv 1 \pmod{r^n}$, we have

$$pq > (2r^n - 1)(r^{n/2} - 1) > N.$$

If $p^2 \equiv -1 \pmod{r^n}$, we must have (Lemma 8.3) q satisfying one of (1) or (2); however, since $pq \equiv -1 \pmod{r^n}$, this cannot be, and consequently both p and q must satisfy either (1) or (2); further, if p satisfies (1), then q must satisfy (2). Thus,

$$N = pq = (x_i + h_1r^n)(r^n - x_j + h_2r^n) \qquad (h_1, h_2 \geqslant 0;\ i, j \leqslant 2;\ i \neq j).$$

If $h_1, h_2 > 0$, $pq > N$ and, if $h_1 = h_2 = 0$, pq is even; hence,

$$N \geqslant x_i(r^n + x_i - 1) \qquad \text{or} \qquad N \geqslant (x_i - 1)(x_i + r^n) \qquad (i \leqslant 2).$$

Now $x_i^2 - x_i \geqslant r^n - 1$; consequently, if $N = pq$, we deduce the contradiction $N > N$.

9. Some special cases. Let q, r be odd primes such that $q \equiv 1 \pmod{r}$. Let $\zeta = \exp(2\pi i/r)$, $\eta = \exp(2\pi i/q)$, Ω be the field generated by adjoining ζ to the rationals, and $\Omega(\eta)$ be the field generated by adjoining η to Ω. For ξ any primitive rth root of unity and $\varkappa$ any primitive qth root of unity, we define the Lagrange Resolvent

$$(\xi, \varkappa) = \sum_{i=0}^{q-2} \xi^i \varkappa^{g^i},$$

where g is any fixed primitive root of q. It is well known (see, for example, Landau [6]) that

$$(\xi, \eta^n) = (\xi, \eta)\,\xi^{-\mathrm{Ind}_g n} \qquad ((n, q) = 1),$$

$$(\xi, \eta)(\xi^{-1}, \eta) = q,$$

$$(\xi, \eta)^r = q\psi_1(\xi)\psi_2(\xi) \dots \psi_{r-2}(\xi),$$

where

$$\psi_i(\xi) = \sum_{j=0}^{q-2} \xi^{\mathrm{Ind}_g j - (i+1)\mathrm{Ind}_g (j+1)} \in \Omega.$$

If we put

$$s = (r-1)/2 \quad \text{and} \quad q\varrho_i = (\zeta^i, \eta)^r + (\zeta^{-i}, \eta)^r,$$

then ϱ_i $(i = 1, 2, \dots, s)$ are the s zeros of a polynomial

$$\sum_{i=0}^{s} x^{s-i}(-1)^i P(i, q, r),$$

where $P(0, q, r) = 1$, and $P(i, q, r)$ $(i = 1, 2, \dots, s)$ are integers. We give some tables of these integers for $r = 5$ and $r = 7$ below.

Table 1 $(r = 5)$

q	$P(1, r, q)$	$P(2, r, q)$
11	−89	1199
31	−409	22289
41	981	239809
61	1111	214049
71	101	−1310731
101	−1779	−522071
131	−4009	3735989
151	596	−4423696
181	1691	−7254661
191	1331	−18326641
211	961	−24801151
241	−3344	1283084

Table 2 $(r = 7)$

q	$P(1, r, q)$	$P(2, r, q)$	$P(3, r, q)$
29	−10961	−19689840	334583935349
43	34399	242623974	−290365049983
71	19965	−4159287778	35260324787309
113	−112965	−35791888036	48967363182583
127	219437	−68889533036	−1128952879891337З
197	−1587949	710594033070	−9617521217237693З
211	513941	−1325614078980	−574749504721836053

For $r = 5$, it can be shown that

$$P(1, q, 5) = \left(x^3 + 625(u^2 - v^2)w\right)/8 - qx, \qquad P(2, q, 5) = (P_1^2 - 5d^2)/4,$$

where

$$d = 25\left(10w(u^2+v^2) + x(u^2 - v^2 - 4uv) - 25w^3\right)/16.$$

The values of the integers x, u, v, w, are determined from the representation (Dickson [4])

$$16q = x^2 + 50u^2 + 50v^2 + 125w^2,$$

where

$$xw = v^2 - u^2 - 4uv, \qquad x \equiv 1 \pmod{5}.$$

We now require

LEMMA 9.1.

