PROPERTIES OF SOME FUNCTIONS SIMILAR TO LUCAS FUNCTIONS

H. C. WILLIAMS
Department of Computer Science, University of Manitoba, Winnipeg, Manitoba, Canada R3T2N2

1. INTRODUCTION

The ordinary Lucas functions are defined by

(1.1) $$v_n = \alpha_1^n + \alpha_2^n, \qquad u_n = (\alpha_1^n - \alpha_2^n)/(\alpha_1 - \alpha_2),$$

where α_1, α_2 are the roots of

$$x^2 = Px - Q,$$

$\Delta = (\alpha_1 - \alpha_2)^2 = P^2 - 4Q$, and P,Q are coprime integers. These functions and their remarkable properties have been discussed by many authors. The best known works are those of Lucas [7] and Carmichael [3]. Lehmer [6] has dealt with a more general form of these functions for which $P = \sqrt{R}$ and R,Q are coprime integers.

Bell [1] attributed the existence of the many properties of the Lucas functions to the simplicity of the functions' form. He added, "this simplicity vanishes, apparently irrevocably, when we pass beyond second order series." The purpose of this paper is to define a set of third order functions W_n, V_n, U_n, and to show that these functions possess much of the "arithmetic fertility" of the Lucas functions.

Consider first the functions v_n and u_n, which are defined in the following manner. We let ρ_1, ρ_2 be the roots of

$$x^2 = rx + s$$

and

$$2\alpha_1 = v_1 + u_1\rho_1, \qquad 2\alpha_2 = v_1 + u_1\rho_2,$$

where s, r, v_1, u_1 are given integers. We then put

$$v_n = \frac{2}{\delta}\begin{vmatrix} \alpha_1^n & \rho_1 \\ \alpha_2^n & \rho_2 \end{vmatrix}, \qquad u_n = \frac{2}{\delta}\begin{vmatrix} 1 & \alpha_1^n \\ 1 & \alpha_2^n \end{vmatrix},$$

where

$$\delta = \begin{vmatrix} 1 & \rho_1 \\ 1 & \rho_2 \end{vmatrix}.$$

If we select values for s, r, v_1, u_1 such that v_n, u_n are both integers for all non-negative integer values of n, then $P = \alpha_1 + \alpha_2$ and $Q = \alpha_1\alpha_2$ will be integers. If we further restrict our choices of values for r, s, v_1, u_1 such that $(P,Q) = 1$, then it can be easily shown that the resulting functions v_n and u_n have many properties analogous to those of the ordinary Lucas functions. Indeed, if we select $s = \Delta$, $r = 0$, $v_1 = P$, $u_1 = 1$, the functions u_n and v_n are the functions given by (1.1).

In this paper we shall be concerned with the third order analogues of the above functions. We let ρ_1, ρ_2, ρ_3 be the roots of

$$x^3 = rx^2 + sx + t \quad \text{and} \quad 3\alpha_i = W_1 + V_1\rho_i + U_1\rho_i^2 \quad (i = 1, 2, 3),$$

where r, s, t, W_1, V_1, U_1 are given integers. We define

(1.3) $$W_n = \frac{3}{\delta}\begin{vmatrix} \alpha_1^n & \rho_1 & \rho_1^2 \\ \alpha_2^n & \rho_2 & \rho_2^2 \\ \alpha_3^n & \rho_3 & \rho_3^2 \end{vmatrix}, \quad V_n = \frac{3}{\delta}\begin{vmatrix} 1 & \alpha_1^n & \rho_1^2 \\ 1 & \alpha_2^n & \rho_2^2 \\ 1 & \alpha_3^n & \rho_3^2 \end{vmatrix}, \quad U_n = \frac{3}{\delta}\begin{vmatrix} 1 & \rho_1 & \alpha_1^n \\ 1 & \rho_2 & \alpha_2^n \\ 1 & \rho_2 & \alpha_3^n \end{vmatrix},$$

where

$$\delta = \begin{vmatrix} 1 & \rho_1 & \rho_1^2 \\ 1 & \rho_2 & \rho_2^2 \\ 1 & \rho_3 & \rho_3^2 \end{vmatrix} \neq 0.$$

We also put $P = a_1 + a_2 + a_3$, $Q = a_1a_2 + a_2a_3 + a_3a_1$, $R = a_1a_2a_3$, $\Delta = \delta^2$.

Let N be the set of positive integers. If we restrict the values of r, s, t, W_1, V_1, U_1 such that

(1) W_n, V_n, U_n are all integers for any $n \in N$,

(2) P, Q, R are integers and $(P,Q,R) = 1$,

(3) there exists $\mu \in N$ such that $U_i \equiv U_{i+k\mu}$ (mod 3) for all $i, k \in N$,

the functions W_n, V_n, U_n have several characteristics similar to those of the Lucas functions. Functions similar to W_n, V_n, U_n have been discussed by Williams [10] and [11, ($q = 3$)], but for these functions $r = s = 0$, $\Delta = t$.

Conditions (1) and (2) are analogous to the two restrictions placed on the functions of (1.2). These two restrictions guarantee that there exists an integer $m \in N$ such that $u_i \equiv u_{i+km}$ (mod 2) for any $i,k \in N$; however, we shall see that conditions (1) and (2) do not imply (3).

It is necessary to demonstrate what the conditions on r, s, t, W_1, V_1, U_1 are such that (1), (2), (3) are true. In order to do this, we require several identities satisfied by W_n, V_n and U_n. These identities, which are independent of (1), (2), (3), are given in Section 2.

2. IDENTITIES

It is not difficult to see from (1.3) that

$$3^{n-1}(W_n + \rho V_n + \rho^2 U_n) = (W_1 + \rho V_1 + \rho^2 U_1)^n, \tag{2.1}$$

where $\rho = \rho_1, \rho_2, \rho_3$. It follows that

$$\begin{aligned} 3W_{n+m} &= W_nW_m + tV_nU_m + tU_nV_m + trU_mU_n, \\ 3V_{n+m} &= V_nW_m + W_nV_m + sV_mU_n + sV_nU_m + (rs+t)U_nU_m. \\ 3U_{n+m} &= W_mU_n + W_nU_m + V_nV_m + rU_mV_n + rU_nV_m + (r^2+s)U_nU_m, \end{aligned} \tag{2.2}$$

$$\begin{aligned} 3W_{2m} &= W_m^2 + 2tV_mU_m + trU_m^2, \\ 3V_{2m} &= (sr+t)U_m^2 + 2sV_mU_m + 2V_mU_m, \\ 3U_{2m} &= V_m^2 + 2W_mU_n + 2rU_mV_m + (r^2+s)U_m^2, \end{aligned} \tag{2.3}$$

$$\begin{aligned} 9W_{3m} &= W_m^3 + tV_m^3 + t(r^2+2rs+t)U_m^3 + 6tW_mV_mU_m \\ &\quad + 3trW_mU_m^2 + 3trU_mV_m^2 + 3t(r^2+s)U_m^2V_m \\ 9V_{3m} &= sV_m^3 + (sr+t)(r^2+2s)U_m^3 + 6sW_mV_mU_m + 3V_mW_m^2 \\ &\quad + 3(sr+t)W_mU_m^2 + 3(t+rs)U_mV_m^2 + 3(s^2+sr^2+t)U_m^2V_m \\ 9U_{3m} &= rV_m^3 + (r^4+3r^2s+s^2+2tr)U_m^3 + 6rW_mV_mU_m + 3U_mW_m^2 \\ &\quad + 3W_mV_m^2 + 3(r^2+s)W_mU_m^2 + 3(r^2+2rs+t)U_m^2V_m, \end{aligned} \tag{2.4}$$

$$\begin{aligned} 3R^mW_{-m} &= W_m^2 + rW_mV_m + (r^2+2s)W_mU_m - sV_m^2 - (rs+t)U_mV_m + (s^2-rt)U_m^2, \\ 3R^mV_{-m} &= -W_mV_m - rV_m^2 - r^2U_mV_m + (rs+t)U_m^2, \\ 3R^mU_{-m} &= -W_mU_m + V_m^2 + rU_mV_m - sU_m^2. \end{aligned} \tag{2.5}$$

By using methods similar to those of Williams [12], we can show that

$$9R^mW_{n-m} = \begin{vmatrix} W_n & tU_m & tV_m + rtU_m \\ V_n & W_m + sU_m & sV_m + (rs+t)U_m \\ U_n & V_m + rU_m & W_m + rV_m + (r^2+s)U_m \end{vmatrix},$$

(2.6)
$$9R^mV_{n-m} = \begin{vmatrix} W_m & W_n & tV_m + rtU_m \\ V_m & V_n & sV_m + (rs+t)U_m \\ U_m & U_n & W_m + rV_m + (r^2+s)U_m \end{vmatrix},$$

$$9R^mU_{n-m} = \begin{vmatrix} W_m & tU_m & W_n \\ V_m & W_m + sU_m & V_n \\ U_m & V_n + rU_m & U_n \end{vmatrix},$$

