PACIFIC JOURNAL OF MATHEMATICS
Vol. 77, No. 1, 1978

SOME PROPERTIES OF A SPECIAL SET OF RECURRING SEQUENCES

H. C. WILLIAMS

Several number theoretic and identity properties of three special second order recurring sequences are established. These are used to develop a necessary and sufficient condition for any integer of the form 2^n3^mA-1 ($A<2^{n+1}3^m-1$) to be prime. This condition can be easily implemented on a computer.

1. **Introduction.** Various tests for primality of integers of the form 2^nA-1 and 3^nA-1 are currently available; for example, Lehmer [2] and Riesel [5] have developed necessary and sufficient conditions for 2^nA-1 to be prime when $A<2^n$ and Williams [6] has given a necessary and sufficient condition for the primality of $2A3^n-1$ when $A<4\cdot 3^n-1$. Of special concern to Riesel was the determination of the primality of $3A2^n-1$; in this paper we present a simple necessary and sufficient condition for 2^n3^mA-1 to be prime when $A<2^{n+1}3^m-1$. In order to obtain this result we must first develop some properties of a special set of second order linear recurring sequences.

Let a, b be two integers and put $\alpha=a+b\rho$, $\beta=a+b\rho^2$, where $\rho^2+\rho+1=0$. We define for any integer n

$$R_n=\frac{\rho\alpha^n-\rho^2\beta^n}{\rho-\rho^2},$$
$$S_n=\frac{\rho^2\alpha^n-\rho\beta^n}{\rho-\rho^2},$$
$$T_n=\frac{\alpha^n-\beta^n}{\rho-\rho^2}.$$

We see that $R_0=1$, $S_0=-1$, $T_0=0$, $R_1=a-b$, $S_1=-a$, $T_1=b$. Putting $G=\alpha+\beta=2a-b$ and $H=\alpha\beta=a^2-ab+b^2$, we get

$$\begin{aligned}R_{n+2}&=GR_{n+1}-HR_n,\\ S_{n+2}&=GS_{n+1}-HS_n,\\ T_{n+2}&=GT_{n+1}-HT_n.\end{aligned}\tag{1.1}$$

It follows that R_n, S_n, T_n are integers for any nonnegative integral value of n.

In the next sections of this paper we present a number of identities satisfied by the R_n, S_n, T_n functions. We also develop some of their number theoretic properties. It should be noted that the function T_n is simply a constant multiple b of the Lucas function $U = (\alpha^n - \beta^n)/(\alpha - \beta)$; hence, many of its properties are easily deduced from the well-known (see, for example, [2]) properties of the Lucas functions.

2. **Some identities.** We first note that from the definition of R_n, S_n, T_n, we obtain the fundamental identity

$$R_n + S_n + T_n = 0 .$$

We can easily verify for any integers m, n that

$$\begin{aligned} R_{m+n} &= R_mR_n - T_mT_n , \\ S_{m+n} &= T_mT_n - S_mS_n , \\ T_{m+n} &= S_mS_n - R_mR_n = T_mR_n - S_mT_n = R_mT_n - T_mS_n . \end{aligned} \tag{2.1}$$

Putting $m = 1$, we get

$$R_{n+1} = aR_n + bS_n , \quad S_{n+1} = (a-b)S_n - bR_n , \quad T_{n+1} = (b-a)R_n - aS_n .$$

Putting $n = m$, we see that

$$\begin{gathered} R_{2n} = -S_n(2R_n + S_n) , \qquad S_{2n} = R_n(2S_n + R_n) , \\ T_{2n} = T_n(R_n - S_n) ; \end{gathered} \tag{2.2}$$

also, by using these results and putting $m = 2n$ above, we get

$$\begin{gathered} R_{3n} = S_n^3 - 3S_nR_n^2 - R_n^3 , \qquad S_{3n} = R_n^3 - 3S_n^2R_n - S_n^3 , \\ T_{3n} = -3R_nS_nT_n = -(R_n^3 + S_n^3 + T_n^3). \quad (\text{Use } -R_n^3 = (S_n + T_n)^3.) \end{gathered}$$

Since

$$H^nR_{-n} = -S_n , \qquad H^nS_{-n} = -R_n , \qquad H^nT_{-n} = -T_n ,$$

it follows that

$$\begin{gathered} H^mR_{n-m} = T_mT_n - S_mR_n , \qquad H^mS_{n-m} = R_mS_n - T_mT_n , \\ H^mT_{n-m} = S_mR_n - R_mS_n = R_mT_n - T_mR_n = T_mS_n - R_mT_n . \end{gathered} \tag{2.3}$$