$$\left(P(1, q, r), P(2, q, r), \dots, P(s, q, r), q\right) = 1.$$

Proof. Suppose the lemma is false; then $q \mid R_i$ $(i = 1, 2, \dots, 2s)$, where

$$\sum_{i=0}^{2s} (-1)^i R_i x^{r-i-1} = 0 \qquad (R_0 = 1)$$

is the equation satisfied by $(\zeta^i, \eta)^r/q$ $(i = 1, 2, \dots, 2s)$. If we put $\gamma = (\zeta, \eta)^r$, it is evident that

$$\gamma^{r-1} = \sum_{i=1}^{r-1} q^i R_i (-1)^{i+1} \gamma^{r-i-1}.$$

Now in Ω we know ([6], p. 289) that the ideal

$$[q] = \prod_{i=0}^{r-2} \mathfrak{q}_i,$$

where the $\mathfrak{q}_i$ are distinct prime ideals,

$$\mathfrak{q}_i = [q, g^h - \zeta^{j^i}], \qquad h = (q-1)/r$$

and j is a fixed primitive root of r. We also have ([6], p. 292)

$$[\gamma] = \prod_{i=0}^{r-2} \mathfrak{q}_i^{t_i},$$

where $t_i \equiv -j^{r-1-i} \pmod{r}$, $1 \leqslant t_i \leqslant r-1$.

Since

$$\gamma \equiv 0 \pmod{[q]},$$

we have

$$\gamma^{r-1} \equiv 0 \pmod{[q]^r}$$

and consequently

$$\mathfrak{q}_s^r \mid [\gamma]^{r-1}.$$

Now

$$[\gamma]^{r-1} = \prod_{i=0}^{r-2} \mathfrak{q}_i^{t_i(r-1)}$$

and $t_s = 1$; hence, $\mathfrak{q}_s^r \nmid [\gamma]^{r-1}$ and it follows that the lemma must be true.

For given values of r and q, we consider the functions A_n and C_n, where $k = s$, $P_i = P(i, q, r)$ $(i = 1, 2, \ldots, s)$, and $Q = q^{r-2}$. It will be seen that these functions have some rather remarkable properties.

Let p be any prime such that $p \neq r, q$ and let p belong to index $\nu \pmod{r}$. Put $\mu = \nu/2$ if ν is even; otherwise, put $\mu = \nu$. Define $\theta(p) = \big(p^\mu + (-1)^\nu\big)/r$ and put $\lambda = \operatorname{Ind}_q p$.

In $\Omega(\eta)$ ([6], p. 301)

$$(\xi, \eta)^{p^\mu} \equiv (\xi^{(-1)^{\nu+1}}, \eta^{p^\mu}) \equiv (\xi^{(-1)^{\nu+1}}, \eta)\,\xi^{-\mu\lambda} \pmod{p}.$$

Thus, if $\theta = \theta(p)$ and $\varepsilon = \big(1 + (-1)^\nu\big)/2$, we have

$$(\xi, \eta)^{r\theta} \equiv \xi^{-\mu\lambda} q^{\varepsilon} \pmod{p}$$

in Ω. Hence

$$q^{\theta m} v_{\theta m}(\varrho_i) \equiv (\zeta^{i\mu\lambda m} + \zeta^{-i\mu\lambda m})\, q^{\varepsilon m} \pmod{p},$$
$$q^{\theta m} \sigma_i u_{\theta m}(\varrho_i) \equiv (\zeta^{i\mu\lambda m} - \zeta^{-i\mu\lambda m})\, q^{\varepsilon m} \pmod{p},$$

where

$$q\sigma_i = (\zeta^i, \eta)^r - (\zeta^{-i}, \eta)^r.$$

THEOREM 9.1. *Let the functions A_n and C_n be those obtained for $k = s$, $P_i = P(i, q, r)$ $(i = 1, 2, \ldots, s)$, $Q = q^{r-2}$ and let p be a prime such that $(p, q\Delta E) = 1$. If $(p \mid q)_r = 1$,*

$$p \mid A_\theta \quad \textit{and} \quad p \mid C_\theta.$$

If $(p \mid q)_r \neq 1$,

$$p \mid A_{r\theta}, \quad p \mid C_{r\theta} \quad \textit{and} \quad p \nmid A_{m\theta} C_{m\theta} \quad \textit{when} \quad (m, r) = 1.$$

Proof. If $r \mid \lambda m$, we have in Ω

$$q^{\theta m} v_{\theta m}(\varrho_i) \equiv 2q^{\varepsilon m} \pmod{p} \quad \text{and} \quad q^{\theta m} \sigma_i u_{\theta m}(\varrho_i) \equiv 0 \pmod{p}.$$

It follows that

$$q^{\theta m} V_{0,\theta m} - 2q^{\varepsilon m} + \sum_{j=1}^{s-1} q^{m\theta} V_{j,m\theta}\, \varrho_i^j \equiv 0 \pmod{p} \qquad (i = 1, 2, \ldots, s)$$

and

$$q^{\theta m} \sum_{j=0}^{s-1} \sigma_i U_{j,m\theta}\, \varrho_i^j \equiv 0 \pmod{p}.$$

Since $p \nmid q\Delta E$, we have $V_{0,\theta m} \equiv 2q^{\varepsilon m} \pmod{p}$ and $p \mid C_{\theta m}$, $p \mid A_{\theta m}$. Now $r \mid \lambda$ if and only if $(p \mid q)_r = 1$; hence, we have proved the first part of the theorem.