(2.7)
$$27R^m = \begin{vmatrix} W_m & tU_m & tV_m + rtU_m \\ V_m & W_m + sU_m & sV_m + (rs+t)U_m \\ U_m & V_m + rU_m & W_m + rV_m + (r^2+s)U_m \end{vmatrix},$$

(2.8)
$$\begin{vmatrix} W_n & V_n & U_n \\ W_{n+m} & V_{n+m} & U_{n+m} \\ W_{n+2m} & V_{n+2m} & U_{n+2m} \end{vmatrix} = R^nN_m,$$

(2.9)
$$27\begin{vmatrix} W_n & W_{n+m} & W_{n+2m} \\ W_{n+m} & W_{n+2m} & W_{n+3m} \\ W_{n+2m} & W_{n+3m} & W_{n+4m} \end{vmatrix} = -R^nt^2N_m^2,$$

$$27\begin{vmatrix} V_n & V_{n+m} & V_{n+2m} \\ V_{n+m} & V_{n+2m} & V_{n+3m} \\ V_{n+2m} & V_{n+3m} & V_{n+4m} \end{vmatrix} = -R^n(rs+t)N_m^2,$$

$$27\begin{vmatrix} U_n & U_{n+m} & U_{n+2m} \\ U_{n+m} & U_{n+2m} & U_{n+3m} \\ U_{n+2m} & U_{n+3m} & U_{n+4m} \end{vmatrix} = -R^nN_m^2,$$

where

$$N_m = 3\begin{vmatrix} V_m & U_m \\ V_{2m} & U_{2m} \end{vmatrix} = (V_m + rU_m)^3 - rU_m(V_m + rU_m)^2 - sU_m^2(V_m + rU_m) - tU_m^3 .$$

Let

$$P_m = \alpha_1^m + \alpha_2^m + \alpha_3^m, \quad Q_m = \alpha_1^m\alpha_2^m + \alpha_2^m\alpha_3^m + \alpha_3^m\alpha_1^m, \quad R_m = \alpha_1^m\alpha_2^m\alpha_3^m = R^m .$$

From (2.1) and (2.7), we have

(2.10)
$$3P_m = 3W_m + rV_m + (r^2+2s)U_m,$$

(2.11)
$$9Q_m = 3W_m^2 + 2rV_mU_m + (2r^2+4s)U_mW_m - sV_m^2 - (sr+3t)U_mV_m + (s^2-2tr)U_m^2$$

(2.7)
$$27R_m = W_m^3 + tV_m^3 + t^2U_m^3 - (3t+rs)W_mV_mU_m + rW_m^2V_m - sV_m^2W_m$$
$$+ (2s+r^2)W_m^2U_m + (s^2-2rt)W_mU_m^2 + trV_m^2U_m - tsV_mU_m^2 .$$

If

$$\epsilon_m = \begin{vmatrix} 1 & a_1^m & a_1^{2m} \\ 1 & a_2^m & a_2^{2m} \\ 1 & a_3^m & a_3^{2m} \end{vmatrix}$$

and $E_m = \epsilon_m^2$, then

(2.14) $$27\epsilon_m = -27R^{2m}\epsilon_{-m} = \delta N_m$$

and

(2.15) $$3^6 E_m = \Delta N_m^2 .$$

It should be noted that

(2.16) $$E_m = P_m^2 Q_m^2 + 18P_m Q_m R_m - 4Q_m^3 - 4P_m^3 R_m - 27R_m^2$$

and

$$\Delta = r^2 s^2 - 18rst + 4s^3 - 4r^3 t - 27t^2 .$$

If

$$F(x,y) = x^3 - rx^2 y - sxy^2 - ty^3 ,$$

we see from (2.14) and (2.5), that

$$R^m F(V_m + rU_m, U_m) = F\{(tU_m^2 - rW_m U_m - W_m V_m)/3, (-W_m U_m + V_m^2 + rU_m V_m - sU_m^2)/3\}.$$

If W_1, V_1, U_1 are selected such that $W_1 = 3a$, $V_1 = 3b$, $U_1 = 3c$, where a, b, c are integers and $a + \rho_1 b + \rho_1^2 c$ is a unit of the cubic field generated by adjoining ρ_1 to the rationals, we can obtain an infinitude of integer solutions of the Diophantine equation

$$F(x,y) = F(z,w).$$

If we define

$$Z_n = \frac{1}{\delta}\begin{vmatrix} 1 & \rho_1 & \rho_1^n \\ 1 & \rho_2 & \rho_2^n \\ 1 & \rho_3 & \rho_3^n \end{vmatrix},$$

then (Bell [1])

$$\rho^n = (Z_{n+2} - rZ_{n+1} - sZ_n) + (Z_{n+1} - rZ_n)\rho + Z_n \rho^2 ,$$

where $\rho = \rho_1, \rho_2, \rho_3$. Using this result together with (2.1), we obtain

(2.17) $$3^{m-1} W_{nm} = \sum_{i,j} \frac{m!}{i!\,j!\,(m-i-j)!} (Z_{2j+i+2} - rZ_{2j+i+1} - sZ_{2j+1}) W_n^{m-i-j} V_n^i U_n^j ,$$

$$3^{m-1} V_{nm} = \sum_{i,j} \frac{m!}{i!\,j!\,(m-i-j)!} (Z_{2j+i+1} - rZ_{2j+1}) W_n^{m-i-j} V_n^i U_n^j ,$$

$$3^{m-1} U_{nm} = \sum_{i,j} \frac{m!}{i!\,j!\,(m-i-j)!} Z_{2j+i} W_n^{m-i-j} V_n^i U_n^j ,$$

where the sum is taken over integers $i, j \geqslant 0$ such that $0 \leqslant i + j \leqslant m$.

Finally, it should be noted that for a fixed value of n, each of $W_{n+km}, V_{n+km}, U_{n+km}$ can be represented as a linear combination of the k^{th} powers of the roots of the equation

$$x^3 = P_m x^2 - Q_m x + R_m ;$$

consequently, we have

(2.18)
$$W_{n+(k+3)m} = P_m W_{n+(k+2)m} - Q_m W_{n+(k+1)m} + R_m W_{n+km},$$
$$V_{n+(k+3)m} = P_m V_{n+(k+2)m} - Q_m V_{n+(k+1)m} + R_m V_{n+km},$$
$$U_{n+(k+3)m} = P_m U_{n+(k+2)m} - Q_m U_{n+(k+1)m} + R_m U_{n+km}.$$

The identities (2.1), (2.2), (2.6), (2.7), (2.9), (2.17), (2.18) are analogous to Lucas' important identities (7), (49), (51), (46), (32) and (33), (49), and (13), respectively.

3. PRELIMINARY RESULTS

We will now show how to obtain values for r, s, t, W_1, V_1, U_1 in such a way that W_n, V_n, U_n are integers for any $n \in N$. We require two lemmas.

Lemma 1. If W_n, V_n, U_n are integers for all $n \in N$, then P, Q, R are integers and one of the following is true.

(i) $3 \mid (W_1, V_1, U_1)$†

(ii) $3 \mid W_1, 3 \nmid U_1, V_1 \equiv -rU_1 \pmod 3, 3 \mid t$, and $3 \mid s$

(iii) $3 \mid W_1, 3 \nmid U_1, V_1 \equiv rU_1 \pmod 3, 3 \mid t$ and $r^2 + s \equiv 0 \pmod 3$

(iv) $3 \nmid W_1, 3 \mid V_1, 3 \nmid U_1, W_1 \equiv -U_1 \pmod 3, s \equiv 1 \pmod 3$, and $t \equiv -r \pmod 3$

(v) $3 \nmid W_1 V_1 U_1, W_1 \equiv U_1 \pmod 3, V_1 \equiv tU_1 \pmod 3, 3 \mid s, 3 \mid r$, and $3 \nmid t$

Proof. Since W_2, V_2, U_2 are integers, it follows from (2.3) that one of the cases (i), (ii), (iii), (iv) or (v) must be true. In each of these cases, we see that
$$rV_1 + (r^2 + 2s)U_1 \equiv 0 \pmod 3;$$
hence, P is an integer.

Now, from (2.18) and the fact that $V_0 = U_0 = 0$, we have
$$V_3 = PV_2 - QV_1,$$
$$U_3 = PU_2 - QU_1;$$
thus, QV_1 and QU_1 are both integers. Since $9Q$ is an integer, we see that Q is an integer if $3 \nmid V_1$ or $3 \nmid U_1$. If $3 \mid (V_1, U_1)$, then it is clear from (2.11) that Q is an integer. Using the equations
$$V_4 = PV_3 - QV_2 + RV_1, \qquad U_4 = PU_3 - QU_2 + RU_1$$
and (2.7), we can show that R must also be an integer.

Lemma 2. If the conditions of (i) of Lemma 1 are true, Q and R are integers.
If the conditions of (ii) hold, Q and R are integers if and only if $9 \mid t$.
If the conditions of (iii) hold, Q and R are integers if and only if $t \equiv r(s - 2r^2) \pmod 9$.
If the conditions of (iv) hold, Q and R are integers if and only if $s \equiv 1 - tr - r^2 \pmod 9$.
If the conditions of (v) hold, Q and R are integers if and only if $s \equiv t^2 - 1 - tr \pmod 9$.