If, in the first of these formulas, we put $n = m$, we have $R_0H^n = T_n^2 - R_nS_n$; hence, we can deduce the following:

$$\begin{gathered} T_n^2 - R_nS_n = R_n^2 - T_nS_n = S_n^2 - T_nR_n = H^n , \\ T_n^2 + R_nT_n + R_n^2 = R_n^2 + S_nR_n + S_n^2 = S_n^2 + T_nS_n + T_n^2 = H^n , \\ T_nS_n + S_nR_n + R_nT_n = -H^n . \end{gathered} \tag{2.4}$$

More generally, we have

$$R_n^2 - R_{n-m}R_{n+m} = S_n^2 - S_{n-m}S_{n+m} = T_n^2 - T_{n-m}T_{n+m} = H^{n-m}T_m^2 ,$$

$$R_n^2 - T_{n-m}S_{m+n} = S_n^2 - R_{n-m}T_{m+n} = T_n^2 - S_{n-m}R_{n+m} = H^{n-m}R_m^2 ,$$

$$R_n^2 - S_{n-m}T_{n+m} = S_n^2 - T_{n-m}R_{m+n} = T_n^2 - R_{n-m}S_{m+n} = H^{n-m}S_m^2 .$$

We also have

$$R_{n+m}^2 - H^{2m}R_{n-m}^2 = T_{2m}S_{2n} , \quad S_{n+m}^2 - H^{2m}S_{n-m}^2 = T_{2m}R_{2n} ,$$
$$T_{n+m}^2 - H^{2m}T_{n-m}^2 = T_{2m}T_{2n} .$$

A great many other identities satisfied by these functions can be developed; for example, since

$$R_n + S_n + T_n = 0 , \qquad R_nS_n + S_nT_n + R_nT_n = -H^n ,$$

we can use Waring's formula (see, for example, [4] p. 5) to obtain

$$R_n^m + S_n^m + T_n^m = \begin{cases} \displaystyle\sum_{j=0}^{[r/3]} \frac{(r-j-1)!2r}{(2j)!(r-3j)!} H^{(r-3j)n}(R_nS_nT_n)^{2j} & (m = 2r) \\ \displaystyle\sum_{j=0}^{[(r-1)/3]} \frac{(r-1-j)!(2r+1)}{(2j+1)!(r-1-3j)!} H^{(r-1-3j)n}(R_nS_nT_n)^{2j+1} & (m = 2r+1) \end{cases}$$

$$(R_nS_n)^m + (S_nT_n)^m + (T_nR_n)^m$$
$$= (-1)^m \sum_{j=0}^{[m/3]} (-1)^j \frac{(m-2j-1)!m}{(m-3j)!j!} H^{n(m-3j)}(R_nS_nT_n)^{2j}$$

for $m > 0$. From these we deduce the rather interesting identities

$$R_n^4 + S_n^4 + T_n^4 = 2H^{2n} ,$$
$$R_n^7 + S_n^7 + T_n^7 = 7H^{2n}R_nS_nT_n ,$$
$$R_n^{10} + S_n^{10} + T_n^{10} = 2H^{5n} + 15H^{2n}R_n^2S_n^2T_n^2 ,$$
$$R_n^5S_n^5 + R_n^5T_n^5 + S_n^5T_n^5 = 5H^{2n}R_n^2S_n^2T_n^2 - H^{5n} .$$

The following identities are also of some interest:

$$(S_n(S_n^2 - 3H^n))^3 + (T_n(T_n^2 - 3H^n))^3 + (R_n(R_n^2 - 3H^n))^3$$
$$= 3(R_nS_nT_n)^3 ,$$

$$(R_nS_n(H^n + T_n^2))^4 + (R_nT_n(H^n + S_n^2))^4 + (S_nT_n(H^n + R_n^2))^4$$
$$= H^{8n} + 28H^{2n}(R_nS_nT_n)^4 .$$

Both of these formulas can be derived by expanding the powers of the binomials and using the formulas above for expressions of the form $R_n^j + S_n^j + T_n^j$ and $(R_nS_n)^j + (S_nT_n)^j + (T_nR_n)^j$.