If $(p \mid q)_r \neq 1$ and $(r, m) = 1$, then, since $p \nmid \Delta$,

$$\zeta^{i\lambda\mu m} - \zeta^{-i\lambda\mu m} \not\equiv 0 \pmod{p}$$

and consequently $p \nmid A_{\theta m}$. If $p \mid C_{m\theta}$, we have the s congruences

$$q^{\theta m} V_{0,\theta m} \equiv (\zeta^{i\lambda\mu m} + \zeta^{-i\lambda\mu m})\, q^{\varepsilon m} \pmod{p} \qquad (i = 1, 2, \ldots, s).$$

These congruences can not all hold unless $r \mid i\lambda\mu m$, which is not so.

COROLLARY 9.1.1. *If $(p, \Delta q) = 1$, $(p \mid q)_r \neq 1$, and $MQ \equiv 1 \pmod{p}$, then*

$$Y_{i,s}(M^\theta V_{0,2\theta}, M^\theta V_{1,2\theta}, \ldots, M^\theta V_{s-1,2\theta}) \equiv 0 \pmod{p}.$$

Proof. We first note that $Q^{-\theta} \equiv q^{2(\theta-\varepsilon)} \pmod{p}$. Since $r \nmid 2\mu\lambda i$, $\zeta^{-2\mu\lambda i} + \zeta^{2\mu\lambda i}$ is a zero of $y_s(x)$. Hence,

$$0 \equiv y_s\big(M^\theta v_{2\theta}(\varrho_i)\big) = \sum_{j=0}^{s-1} Y_{j,s}(M^\theta V_{0,2\theta}, M^\theta V_{1,2\theta}, \ldots, M^\theta V_{s-1,2\theta})\, \varrho_i^j \pmod{p}.$$

Since $p \nmid \Delta$, the corollary follows.

COROLLARY 9.1.2. *If $(p, q\Delta E) = 1$, $p \mid A_n$ and $r \nmid n$, then $(p \mid q)_r = 1$.*

Proof. Let $\omega = \omega(p)$; then $\omega \mid n$ and $r \nmid \omega$. By the theorem $\omega \mid r\theta$; hence, $\omega \mid \theta$. If $(p \mid q)_r \neq 1$, $p \nmid A_\theta$; thus, $(p \mid q)_r = 1$.

COROLLARY 9.1.3. *If $(p, q\Delta E) = 1$, $p \mid C_n$ and $r \nmid n$, then $(p \mid q)_r = 1$.*

Proof. If $p \mid C_n$, let τ be an order of apparition of p such that $\tau \mid n$. Since $\tau \mid 2\omega$, $2\omega \mid 2r\theta$, and $r \nmid \tau$, we have $\tau \mid 2\theta$. Since $p \nmid C_{2\theta}$ if $(p \mid q)_r \neq 1$, we must have $(p \mid q)_r = 1$.

If, for $k = 2$, we put $T_n = 2V_{0,n} + P_1 V_{1,n}$, we see that

$$C_{2n} = V_{1,2n} = V_{1,n} T_n.$$

It is also possible to show that $T_n \mid T_{(2m+1)n}$. For $k = 2$, $r = 5$, $P_1 = P(1, q, r)$, $P_2 = P(2, q, r)$, $Q = q^3$, the T_n function is the same as the function V_n considered by Lehmer and Lehmer [10]. In [10] they showed that if $p \mid V_n$, $5 \nmid n$ and $p \neq q$, then $(p|q)_5 = 1$, this result is somewhat more general than the result that we are able to deduce from Corollary 9.1.3.

We close with two theorems on primes of the form $2A5^n - 1$ and $2A7^n - 1$. These theorems are extensions of a result of Williams [14].