Proof. The proof of the first statement of the lemma is clear from Eqs. (2.11) and (2.7). We show how the other statements can be proved by demonstrating the truth of the fourth statement. (The proofs of the others are similar.)

We write
$$W_1 = -U_1 + 3L, \quad V_1 = 3K,$$
where L, K are integers. Substituting these values for W_1 and V_1 in (2.11), we get
$$9Q \equiv 2U_1^2[1 - s - tr - r^2] \pmod 9.$$
Hence, Q is an integer if and only if
$$s \equiv 1 - tr - r^2 \pmod 9.$$

†If $x,y,z,\cdots$ are rational integers, we write as usual $x \mid y$ for x divides y, $x \nmid y$ for x does not divide y, and $(x,y,z,\cdots)$ for the greatest common divisor of $x,y,z,\cdots$. We also write $y^n \| x$ to indicate that $y^n \mid x$ and $y^{n+1} \nmid x$.

Assuming that Q is an integer and repeating the above method using (2.7), we get

$$27R \equiv [-1+t^2+2s+r^2-s^2+2rt]U_1^3 \pmod{27}.$$

Thus,

$$3R \equiv ((t+r)/3-(s-1)/3)((t+r)/3+(s-1)/3)U_1^3 \pmod 3.$$

Since $(s-1)/3 \equiv r(t+r)/3$ and $3 \nmid r$, we see that R is an integer if Q is.

The answer to the problem of this section is given as

Theorem 1. W_n, V_n, U_n are integers for any $n \in N$ if and only if one of the following is true.

(a) $3 \mid (W_1, V_1, U_1)$

(b) $3 \mid W_1, 3 \nmid U_1, V_1 \equiv -rU_1 \pmod 3, 3 \mid s, 9 \mid t$

(c) $3 \mid W_1, 3 \nmid U_1, V_1 \equiv rU_1 \pmod 3, 3 \nmid s, r^2+s \equiv 0 \pmod 3, t \equiv r(s-2r^2) \pmod 9$

(d) $3 \nmid W_1, 3 \mid V_1, 3 \nmid U_1, W_1 \equiv U_1 \pmod 3, s \equiv 1 \pmod 3, t \equiv -r \pmod 3, s \equiv 1-tr-r^2 \pmod 9$

(e) $3 \nmid W_1V_1U_1, W_1 \equiv U_1 \pmod 3, V_1 \equiv tU_1 \pmod 3, 3 \mid s, 3 \mid r, 3 \nmid t, s \equiv t^2-1-tr \pmod 9$.

Proof. By Lemmas 1 and 2, one of the above conditions is necessary in order for W_n, V_n, U_n to be integers for any $n \in N$. To show sufficiency of the conditions, we note that in each case W_2, V_2, U_2, P, Q, R are integers. The fact that W_n, V_n, U_n are integers for any $n \in N$ follows by induction on (2.18).

Corollary. Let $n \in N$.

If the conditions of (a) are true,

$$W_n \equiv V_n \equiv U_n \equiv 0 \pmod 3.$$

If the conditions of (b) hold,

$$W_n \equiv 0, \quad V_n \equiv -rU_n \pmod 3.$$

If the conditions of (c) hold,

$$W_n \equiv 0, \quad V_n \equiv rU_n \pmod 3.$$

If the conditions of (d) hold,

$$W_n \equiv -U_n, \quad V_n \equiv 0 \pmod 3.$$

If the conditions of (e) hold,

$$W_n \equiv U_n, \quad V_n \equiv tU_n \pmod 3.$$

Proof. These results are easily verified for $n = 2$. The results for general $n \in N$ follow by using induction on (2.18).

For the sake of brevity, we shall say that the functions W_n, V_n, U_n are given by (a), (b), (c), (d), or (e) if W_1, V_1, U_1, r, s, t obey the conditions of the cases (a), (b), (c), (d), or (e) above. From this point on, we consider only those functions W_n, V_n, U_n which are given by one of these cases.

4. CONGRUENCE PROPERTIES MODULO 3

Since $3 \mid (W_n, V_n, U_n)$ for W_n, V_n, U_n given by (a), we will confine ourselves here to an investigation of the congruence properties (mod 3) of W_n, V_n, U_n when they are given by (b), (c), (d) or (e). In each of these cases, $9 \mid \Delta$ and we let $H = \Delta/9$. From the corollary to Theorem 1, we see that it is sufficient to discuss U_n only.

We define μ to be the least positive integer such that

$$U_i \equiv U_{i+k\mu} \pmod 3$$

for all $i, k \in N$. We further define

$$B = \{X_1, X_2, \cdots, X_\mu\},$$

where $U_i \equiv U_1X_i \pmod 3$.

Lemma 3. For W_n, V_n, U_n given by (b), (c), (d) or (e), μ and B are determined from the following results.

Case (i) $3 \nmid Pr$. The values of μ, R (mod 3), B are functions of the values of H and Q (mod 3). These values (mod 3) are given in Table 1.

Table 1

H	Q	μ	R	B
1	$0, 1$	2	0	$\{1, (Q+1)P\}$
1	-1	2	P	$\{1, 0\}$
-1	1	4	P	$\{1, 0, -1, 0\}$
-1	$0, -1$	$4, 8$	$P(1+Q)$	$\{1, (Q-1)P, -1, 0, -1, -(Q-1)P, 1, 0\}$
0	P	6	$P-1$	$\{1, 1, 0, -1, -1, 0\}$
0	$-P$	3	$P+1$	$\{1, -1, 0\}$

Case (ii). $3 \nmid P,\ 3 \mid r$

In this case, $\mu = 2$, $R \equiv PQ(Q-1) \pmod 3$, and $B = \{1, P+PQ\}$.

Case (iii). $3 \mid P$

In this case, $Q \equiv -H \pmod 3$ and the value of R is independent of Q and H. The values of μ and B are given in Table 2.

Table 2

H	Q	R	μ	B
0	0	$-F$	6	$\{1, F, 0, F, -1, 0\}$
-1	1	$F \equiv 0$	4	$\{1, 0, -1, 0\}$
-1	1	$F \not\equiv 0$	8	$\{1, F, -1, 0, -1, -F, 1, 0\}$
1	-1	0	2	$\{1, F\}$

Here

$$F = (-W_1 + sU_1)/3 \quad \text{for } W_n, V_n, U_n \text{ given by (b),}$$
$$F = (-W_1 + rV_1 + (tr - 3 - r^2)U_1)/3 \quad \text{for } W_n, V_n, U_n \text{ given by (c),}$$
$$F = (-W_1 + rV_1 - sU_1)/3 \quad \text{for } W_n, V_n, U_n \text{ given by (d),}$$

and

$$F = (-W_1 - tV_1 + (s+2)U_1)/3 \quad \text{for } W_n, V_n, U_n \text{ given by (e).}$$

Proof. For W_n, V_n, U_n given by (b), put

$$W_1 = 3L,\quad V_1 = -rU_1 + 3K,\quad a = s/3,\quad b = rt/9,\quad A_1 = L + rK + aU_1,\ A_2 = L,\quad A_3 = L + aU_1.$$

Then it can be shown by substitution into (2.10), (2.11), (2.7), that

$$P \equiv A_1 + A_2 + A_3,\quad Q \equiv A_1A_2 + A_2A_3 + A_3A_1 + b,\qquad R \equiv A_1A_2A_3 + bA_1,$$
$$A_2A_3 \equiv (A_2+A_3)^2 - (A_2-A_3)^2 \equiv (A_2+A_3)^2 - a^2 \pmod 3.$$

Also, if $3 \nmid r$, $H \equiv a^2 - b \pmod 3$ and if $3 \mid r$, $H \equiv 0 \pmod 3$. Hence, if $3 \nmid r$,

$$Q \equiv P(A_2+A_3) - H \pmod 3$$
$$R \equiv \begin{cases} P(Q-H)(Q+H-1) \pmod 3 & \text{when } 3 \nmid P \\ (A_2+A_3)(H-1) \pmod 3 & \text{when } 3 \mid P, \end{cases}$$
$$U_2 \equiv U_1(A_2+A_3) \equiv U_1(PQ+PH) \quad \text{when } 3 \nmid P.$$

If $3 \mid r$,

$$P \equiv 2aU_1 \pmod 3$$
$$Q \equiv P(A_2+A_3) - a^2 \pmod 3$$
$$R \equiv \begin{cases} PQ(Q-1) \pmod 3 & \text{when } 3 \nmid P \\ -(A_2+A_3) \pmod 3 & \text{when } 3 \mid P \end{cases}$$
$$U_2 \equiv (A_2+A_3)U_1 \equiv P(Q+1)U_1 \quad \text{when } 3 \nmid P.$$

The proof of the lemma for W_n, V_n, U_n given by (b) follows by using induction on (2.18).