If we put $W_n = R_n - S_n$, $X_n = S_n - T_n = 2S_n + R_n$, $Y_n = T_n - R_n = -2R_n - S_n$, we have

$$W_n + X_n + Y_n = 0 ,$$

$$3R_n = W_n - Y_n , \qquad 3S_n = X_n - W_n , \qquad 3T_n = Y_n - X_n$$

$$R_{2n} = S_n Y_n , \qquad S_{2n} = R_n X_n , \qquad T_{2n} = T_n W_n .$$

We also have

$$3W_{m+n} = W_m W_n + Y_m X_n + Y_n X_m ,$$

$$3X_{m+n} = Y_m Y_n + X_m W_n + W_m X_n ,$$

$$3Y_{m+n} = X_m X_n + Y_m W_n + W_m Y_n ,$$

and from these we are able to derive

$$W_{2n} = (W_n^2 + 2X_n Y_n)/3 = X_n Y_n + H^n = W_n^2 - 2H^n ,$$

$$Y_{2n} = (X_n^2 + 2W_n Y_n)/3 = W_n Y_n + H^n = X_n^2 - 2H^n ,$$

$$X_{2n} = (Y_n^2 + 2X_n W_n)/3 = W_n X_n + H^n = Y_n^2 - 2H^n ,$$

and

$$3X_{3n} = X_n^3 + 3X_n^2 Y_n - Y_n^3 ,$$

$$3Y_{3n} = Y_n^3 + 3Y_n^2 X_n - X_n^3 ,$$

$$W_{3n} = X_n Y_n W_n .$$

Many other identities similar to those satisfied by the R_n, S_n, T_n functions are satisfied by W_n, X_n, Y_n functions.

3. Some number theoretic results. In the discussion that follows we will assume that a and b satisfy the following two properties:

(1) $$(a, b) = 1 ,$$

(2) $$a \not\equiv -b \pmod 3 .$$

It follows from (1) and (2) that $(G, H) = 1$. We can now develop several divisibility properties of the R_n, S_n, T_n functions. We will also assume in what follows that n, m represent positive integers.

LEMMA 1. *For any n, $(R_n, H) = (S_n, H) = (T_n, H) = 1$.*

Proof. If p is any prime divisor of R_n and H, then by (1.1) p is a divisor of R_{n-1}. By continuing this reasoning, we see that $p \mid R_1$. If $p \mid R_1$ and $p \mid H$, then $R_0 = 1$ and $p \mid G$, which is impossible. In the same way we see that $(S_n, H) = 1$. Also, if $p \mid (T_n, H)$, then by the above reasoning $p \mid T_1 = b$. Since $p \mid H$, we have $p \mid a$ and consequently $p \mid G$.

LEMMA 2. *For any n, $(R_n, S_n) = (S_n, T_n) = (T_n, R_n) = 1$.*

Proof. If p is any prime divisor of any two of R_n, S_n, T_n, then by (2.4) p must divide H, which is impossible by the preceding lemma.

Since T_n is a simple multiple of the Lucas function U_n, $\{T_n\}$ is divisibility sequence, i.e., $T_n \mid T_m$ whenever $n \mid m$. The analogous properties of R_n and S_n are given in

THEOREM 1. *Suppose $n \mid m$. If $m/n \equiv 1 \pmod 3$, then $R_n \mid R_m$ and $S_n \mid S_m$; if $m/n \equiv -1 \pmod 3$, then $R_n \mid S_m$, $S_n \mid R_m$; if $m/n \equiv 0 \pmod 3$, then $R_n \mid T_m$, $S_n \mid T_m$.*

Proof. From the identities of §1 we see that $R_n \mid S_{2n}$, $S_n \mid R_{2n}$, $R_n \mid T_{3n}$, $S_n \mid T_{3n}$. Now since $T_{3n} \mid T_{3kn}$,

$$\begin{aligned} R_{(3k+t)n} &= R_{3kn}R_{tn} - T_{3kn}T_{tn} \\ &\equiv R_{3kn}R_{tn} \pmod{R_nS_n} . \end{aligned}$$

If $t = 1$, $R_n \mid R_{(3k+t)n}$; if $t = 2$, $S_n \mid R_{(3k+t)n}$. The remaining results are proved in a similar manner.

Let $T_{\omega(m)}$ be the first term of the sequence

$$T_1, T_2, T_3, \cdots, T_n ,$$

in which m occurs as a factor. We will call $\omega = \omega(m)$ the "rank of apparition" of m. From the theory of Lucas functions, it follows that if $m \mid T_n$, then $\omega(m) \mid n$ and consequently that $(T_m, T_n) = T_{(m,n)}$. We also have the result that if $(H, m) = 1$, then $\omega(m)$ always exists.