THEOREM 9.3. *If $N = 2A5^n - 1$ $(A < 5^{n/2})$ and q is a prime such that $q \equiv 1 \pmod 5$ and $(N|q)_5 \neq 1$, put $P_1 = P(1, q, 5)$, $P_2 = P_2(2, q, 5)$, $Q = q^3$. If $(N, q\Delta EP_2) = 1$, $MQ \equiv 1 \pmod N$, and N is not a perfect square, then N is a prime if and only if*

$$P_2^4 W_{0,2\theta}^2 - P_2^5 W_{1,2\theta}^2 + P_2^2 W_{0,2\theta} - 1$$
$$\equiv 2P_2^2 W_{0,2\theta} W_{1,2\theta} + P_1 P_2^2 W_{1,2\theta}^2 + W_{1,2\theta} \equiv 0 \pmod N,$$

where $\theta = (N+1)/5$.

Proof. Follows easily from Corollary 9.1.1, Lemma 8.2, Theorem 8.3, and Lemma 8.3.

We give a modified form of this result in the following example. If $N = 2 \cdot 5^n - 1$, N can not be a perfect square if $n \geqslant 3$. For these N values, we find a prime q such that $q \equiv 1 \pmod 5$ and $N^{(q-1)/5} \not\equiv 1 \pmod q$. Let $2q^3 M \equiv 1 \pmod N$ and put $5d^2 = P_1^2 - 4P_2$,

$$S_1 \equiv MdP(1, q, 5), \quad T_1 \equiv M\big(P_1(1, q, 5)^2 - 2P(2, q, 5)\big) - 2 \pmod N.$$

If

$$\left.\begin{aligned} T_{r+1} &\equiv T_r(T_r^4 + 50T_r^2 S_r^2 + 125 S_r^4 - 5T_r^2 - 75 S_r^2 + 5) \\ S_{r+1} &\equiv S_r(5T_r^4 + 50T_r^2 S_r^2 + 25 S_r^4 - 15 T_r^2 - 25 S_r^2 + 5) \end{aligned}\right\} \pmod N,$$

then N is a prime if and only if

$$4T_n^2 \equiv 4S_n^2 \equiv 1 \pmod N.$$

THEOREM 9.4. *If $N = 2A7^n - 1$ $(2A < 7^{n/2})$ and q is a prime such that*

$$q \equiv 1 \pmod 7 \quad \text{and} \quad (N|q)_7 \neq 1,$$

put $P_1 = P(1, q, 7)$, $P_2 = P(2, q, 7)$, $P_3 = P(3, q, 7)$, $Q = q^5$. If $(N, q\Delta EP_3) = 1$ and $MQ \equiv 1 \pmod N$, then N is a prime if and only if

$$Y_{i,3}(P_3^2 W_{0,2\theta}, P_3^2 W_{1,2\theta}, P_3^2 W_{2,2\theta}) \equiv 0 \pmod N \quad (i = 0, 1, 2),$$

where $\theta = (N+1)/7$.

Bibliography

[1] E. T. Bell, *Notes on recurring series of the third order*, Tôhoku Math. Journ. 24 (1924), pp. 168–184.

[2] R. D. Carmichael, *On the numerical factors of the arithmetic forms $\alpha^n \pm \beta^n$*, Ann. of Math. (2), 15 (1913–14), pp. 30–70.

[3] — *A simple principle of unification in the elementary theory of numbers*, Amer. Math. Monthly 36 (1929), pp. 132–143.

[4] L. E. Dickson, *Cyclotomy, higher congruences, and Waring's problem*, Amer. Journ. Math. 57 (1935), pp. 391–424.

[5] H. T. Engstrom, *On sequences defined by linear recurrence relations*, Trans. Amer. Math. Soc. 33 (1931), pp. 210–218.

[6] E. Landau, *Vorlesungen über Zahlentheorie*, Vol. III, New York 1947.

[7] D. H. Lehmer, *An extended theory of Lucas' functions*, Ann. of Math. (2), 31 (1930), pp. 419–448.

[8] — *Factorization of certain cyclotomic functions*, ibid. (2), 34 (1933), pp. 461–479.

[9] — *Computer technology applied to the theory of numbers*, MAA Studies in Mathematics, Vol. 6 (1969), pp. 117–151.

[10] D. H. Lehmer and Emma Lehmer, *Cyclotomy of hyper-Kloosterman sums*, Acta Arith. 14 (1968), pp. 89–111.

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

[12] T. A. Pierce, *The numerical factors of the arithmetic forms $\Pi(1 \pm \alpha_i^m)$*, Ann. of Math. (2), 18 (1916), pp. 53–64.

[13] H. C. Williams, *On a generalization of the Lucas functions*, Acta. Arith. 20 (1972), pp. 33–52.

[14] — *The primality of $2A3^n - 1$*, Canad. Math. Bull. 15 (1972), pp. 585–589.

UNIVERSITY OF MANITOBA

Received on 29. 3. 1974 (550)