For (c), put

$$W_1 = 3L,\quad V_1 = rU_1 + 3K,\quad a = rt/3 - 1,\quad b = r(t - r(s - 2r^2))/9,\quad A_1 = L + (a+1)U_1,$$
$$A_2 = L - rK,\quad A_3 = L + 2rK + aU_1 .$$

Then

$$H \equiv a^2 - b,\quad P \equiv A_1 + A_2 + A_3,\quad Q \equiv A_1A_2 + A_2A_3 + A_3A_1 + b,$$
$$R \equiv A_1A_2A_3 + bA_1,\quad (A_2 - A_3)^2 \equiv a^2,\quad A_2A_3 \equiv (A_2 + A_3)^2 - a^2 \pmod 3 .$$

For (d), put

$$W_1 = U_1 + 3L,\quad V_1 = 3K,\quad a = rK,\quad b = r(t + sr)/9,\quad A_1 = L + rK + U_1(r^2 - 1)/3,$$
$$A_2 = L + \sqrt{s}\,K + U_1(s - 1)/3,\quad A_3 = L - \sqrt{s}\,K + U_1(s - 1)/3.$$

Then

$$H \equiv (a - P)^2 - b,\quad P \equiv A_1 + A_2 + A_3,\quad Q \equiv A_1A_2 + A_1A_3 + A_2A_3 + b,$$
$$R \equiv A_1A_2A_3 - b(a + A_2 + A_3),\quad (A_2 - A_3)^2 \equiv a^2,\quad A_2A_3 \equiv (A_2 + A_3)^2 - a^2 \pmod 3.$$

For (e), put

$$V_1 = tU_1 + 3K,\quad W_1 = U_1 + 3L,\quad A_1 = L + tK + U_1(1 + 2t^2)/3,$$
$$A_2 = L + \beta_1K + \beta_1U_1r/3,\quad C = L + \beta_2K + \beta_2U_1r/3,$$

where β_1, β_2 are the zeros of $x^2 + (t - r)x + 1$. Then $H \equiv 0,\ P \equiv A_1 + A_2 + A_3$.

$$Q \equiv A_1A_2 + A_3A_1 + A_2A_3,\quad R \equiv A_1A_2A_3,\quad (A_2 - A_3)^2 \equiv 0,\quad A_2A_3 \equiv (A_2 + A_3)^2 \pmod 3.$$

The remainder of the proof of this lemma for W_n, V_n, U_n given by (c), (d), or (e) can now be obtained in the same way as that for W_n, V_n, U_n given by (b).

Corollary. If $n \in N$, $3 \mid U_n$ if and only if $\psi \mid n$, where ψ is the least positive integer value for m such that $3 \mid U_m$. From the statement of Lemma 3, it is clear that $\psi = \mu$, $\mu/2$ or no value for ψ exists.

In the statement of Lemma 3, we have neglected the case for which $3 \nmid Pr$, $3 \mid Q$ and $3 \mid H$. In this case, it can be shown that μ does not exist. By the definition of W_n, V_n, U_n, we exclude this case; hence, we may not have values of r, s, t, W_1, V_1, U_1 such that $3 \nmid Pr$, $3 \mid F$, $27 \mid \Delta$ for W_n, V_n, U_n given by (b) or (c) or values of r, s, t, W_1, V_1, U_1 such that $3 \nmid P$, $3 \mid (F + P)$, $27 \mid \Delta$ for W_n, V_n, U_n given by (d).

We have now found the conditions on r, s, t, W_1, V_1, U_1 in order that the functions W_n, V_n, U_n satisfy the requirements (1) and (3) of Section 1. We give the conditions for $(P,Q,R) = 1$ ((2) of Section 1) in Section **5**.

5. FURTHER RESTRICTIONS ON r, s, t, W_1, V_1, U_1

It is not immediately clear how to select r, s, t, W_1, V_1, U_1 In order that $(P,Q,R) = 1$. We show how such selections may be made in

Theorem 2. Let $3G = (2r^2 + 6s)V_1 + (2r^3 + 7rs + 9t)U_1$.

1. If W_n, V_n, U_n are given by (a), $(P,Q,R) = 1$ if and only if $(W_1, V_1, U_1) = 3$ and $(P,G,\Delta) = 2^\alpha 3^\beta$, where $\alpha > 0$ only if $2 \nmid (s + r)(V_1 + U_1)$ and $\beta > 0$ only if none of the following is true.
   (i) $3 \mid r$ and $W_1 + tV_1 + t^2U_1 \equiv 0 \pmod 9$
   (ii) $3 \nmid r$, $s \equiv 1 \pmod 3$, and $W_1 + tU_1 \equiv 0 \pmod 9$
   (iii) $3 \nmid r$, $3 \mid s$, and $W_1(W_1 + rV_1 + U_1) \equiv 0 \pmod{27}$
   (iv) $3 \nmid r$, $s \equiv -1 \pmod 3$, and $9 \mid W_1$.
2. If W_n, V_n, U_n are given by (b), (c), (d), or (e), then $(P,Q,R) = 1$ if and only if $(W_1, V_1, U_1) = 1$ and $(P,G,H) = 2^\alpha 3^\gamma$, where $\alpha > 0$ only if $2 \nmid (s + r)(V_1 + U_1)$ and $\gamma > 0$ only if $3 \nmid F$.

Proof. We first prove the necessity of the conditions of the theorem.

If p $(\neq 3)$ is a prime and $p \mid (W_1, V_1, U_1)$, then it is clear from (2.10), (2.11), and (2.7) that $p \mid (P,Q,R)$. If $9 \mid (W_1, V_1, U_1)$, then $3 \mid (P,Q,R)$. Hence, if $(P,Q,R) = 1$, $(W_1, V_1, U_1) \mid 3$.

Now, suppose that p $(\neq 3)$ is a prime divisor of (P,G,Δ). Since

$$3W_1 \equiv -rV_1 - (r^2+2s)U_1 \pmod p,$$

we have

$$-27Q \equiv (r^2+3s)V_1^2 + (2r^3+7rs+9t)U_1V_1 + (r^4+4sr^2+6tr+s^2)U_1^2 \pmod p.$$

Since

$$(5.1) \qquad -3\Delta = (2r^3+7rs+9t)^2 - 4(r^2+3s)(r^4+4sr^2+6tr+s^2),$$

we see that

$$27\cdot 4\cdot(r^2+3s)Q \equiv 9G^2 \pmod p.$$

If $p \nmid 2(r^2+3s)$, then $p \mid Q$. If $p \mid (r^2+3s)$, then, from (5.1), $p \mid (2r^3+7rs+9t)$. As a consequence of these two facts, we deduce that $p \mid (rs+9t)$ and $p \mid (3tr - s^2)$; thus, $p \mid (r^4+4sr^2+6tr+s^2)$ and $p \mid Q$. Combining (2.15) and (2.16), we get

$$27^2(P^2Q^2+18PQR-4Q^3-4P^3R-27R^2) = \Delta N_1^2\ ;$$

consequently, if $p \mid (Q,P,\Delta)$ and $p \neq 3$, then $p \mid R$. Thus, if $(P,Q,R)=1$, then $(P,G,\Delta) = 2^\alpha 3^\beta$, $((P,G,H) = 2^\alpha 3^\gamma)$. If $2 \mid (P,G,\Delta)$ and $(P,Q,R)=1$, then $2 \nmid Q$. Q is odd if and only if $(s+q)(V_1+U_1)$ is. If $3 \mid (P,G,\Delta)$ (or $3 \mid (P,G,H)$) and $(P,Q,R)=1$, then $3 \nmid (Q,R)$. We will show the conditions under which $3 \nmid (Q,R)$ for part 1 of the theorem only. The conditions for part 2 are quite easy to obtain from results used in the proof of Lemma 3.

Since $3 \mid P$ and $3 \mid \Delta$, we have

$$rV_1/3 \equiv -(r^2+2s)U_1/3 \pmod 3 \quad\text{and}\quad r^2s^2+s \equiv rt \pmod 3.$$

We now deal with four cases.

(i) $\underline{3 \mid r}$. If $3 \mid r$, then $3 \mid s$ and $3 \mid Q$. Hence $3 \nmid (Q,R)$ if and only if $3 \nmid (W_1/3 + tV_1/3 + t^2U_1/3\ .)$

(ii) $\underline{3 \nmid r,\ s \equiv 1 \pmod 3}$. Here we have $9 \mid V_1$ and $tr \equiv -1 \pmod 3$; thus, $s^2 - 2tr \equiv 0 \pmod 3$ and $3 \mid Q$. Hence, $3 \nmid (Q,R)$ if and only if $3 \nmid (W_1/3 + tU_1/3)$.

(iii) $\underline{3 \nmid r,\ 3 \mid s}$. We must have $3 \mid t$ and $3 \mid Q$. (R,Q) is not divisible by 3 if and only if $9 \nmid W_1(W_1/3 + rV_1/3 + U_1/3)$.

(iv) $\underline{3 \nmid r,\ s \equiv -1}$ (mod 3). Once more, we get $3 \mid t$. Also $U_1 \equiv -V_1$ (mod 9); hence $3 \mid Q$. $3 \nmid (R,Q)$ if and only if $\underline{3 \nmid W_1/3}$.