We now define $\omega_1 = \omega_1(m)$ and $\omega_2 = \omega_2(m)$ as analogues of $\omega(m)$. We say for a given m that R_{ω_1} and S_{ω_2} are respectively the first term of the sequences

$$\{R_k\}_{k=1}^{\infty} \quad \text{and} \quad \{S_k\}_{k=1}^{\infty} \quad \text{which } m \text{ divides} .$$

It is not in general true that $\omega_1(m)$ or $\omega_2(m)$ exist for any m such that $(m, H) = 1$. In the results that follow we give some characterization of those values of m such that $\omega_1(m)$ or $\omega_2(m)$ do exist. In Theorems 2, 3, 4, and Lemma 3 we give results concerning R_n and ω_1 only; however, analogous results involving S_n and ω_2 for each of these are also true and their proofs are similar.

THEOREM 2. *If $(m, H) = 1$ and ω_1 exists, then ω_2 exists, $3 \mid \omega$, $\omega_1 = \omega/3$ or $2\omega/3$, and $\omega_1 + \omega_2 = \omega$.*

Proof. Suppose $\omega_1 \geqq \omega$. We have

$$\omega_1 = q\omega + r \quad (0 \leqq r < \omega \leqq \omega_1)$$

and

$$0 \equiv R_{\omega_1} = R_{q\omega}R_r - T_{q\omega}T_r \equiv R_{q\omega}R_r \,(\mathrm{mod}\, m)\,.$$

Since $m \mid T_{q\omega}$ and $(T_{q\omega}, R_{q\omega}) = 1$, we see that $m \mid R_r$, which is impossible. Thus, $\omega_1 < \omega$.

Since $m \mid T_{3\omega_1}$, we must have $\omega \mid 3\omega_1$; since $\omega > \omega_1$, we see that $3 \mid \omega$ and $\omega_1 = \omega/3$ or $2\omega/3$. Now

$$H^{\omega_1}S_{\omega-\omega_1} = S_\omega R_{\omega_1} - T_\omega T_{\omega_1} \equiv 0 \,(\mathrm{mod}\, m)\,;$$

thus, $m \mid S_{\omega-\omega_1}$ and $\omega_2 \leqq \omega - \omega_1 < \omega$. Since as with ω_1, $m \mid T_{3\omega_2}$, it follows that $\omega \mid 3\omega_2$, so $\omega_2 = \omega/3$ or $2\omega/3$. Now if $\omega_1 = \omega_2 = \omega/3$ or $2\omega/3$, then $R_{\omega_1} + S_{\omega_1} + T_{\omega_1} = 0$ implies $m \mid T_{\omega_1}$, which is a contradiction since $\omega_1 < \omega$. Thus, since $\omega_1 \neq \omega_2$, we must have $\omega_1 + \omega_2 = \omega$.

THEOREM 3. *If* $(m, H) = 1$ *and* $m \mid R_n$, *then* ω_1 *exists and either* $\omega_1 \mid n$ *and* $n/\omega_1 \equiv 1 \,(\mathrm{mod}\, 3)$ *or* $w_2 \mid n$, $\omega_2 = \omega_1/2$ *and* $n/\omega_2 \equiv -1 \,(\mathrm{mod}\, 6)$.

Proof. Let $n = 3\omega_1 q + r$ $(0 \leqq r < 3\omega_1)$; then

$$0 \equiv R_n = R_{3\omega_1 q}R_r - T_{3\omega_1 q}T_r \equiv R_{3\omega_1 q}R_r \,(\mathrm{mod}\, m)$$

and $m \mid R_r$. We now distinguish two cases.

Case 1. $\omega_1 = \omega/3$. Here we have $r < \omega$ and $3r < 3\omega$. Since $m \mid T_{3r}$, we see that $3r = \omega$ or 2ω. If $3r = 2\omega$, then $r = \omega_2$, which, since $(R_r, S_r) = 1$, is impossible. Thus, $r = \omega/3 = \omega_1$, $\omega_1 \mid n$ and $n/\omega_1 \equiv 1 \,(\mathrm{mod}\, 3)$.

Case 2. $\omega_1 = 2\omega/3$. In this case we see that $r < 2\omega$ and $3r < 6\omega$. Thus, $3r$ is one of ω, 2ω, 4ω, 5ω. If $3r = \omega$ or 4ω, then $r = \omega_2$ or $4\omega_2$. Since $(R_r, S_r) = 1$, this is impossible. Thus $r = \omega_1$ or $\omega + \omega_1$. If $r = \omega_1$, we have $\omega_1 \mid n$ and $n/\omega_1 \equiv 1 \,(\mathrm{mod}\, 3)$; if $r = \omega + \omega_1$, then $n = 3\omega_1 q + \omega + \omega_1 = 6\omega_2 q + 3\omega_2 + 2\omega_2 = (6q + 5)\omega_2$.