We now show the sufficiency of the conditions. Let p ($\neq 3$) be a prime such $p \mid (P, Q, R)$ and $p \nmid \Delta$. Put $T = V_1 + rU_1$. Since $p \mid E_1$ and $p \nmid \Delta$, we must have $p \mid N_1$ and

$$(5.2) \qquad T^3 - rT^2U_1 - sTU_1^2 - tU_1^3 \equiv 0 \pmod p.$$

Also

$$3W_1 \equiv -rT - 2sU_1 \pmod p \quad\text{and}\quad p \mid 27Q\ ;$$

hence,

$$(5.3) \qquad T^2(-r^2-3s) + U_1T(-sr-9t) + U_1^2(-s^2+3tr) \equiv 0 \pmod p.$$

If $p \mid U_1$, then $p \mid V_1$ and $p \mid W_1$. Suppose $p \nmid U_1$; then

$$\begin{vmatrix} -9t-rs & -3s-r^2 & 0 \\ -s & -r & 1 \\ 3rt-s^2 & -9t-rs & -3s-r^2 \end{vmatrix} TU_1^{-1} + \begin{vmatrix} -3rt-s^2 & -3s-r^2 & 0 \\ -t & -r & 1 \\ 0 & -9t-rs & -3s-r^2 \end{vmatrix} \equiv 0 \pmod p\,.$$

Evaluating the determinants, we have

$$-3\Delta TU_1^{-1} + r\Delta \equiv 0 \pmod p$$

and, consequently, $T \equiv 3^{-1}rU_1 \pmod p$. Putting this result into (5.2) and (5.3), we get $r^2+3s \equiv 0 \pmod p$ and $2r^3+9sr+27t \equiv 0 \pmod p$. By (5.1) $p \mid \Delta$, this is a contradiction; thus $p \mid (W_1, V_1, U_1)$.

If $3 \mid (P,Q,R)$ and $3 \nmid \Delta$, then W_n, V_n, U_n are given by (a) and we discuss two cases. If $3 \mid r$, then $3 \nmid s$ and from (2.10), we must have $9 \mid U_1$. Using these results in (2.11) and (2.7), we see that $9 \mid V_1$ and $9 \mid W_1$. If $3 \nmid r$, we obtain from (2.10) the fact that

$$V_1/3 \equiv -r(1+2s)U_1/3 \pmod 3.$$

Putting this result into (2.11), we deduce

$$(-s-s^2+tr)(U_1/3)^2 \equiv 0 \pmod 3.$$

Since $3 \nmid \Delta$, $3 | U_1/3$ and $3 | V_1/3$, from (2.7), we have $3 | W_1/3$.

If p ($\neq 3$) is a prime and $p | (P,Q,R,\Delta)$, then

$$4 \cdot 27(r^2+2s)Q \equiv 9G^2 \pmod p$$

and $p | G$. If $p = 2$, then $2 | (P,G,\Delta)$ and we have $2 | (s+r)(U_1+V_1)$.

If $3 | (P,Q,R,\Delta)$ and W_n, V_n, U_n are given by (a), it follows from (2.10) that

$$rV_1/3 + (r^2+2s)U_1/3 \equiv 0 \pmod 3.$$

Hence,

$$G \equiv 2r(rV_1/3+(r^2+2s)U_1/3) + 3rsU_1/3 + 9tU_1/3 + 6sV_1/3 \equiv 0 \pmod 3$$

and $3 | (P,G,\Delta)$. By the reasoning given above, one of (i), (ii), (iii), or (iv) must be true. If W_n, V_n, U_n are given by (b), (c), (d), or (e), then by Lemma 3, $3 | H$, and we have

$$-4 \cdot 27 \cdot (r^2+2s)Q \equiv 9G^2 \pmod{27};$$

hence, $3 | (P,G,H)$ and $3 | F$.

The values of α, β, γ in Theorem 2 can be bounded. We give these bounds in

Lemma 4. If $(P,Q,R) = 1$, then $\alpha < 3$, $\beta < 4$, and $\gamma < 6$.

Proof. If $8 | (P,G,\Delta)$, then

$$-12(r^2+3s)Q \equiv 9G^2 \pmod 8.$$

Since $2 \nmid (r^2+3s)$, we have $2 | Q$ and it follows that $2 | R$.

If $\beta \geqslant 4$,

$$3W_1/3 + rV_1/3 + (r^2+2s)U_1/3 \equiv 0 \pmod{81}$$

and

$$3Q \equiv -[(r^2+3s)(V_1/3)^2 + (2r^3+7rs+9t)(U_1/3)(V_1/3) + 3(s^2-2rt)(U_1/3)^2] \pmod{243}.$$

If $27 \nmid (r^2+3s)$, then $9 | Q$. If $27 | (r^2+3s)$, we have $3 | r$, $3 | s$ and $(r/3)^2 + (s/3) \equiv 0 \pmod 3$. Since $81 | \Delta$, we also have $r/3 \equiv t \pmod 3$. Since

$$-3Q \equiv (7rs+9t)(U_1/3)(V_1/3) + (6rt+s^2)(U_1/3)^2 \pmod{27}$$

and $7rs + 9t \equiv 6tr + s^2 \equiv 0 \pmod{27}$, it follows that $9 | Q$. From the facts that $9 | Q$, $81 | \Delta$, $27 | N_1$, and

$$E_1 = \Delta(N_1/27)^2,$$

we see that $3 | R$.

If $\gamma \geqslant 6$, then $3^8 | -3\Delta$ and

$$-4 \cdot 27(r^2+3s)Q \equiv 9G^2 \pmod{3^8};$$

hence, $3^5 | (r^2+3s)Q$. It is not difficult to show that $9 | Q$. Since $3 | N_1$ and $3^8 | \Delta$, we have $3^{10} | \Delta N_1^2$, and consequently, $3 | R$.

6. PROPERTIES OF W_n, V_n, U_n

In the following sections, we will be demonstrating several divisibility properties of the W_n, V_n, U_n functions. Most of these results depend upon

Theorem 3. If $n \in N$, $(W_n, V_n, U_n) | 3$.

Proof. Suppose p ($\neq 3$) is a prime such that $p | (W_2, V_2, U_2)$. From (2.10), (2.11), (2.7), it is clear that $p | P_2$, $p | Q_2$, $p | R$. Since $P_2 = P^2 - 2Q$ and $Q_2 = Q^2 - 2RP$, we have $p | (P,Q,R)$, which is impossible by definition of W_n, V_n, U_n. If $9 | (W_2, V_2, U_2)$, then $3 | R$, $3 | P_2$, $9 | Q_2$; hence, $3 | (P,Q,R)$. The theorem is true for $n = 1, 2$.

Suppose $n > 2$ is the least positive integer such that $p | (W_n, V_n, U_n)$, where p ($\neq 3$) is a prime. Since $P | R$, by (2.18), it follows that

$$PW_{n-1} \equiv QW_{n-2},\quad PV_{n-1} \equiv QV_{n-2}, PU_{n-1} \equiv QU_{n-2} \pmod p.$$

If $p | P$, then $p \nmid Q$; hence, $p | (W_{n-2}, V_{n-2}, U_{n-2})$, which is impossible by the definition of n. If $p | Q$, then

$p \mid (W_{n-1}, V_{n-1}, U_{n-1})$, which is also impossible. This enables us to write

$$W_{n-1} \equiv P^{-1}QW_{n-2}, \quad V_{n-1} \equiv P^{-1}QV_{n-2}, \quad U_{n-1} \equiv P^{-1}QU_{n-2} \pmod p,$$

where $P^{-1}Q \not\equiv 0 \pmod p$. From (2.2), we see that

$$W_n \equiv P^{-1}QW_{n-1}, \quad V_n \equiv P^{-1}QV_{n-1}, \quad U_n \equiv P^{-1}QU_{n-1} \pmod p$$

and consequently $p \mid (W_{n-1}, V_{n-1}, U_{n-1})$, which is impossible.

Suppose $n > 2$ is the least positive integer such that $9 \mid (W_n, V_n, U_n)$. From (2.2), it is evident that

$$3 \mid (W_{n+1}, V_{n+1}, U_{n+1}).$$

If ψ has the same meaning as that assigned to it in the corollary of Lemma 3, we have $\psi \mid n$ and $\psi \mid n+1$; that is, $\psi = 1$. Since $3 \mid W_{n-3}$ and $3 \mid R$, we have

$$P(W_{n-1}/3) \equiv Q(W_{n-2}/3) \pmod 3$$

and similar results for V_{n-1} and U_{n-1}. By reasoning similar to that above, we obtain the result that

$$3 \mid (W_{n-1}/3, V_{n-1}/3, U_{n-1}/3),$$

which cannot be.

Corollary. If $n \in N$, $(U_n, V_n, R) \mid 3$.

Proof. If p ($\neq 3$) is a prime and $p \mid (U_n, V_n, R)$, then $p \mid W_n$, which contradicts the theorem. If $9 \mid (U_n, V_n, R)$, then by (2.7), $81 \mid W_n^3$ and $9 \mid W_n$, which is also a contradiction.

We have, with the aid of Theorem 3 and Lemma 3, completely characterized all the divisors of (W_n, V_n, U_n). We will now begin to develop some results concerning $D_n = (V_n, U_n)$. It will be seen that the divisibility properties of D_n are similar to those of Lucas' u_n (Carmichael's D_n). In fact, we have analogues of Carmichael's theorems I, II, III, IV, VI, X, XII, XIII, XVII (corollary), in Theorem 3 (corollary), Theorem 3, Lemma 3, Theorem 4, Theorem 5 (corollary), Theorem 7, Theorem 8, Theorem 8 (corollary), Theorem 7 (corollary), respectively. We also have the analogues of Corollaries I and II of Carmichael's Theorem VIII as a consequence of Theorem 5 and a result of Ward [9].

Theorem 4. If $n, k \in N$ and $m \mid D_n$, then $m \mid D_{kn}$.

Proof. This theorem is true for $k = 1$. Suppose it is true for $k = j$.

Since

$$3V_{(j+1)n} = V_nW_{jn} + W_nV_{jn} + sV_{jn}U_n + sV_nU_{jn} + (rs+t)U_nU_{jn}$$

and

$$3U_{(j+1)n} = W_{jn}U_n + U_{jn}W_n + V_nV_{jn} + rU_{jn}V_n + rU_nV_{jn} + (r^2+s)U_nU_{jn},$$

we have $m \mid D_{(j+1)m}$, when $3 \nmid m$. If $3 \mid m$, then $3 \mid W_n$ and $3 \mid W_{jn}$; hence, $3m \mid 3V_{(j+1)n}$, $3m \mid 3U_{(j+1)n}$ and $m \mid D_{(j+1)m}$. The theorem is true by induction.

Let D_ω be the first term of the sequence

$$D_1, D_2, D_3, \cdots, D_k, \cdots$$

in which m occurs as a factor. We call $\omega = \omega(m)$ the *rank of apparition of* n.

Theorem 5. If $n \in N$ and m is a divisor of D_n, then $\omega(m) \mid n$.

Proof. Suppose $\omega \nmid n$; then $n = k\omega + j$ $(0 < j < \omega)$. From (2.2)

$$3V_n = V_jW_{k\omega} + W_jV_{k\omega} + sV_jU_{k\omega} + sV_{k\omega}U_j + (rs+t)U_{k\omega}U_j,$$

$$3U_n = U_jW_{k\omega} + W_jU_{k\omega} + V_jV_{k\omega} + rU_{k\omega}V_j + rU_jU_{k\omega} + (r^2+s)U_{k\omega}U_j.$$

If $3 \nmid m$, $m \mid (V_jW_{k\omega}, U_jW_{k\omega})$. Since $m \mid D_{k\omega}$, $(m, W_{k\omega}) = 1$ and $m \mid D_j$.

If $3 \mid m$, then $3 \mid W_{k\omega}$ and $3 \mid W_n$. If ψ is the rank of apparition of 3, we know that $\psi \mid n$ and $\psi \mid k\omega$; hence, $\psi \mid j$ and $3 \mid (W_j, V_j, U_j)$. We now have $3m \mid (V_jW_{k\omega}, U_jW_{k\omega})$. If $3 \| m$, then $(m/3, W_{k\omega}) = 1$, $m/3 \mid (V_j, U_j)$, $3 \mid (V_j, U_j)$ and consequently $m \mid D_j$. If $3^\alpha \| m$ and $\alpha > 1$, then $3 \| W_{k\omega}$ and $m \mid D_j$.

If $\omega \nmid n$, we can find $j < \omega$ such that $m | D_j$. This contradicts the definition of ω.

Corollary. If $n,m \in N$, then $D_{(m,n)} = (D_m, D_n)$.

Proof. This result follows from the theorem and a result of Ward [9].

Corollary. If m,n are integers and $(m,n) = 1$, $\omega(mn)$ is the least common multiple of $\omega(m)$ and $\omega(n)$.

7. THE LAWS OF REPETITION AND APPARITION

We have defined the rank of apparition of an integer m without having shown whether it exists or, if it does exist, what its value is. We give in this section those values of m for which ω exists and we partially answer the question of the value of ω for these m values. *The Law of Repetition* describes how $\omega(p^n)$ (p a prime) may be determined once $\omega(p)$ is known. In order to prove the Law of Repetition, we must first give a few preliminary results.

Lemma 5. Suppose $3 \nmid R$ and $3 | D_m$; then $3 | (P_m, Q_m)$ if and only if $9 | D_{3m}$. If $3 \nmid \Delta$, then $3 | (P_m, Q_m)$ if and only if $9 | D_m$.

Proof. If $9 | D_k$, then $3 | W_k$ and $3 | (P_k, Q_k)$. If $\Delta \equiv r^2s^2 + s - tr \not\equiv 0 \pmod 3$ and $3 | (P_m, Q_m)$, then

$$r(V_m/3) + (r^2 + 2s)(U_m/3) \equiv 0 \pmod 3$$

and

$$-s(V_m/3)^2 - sr(U_m/3)(V_m/3) + (s^2 - 2tr)(U_m/3)^2 \equiv 0 \pmod 3 .$$

If $3 | r$, then $3 \nmid s$; hence, if $3 | U_m/3$, $9 | D_m$. If $3 \nmid r$, then $(V_m/3) \equiv -r(r^2 + 2s)U_m/3 \pmod 3$; thus,

$$-\Delta(U_m/3)^2 \equiv 0 \pmod 3$$

and $9 | D_m$.

If $9 | D_{3m}$, we have $3 | P_{3m}$ and $3 | Q_{3m}$. Now

$$P_{3m} = P_m^3 - 3Q_mP_m + 3R_m,$$
$$Q_{3m} = Q_m^3 - 3R_mP_mQ_m + 3R_m^2 ;$$

consequently, $3 | (P_m, Q_m)$. If $3 | (P_m, Q_m)$, then since

$$V_{3m}/3 = P_mV_{2m}/3 - Q_mV_m/3 \equiv 0 \pmod 3$$

and

$$U_{3m}/3 = P_mU_{2m}/3 - Q_mU_m/3 \equiv 0 \pmod 3,$$

we have $9 | D_{3m}$.

Lemma 6. Suppose $3 \nmid R$, $3 | D_m$, and $3 | \Delta$. If $3 \nmid P_m$, $9 | D_{2m}$ if and only if one of the following is true.

(i) $3 | s$, $3 | t$, $3 \nmid r$, $W_m \equiv U_m \not\equiv 0 \pmod 9$, and $9 | V_m$.
(ii) $s \equiv 1 \pmod 3$, $t \equiv -r \not\equiv 0 \pmod 3$, $W_m \equiv -U_m \not\equiv 0 \pmod 9$ and $V_m \equiv rU_m \pmod 9$.
(iii) $s \equiv -1 \pmod 3$, $3 | t$, $3 \nmid r$, and $W_m \equiv -rV_m + U_m \not\equiv 0 \pmod 9$.

Proof. Since $3 \nmid P_m$ and $3 | \Delta$, it is clear that $3 \nmid r$.

We show the necessity of one of (i), (ii), or (iii). If $9 | D_{2m}$, then

$$(sr + t)(U_m/3)^2 + 2s(V_m/3)(U_m/3) + 2(V_m/3)(W_m/3) \equiv 0 \pmod 3$$

and

$$(V_m/3)^2 + 2(W_m/3)(U_m/3) + 2r(U_m/3)(V_m/3) + (r^2 + s)(U_m/3) \equiv 0 \pmod 3.$$

If $9 | U_m$, then $9 | V_m$ and $3 | P_m$, which is impossible. If $9 | V_m$, then $3 | (rs + t)$ and $(r^2 + s)U_m \equiv W_m \pmod 9$. Now since $3 \nmid (s + 1)$, we have $3 | s - 1$ or $3 | s$. If $3 | (s - 1)$, then $3 | (r^2 + 2s)$ and $3 | P_m$. If $3 | s$, then $3 | t$ and $W_m \equiv U_m \not\equiv 0 \pmod 9$.

If $9 \nmid U_m$ and $9 \nmid V_m$, then

$$W_m - (sr + t)V_m + sU_m \equiv 0 \pmod 9$$
$$W_m + rV_m - (1 + r^2 + s)U_m \equiv 0 \pmod 9$$

and

$$r(s+1)^2V_m \equiv -(s+1)U_m \pmod 9.$$

If $3|s$, $rV_m \equiv -U_m \pmod 9$ and $3|P_m$. If $s \equiv 1 \pmod 3$, then $t \equiv -r \pmod 3$, $rV_m \equiv U_m \not\equiv 0 \pmod 9$ and $W_m \equiv -U_m \pmod 9$. If $s \equiv -1 \pmod 3$, then $3|t$, and $W_m \equiv -rV_m + U_m \pmod 9$.

It is clear that any one of the conditions (i), (ii), or (iii) is sufficient for $9|D_{2m}$.

Theorem 6. If $3\nmid R$, ψ is the rank of apparition of 3, and $9\nmid D_\psi$, then the rank of apparition of 9 is $\sigma\psi$, where the value of σ is given below.

I. $3\nmid\Delta$.

In this case, W_n, V_n, U_n are given by (a) and the value of σ is a function of the values (modulo 3) of $N_1/27$, Δ, P, Q. The values of σ are given in Table 3.

Table 3

$N_1/27$	Δ	P	Q	σ
0	± 1	P	Q	2
± 1	-1	± 1	± 1	4
± 1	-1	± 1	0	8
± 1	-1	0	Q	8
± 1	1	P	Q	13

II. $3|\Delta$.

Here $\sigma = 2$ if $3\nmid P_\psi$ and one of the following is true.

(i) $3|s$, $3|t$, $3\nmid r$, $W_\psi \equiv U_\psi \not\equiv 0 \pmod 9$ and $9|V_\psi$;

(ii) $s \equiv 1 \pmod 3$, $t \equiv -r \not\equiv 0 \pmod 3$, $W_\psi \equiv -U_\psi \not\equiv 0 \pmod 9$, and $V_\psi \equiv rU_\psi \pmod 9$;

(iii) $s \equiv -1 \pmod 3$, $3|t$, $3\nmid r$, and $W_\psi \equiv -rV_\psi + U_\psi \not\equiv 0 \pmod 9$.

$\sigma = 3$ if $3|P_\psi$.

$\sigma = 6$ if $3\nmid P_\psi$ and none of (i), (ii), (iii) is true.

Proof. Since $3|D_\psi$, we have $27|N_\psi$; hence

$$E_\psi = \Delta(N_\psi/27)^2.$$

If $3|\Delta$,

$$P_\psi R_\psi \equiv Q_\psi(Q_\psi P_\psi^2 - 1) \pmod 3.$$

If $3|P_\psi$, then $3|Q_\psi$ and $9|(V_{3\psi}, U_{3\psi})$. If $3\nmid P_\psi$, then

$$R_\psi \equiv P_\psi Q_\psi(Q_\psi - 1) \pmod 3;$$

thus, $Q_\psi \equiv -1 \pmod 3$ and $R_\psi \equiv -P_\psi \pmod 3$. Since

$$P_{2\psi} = P_\psi^2 - 2Q_\psi \equiv 0 \quad\text{and}\quad Q_{2\psi} = Q_\psi^2 - 2R_\psi P_\psi \equiv 0 \pmod 3,$$

it follows from Lemma 5 that $9|D_{6\psi}$ and $9\nmid D_{3\psi}$. From Lemma 6, we see that $9|D_{2\psi}$ if and only if one of (i), (ii) or (iii) is true.

If $3\nmid\Delta$ and $81|N_1$, then $3|E_1$, $3|(P_2, Q_2)$ and $\sigma = 2$.

If $\Delta \equiv -1 \pmod 3$ and $81|N_1$, then

$$PR \equiv P^2Q^2 - Q + 1 \pmod 3.$$

Using the formulas

$$P_{2k} = P_k^2 - 2Q_k \quad\text{and}\quad Q_{2k} = Q_k^2 - 2P_kR_k,$$

we see that if $3|P$, then $Q \equiv 1 \pmod 3$ and $P_2 \equiv Q_2 \equiv 1 \pmod 3$, $Q_4 \equiv P_4 \equiv -1 \pmod 3$, $Q_8 \equiv P_8 \equiv 0 \pmod 3$; consequently, $\sigma = 8$. The remaining results for this case are proved in the same way.

If $\Delta \equiv 1 \pmod 3$ and $81\nmid N_1$, then

$$PR \equiv P^2Q^2 - Q - 1 \pmod 3.$$

Using the formulas

$$P_{n+3} = PP_{n+2} - QP_{n+1} + RP_n$$
$$Q_{n+3} = QQ_{n+2} - PRQ_{n+1} + R^2Q_n\,,$$

we see that if $3|P$, then $Q \equiv -1 \pmod 3$ and $P_{13} \equiv Q_{13} \equiv 0 \pmod 3$. If $3\nmid P$, then $R \equiv P(Q^2 - Q - 1)$ and $P_{13} \equiv Q_{13} \equiv 0 \pmod 3$.

Theorem 7. (Law of Repetition). Let p be a prime. If, for $\lambda > 0$, $p^\lambda \neq 3, 2$ and $p^\lambda \| D_m$, then

$$p^{\alpha+\lambda} \| D_{m\nu p^\alpha}, \quad \text{where} \quad (\nu, p) = 1.$$

If $p^\lambda = 2$ and ν is odd, $p^{\alpha+1} | D_{m\nu p^\alpha}$ and $4 | D_{m\nu}$. If $p^\lambda = 3$ and $3\nmid R$, then

$$3^{\alpha+1} | D_{m\tau 3^{\alpha-1}} \quad \text{and} \quad 9\nmid D_{m\nu}, \quad \text{if} \quad \tau \nmid \nu.$$

Here

$$\tau = \sigma/(m/\psi, \sigma),$$

where ψ, σ have the meanings assigned to them in Theorem 6. If $3|R$, then $3\|D_n$ for any $n \in N$.

Proof. Since p is a divisor of $p!/[i!j!(p-i-j)!]$ when $i,j \neq 0,p$, we have (from (2.17))

$$3^{p-1}V_{mp} \equiv pW_m^{p-1}V_m \pmod{p^{\lambda+2}}$$
$$3^{p-1}U_{mp} \equiv pW_m^{p-1}U_m \pmod{p^{\lambda+2}}$$

if $p \neq 2$ or if $p = 2$ and $\lambda > 1$. If $p \neq 3$, then $p\nmid W_n$; hence $p^{\lambda+1}\|D_{mp}$. By induction $p^{\lambda+\alpha}\|D_{mp^\alpha}$. If

$$p^{\lambda+\alpha+1} | D_{m\mu p^\alpha}, \quad \text{then} \quad p^{\lambda+\alpha+1} | (D_{mp^\alpha\mu}, D_{mp^{\alpha+1}}) = D_{mp^\alpha},$$

which is impossible. If $p = 2$ and $\lambda = 1$, $3V_{2m} \equiv 3U_{2m} \equiv 0 \pmod 4$; hence, $2^{\alpha+1}|D_{2^\alpha m}$ and $4\nmid D_{m\mu}$.

If $3^\lambda\|D_m$ and $\lambda > 1$, then $3|W_m$ and $3\lambda \geq \lambda + 4$, $2\lambda + 2 \geq \lambda + 4$. Using the triplication formulas (2.4), we have

$$3^{\lambda+3} | 9V_{3m} \quad \text{and} \quad 3^{\lambda+3} | 9U_{3m}$$

or $3^{\lambda+1}|D_{3m}$. Also

$$9V_{3m} \equiv 3V_mW_m^2 \pmod{3^{\lambda+4}}$$
$$9U_{3m} \equiv 3U_mW_m^2 \pmod{3^{\lambda+4}}\,.$$

Since $9\nmid W_m$,

$$3^{\lambda+2}\nmid D_{3m} \quad \text{and} \quad 3^{\lambda+1}\|D_{3m}.$$

If $3\|D_m$, then $\psi|m$ and $9|D_n$ if and only if $\sigma\psi|n$. Since $\sigma\psi|m\tau$, we have $9|D_{m\tau}$ and $3^{\alpha+1}|D_{m\tau 3^{\alpha-1}}$. If $\tau\nmid\nu$, then $\sigma\psi\nmid\nu m$ and $9\nmid D_{\nu m}$.

If $3|R$ and $9|D_n$, then $81|W_n^3$ or $9|W_n$, which is impossible.

The *Law of Apparition* gives those primes for which the rank of apparition exists and also gives us some information concerning the value of the rank of apparition. We first define an auxiliary function y_n.

If p is a prime such that $p\nmid 3N_1R$, we define the function y_n to be the Lucas function u_n of (1.1), where $a_1 + a_2 \equiv g \pmod p$, $a_1a_2 \equiv h^3 \pmod p$, and

$$h = r^2 + 3s, \qquad g = 2r^3 + 9rs + 27t.$$

Theorem 8. (Law of Apparition). If p is a prime such that $p\nmid R$, then ω, the rank of apparition of p, exists. If $p = 3$, then $\omega = \psi$. Suppose $p\nmid 3R$; then $\omega(p)|\Phi(p)$, where the value of Φ is given below.

We let $p \equiv q \pmod 3$, where $|q| = 1$.

If $p\nmid \Delta N_1$ and $(\Delta|p) = -1$, then $(p-1)\nmid\omega$ and $\Phi(p) = p^2 - 1$.

If $p\nmid \Delta N_1h$ and $(\Delta|p) = +1$, then $\Phi(p) = p - 1$, when $y_{(p-q)/3} \equiv 0 \pmod p$; $\Phi(p) = p^2 + p + 1$, when $y_{(p-q)/3} \not\equiv 0 \pmod p$.

If $p\nmid \Delta N_1$, $(\Delta|p) = +1$, and $p|h$, then $p \equiv 1 \pmod 3$ and $\Phi(p) = p - 1$, when $(g|p)_3 = 1$; $\Phi(p) = p^2 + p + 1$, when $(g|p)_3 \neq 1$.

If $p \nmid \Delta$ and $p | N_1$, then $\Phi(p) = p - 1$.
If $p = 2$ and $p | \Delta$, then $\Phi(p) = 4$.
If $p \neq 2$, $p | \Delta$ and $p \nmid N_1$, then $p | \omega$ and $\Phi(p) = p(p-1)$.
If $p \neq 2$, $p | \Delta$ and $p | N_1$, then $\Phi(p) = p$, when $p | G$; $\Phi(p) = p - 1$, when $p \nmid G$.

Proof. These results may be deduced without much difficulty from (2.15) and results of Engstrom [5], Ward [8], and Cailler [2]. (See also Duparc [4].)

Corollary. If we define $\Phi(p^n) = p^{n-1}\Phi(p)$ for $p \neq 3$, $\Phi(3^2) = \sigma\psi$, $\Phi(3^n) = 3^{n-2}\Phi(3^2)$, and $\Phi(mn)$ to be the least common multiple of $\Phi(m)$ and $\Phi(n)$, when $(m,n) = 1$, then $\omega(m) | \Phi(m)$.

If p is of the form $3k + 1$ and $p \nmid \Delta N_1 R$, we can sharpen some of the results in the Law of Apparition.

Theorem 9. Let p ($\equiv 1 \pmod 3$) be a prime such that $p \nmid \Delta N_1 R$. If $(\Delta | p) = -1$, $\omega | (p^2 - 1)/3$ if and only if $(R|p)_3 = 1$. If $(\Delta | p) = +1$ and $y_{(p-q)/3} \not\equiv 0 \pmod p$, then $\omega | (p^2 + p + 1)/3$ if and only if $(R|p)_3 = 1$. If $(\Delta|p) = +1$ and $y_{(p-q)/3} \equiv 0 \pmod p$, $\omega | (p-1)/3$ only if $(R|p)_3 = 1$.

Proof. If $(\Delta | p) = -1$, then $(E_1 | p) = -1$ and the polynomial $x^3 - Px^2 + Qx - R$ factors modulo p into the product of a linear and irreducible quadratic factor. Let $K = GF(p^2)$ be the splitting field for this polynomial modulo p and let the roots of

$$x^3 - Px^2 - Qx - R = 0 \tag{7.1}$$

be θ, ϕ, ψ in K. Then in K

$$\theta^p = \theta, \quad \chi = \phi^p, \quad \chi^p = \phi, \quad R = \theta\phi\chi = \theta\phi^{p+1}.$$

If $R^{(p-1)/3} \equiv 1 \pmod p$, we have

$$\theta^{(p-1)/3}\phi^{(p^2-1)/3} = 1 \quad \text{and} \quad \theta^{(p^2-1)/3} = \phi^{(p^2-1)/3} = \phi^{p(p^2-1)/3}. \tag{7.2}$$

Since $p \nmid \Delta$, it follows that $p | D_{(p^2-1)/3}$. If $R^{(p-1)/3} \not\equiv 1 \pmod 3$, we cannot have (7.2). Since $p \nmid \Delta N_1$, it is clear that $p \nmid D_{(p^2-1)/3}$.

If $(\Delta | p) = +1$ and $p \nmid y_{(p-q)/3}$, the polynomial $x^3 - rx^2 - sx - t$ is irreducible modulo p; hence, the polynomial $x^3 - Px^2 + Qx - R$ is irreducible modulo p. If $K = GF(p^3)$ is the splitting field of this polynomial (modulo p) and θ, ϕ, χ are the roots of (7.1) in K, then

$$\theta^p = \phi, \quad \theta^{p^2} = \chi, \quad \theta^{p^3} = \theta, \quad R = \theta^{1+p+p^2}.$$

If $R^{(p-1)/3} \equiv 1 \pmod p$,

$$\theta^{(p^3-1)/3} = 1 \quad \text{and} \quad \theta^{p(p^2+p+1)/3} = \theta^{p^2(p^2+p+1)/3} = \theta^{(p^2+p+1)/3};$$

hence $p | D_{(p^2+p+1)/3}$. If $R^{(p-1)/3} \not\equiv 1 \pmod p$, then $p \nmid D_{(p^2+p+1)/3}$.

If $(\Delta | p) = +1$ and $p | y_{(p-q)/3}$, the polynomial $x^3 - Px^2 + Qx - R$ splits modulo p into the product of three linear factors. It is not difficult to show that if $p | D_{(p-1)/3}$, then $R^{(p-1)/3} \equiv 1 \pmod p$.

We have not discussed the functions

$$B_n = (W_n, V_n) \quad \text{and} \quad C_n = (W_n, U_n)$$

which are somewhat analogous in their divisibility properties to Lucas' V_n or Carmichael's S_n. The functions B_n and C_n behave in a rather complicated fashion and in a further paper results concerning these functions will be presented together with other results on the W_n, V_n, U_n functions.

REFERENCES

1. E. T. Bell, "Notes on Recurring Series of the Third Order," *Tôhoku Math. Journal*, Vol. 24 (1924), pp. 168–184.
2. C. Cailler, "Sur les Congruences du Troisième Degré," *L'Enseig. Math.*, Vol. 10 (1908), pp. 474–487.
3. R. D. Carmichael, "On the Numerical Factors of the Arithmetic Forms $\alpha^n \pm \beta^n$," *Annals of Math. (2)*, Vol. 15 (1913–1914), pp. 30–70.
4. H. J. A. Duparc, "Periodicity Properties of Recurring Sequences II," *Indagationes Math.*, Vol. 16 (1954), pp. 473–485.

5. H. T. Engstrom, "On Sequences Defined by Linear Recurrence Relations," *Trans. Amer. Math. Soc.,* Vol. 33 (1931), pp. 210–218.
6. D. H. Lehmer, "An Extended Theory of Lucas' Functions," *Annals of Math. (2),* Vol. 30 (1929), pp. 66–72.
7. Edouard Lucas, "Theorie des Fonctions Numeriques Implement Periodiques," *Amer. J. of Math.,* Vol. 1 (1878), pp. 184–240, 289–321.
8. Morgan Ward, "The Characteristic Number of a Sequence of Integers Satisfying a Linear Recursion Relation," *Trans. Amer. Math. Soc.,* Vol. 33 (1931), pp. 153–165.
9. Morgan Ward, "A Note on Divisbility Sequences," *Bull. Amer. Math. Soc.,* Vol. 42 (1936), pp. 843–845.
10. H. C. Williams, "A Generalization of the Lucas Functions," unpublished Ph.D. thesis, University of Waterloo, Ontario, 1969.
11. H. C. Williams, "On a Generalization of the Lucas Functions," *Acta Arith.,* Vol. 20 (1972), pp. 33–51.
12. H. C. Williams, "Fibonacci Numbers Obtained from Pascal's Triangle with Generalizations," *The Fibonacci Quarterly,* Vol. 10 (1972), pp. 405–412.

****

PHI AGAIN: A RELATIONSHIP BETWEEN THE GOLDEN RATIO AND THE LIMIT OF A RATIO OF MODIFIED BESSEL FUNCTIONS

HARVEY J. HINDIN
State University of New York, Empire State College-Stony Brook University, Stony Brook, New York 11790

In his study of infinite continued fractions whose partial quotients form a general arithmetic progression, D. H. Lehmer derived a formula for their evaluation in terms of modified Bessel Functions [1]. We have

$$F(a,b) = a_0 + \frac{1}{a_1} + \frac{1}{a_2} + \cdots = [a_0, a_1, a_2, \cdots], \tag{1}$$

where $a_n = an + b$. It was shown that

$$F(a,b) = \frac{I_{\alpha-1}(2/a)}{I_\alpha(2/a)}, \tag{2}$$

where $\alpha = b/a$ and I_α is the modified Bessel function

$$I_\alpha(z) = i^{-\alpha} J_\alpha(iz) \sum_{m=0}^{\infty} \frac{(z/2)^{\alpha+2m}}{\Gamma(m+1)\Gamma(\alpha+m+1)}. \tag{3}$$

Using (1) and (2) with $c\alpha = 2/a$ and $b = c/2$, we have

$$F(a,b) = [b, a+b, 2a+b, \cdots] = \frac{I_{\alpha-1}(c\alpha)}{I_\alpha(c\alpha)}. \tag{4}$$

As $\alpha \to \infty$ $(a \to 0)$, in the limit (Theorem 5 of [1]),

$$\lim_{\alpha \to \infty} \frac{I_{\alpha-1}(c\alpha)}{I_\alpha(c\alpha)} = F(0,b) = [b, b, b, \cdots]. \tag{5}$$

But, for $b = 1$, $(c = 2)$, $F(0,1)$ is the positive root of the quadratic equation

$$1 + \frac{1}{x} = x \tag{6}$$

which is represented by the infinite continued fraction expansion $[1, 1, 1, \cdots]$.

[Continued on p. 152.]