COROLLARY. *Under the conditions of Theorem* 3, *we must have* $n \equiv \omega_1 \,(\mathrm{mod}\, 3^{\nu+1})$, *where* $3^\nu \,\|\, \omega_1$, $\nu \geqq 0$.

THEOREM 4. *If* m *and* n *are integers such that* $(m, n) = 1$, *then* $\omega_1(mn)$ *exists if and only if* $\omega_1(m)$ *and* $\omega_1(n)$ *exist and* $\omega_1(m) \equiv \omega_1(n)$ $(\mathrm{mod}\, 3^{\nu+1})$, *where* $3^\nu \,\|\, \omega_1(m)$, $\nu \geqq 0$.

Proof. Suppose $\Omega_1 = \omega_1(mn)$ exists; then clearly $\omega_1 = \omega_1(m)$ and $\omega_1^* = \omega_1(n)$ exist and

$$\Omega_1 \equiv \omega_1 \pmod{3^{\nu+1}} \qquad (3^\nu \| \omega_1) ,$$
$$\Omega_1 \equiv \omega_1^* \pmod{3^{\nu^*+1}} \qquad (3^{\nu^*} \| \omega_1^*) .$$

It follows that $\nu = \nu^*$ and $\omega_1 \equiv \omega_1^* \pmod{3^{\nu+1}}$.

If ω_1 and ω_1^* exist and $\omega_1 \equiv \omega_1^* \pmod{3^{\nu+1}}$ $(3^\nu \| \omega_1)$, put $\Omega = [\omega_1, \omega_1^*]$. We see that

$$\frac{\Omega}{\omega_1} \equiv \frac{\Omega}{\omega_1^*} \not\equiv 0 \pmod 3 .$$

If $\Omega/\omega_1 \equiv 1 \pmod 3$, then $R_\Omega \equiv 0 \pmod{mn}$; if $\Omega/\omega \equiv -1 \pmod 3$, then $S_\Omega \equiv R_{2\Omega} \equiv 0 \pmod{mn}$. In either case we see that $\omega_1(mn)$ must exist.

In order to continue our discussion of the existence of $\omega_1(m)$ and $\omega_2(m)$ it is necessary to consider the question of the existence of $\omega_1(p^n)$, $\omega_2(p^n)$, where p is a prime. This is done in the next section.

4. Some results modulo p. From the theory of Lucas functions we know that if $p^\lambda > 2$, and $p^\lambda \| T_n$ then $p^{\lambda+\nu} \| T_{np^\nu}$; also, if $p^\lambda = 2$ and $2 | T_n$, then $4 | T_{2n}$. We will attempt to discover similar results for R_n and S_n. We must deal with the special case $p = 3$ separately.

LEMMA 3. *If $3^\nu \| R_m$ when $\nu \geqq 1$, then $3^\nu \| R_{mn}$ when $n \equiv 1 \pmod 3$; otherwise, $3 \nmid R_{mn}$.*

Proof. Certainly $3^\nu | R_{mn}$ when $n \equiv 1 \pmod 3$ (Theorem 1); suppose $3^{\nu+1} | R_{mn}$. Now $3^{\nu+2} | T_{9m}$ and $3^{\nu+2} | T_{3mn}$; hence, $3^{\nu+2} | T_{3m} = (T_{9m}, T_{3mn})$, which is impossible. If $3 | R_{mn}$ when $n \not\equiv 1 \pmod 3$, then since $3 | R_m$, we have $3 | (T_m, R_m)$ or $3 | (R_m, S_m)$, neither of which is possible.

We deal now with any prime $p \neq 3$.

THEOREM 5. *Let p be any prime which is not 3 and suppose $\lambda > 1$. If $p^\lambda \neq 2$ and $p^\lambda \| R_m$, then $p^{\lambda+\nu} \| R_{mp^\nu}$ when $p^\nu \equiv 1 \pmod 3$ and $p^{\lambda+\nu} \| S_{mp^\nu}$ when $p^\nu \equiv -1 \pmod 3$. If $p^\lambda \neq 2$ and $p^\lambda \| S_m$, then $p^{\lambda+\nu} \| S_{mp^\nu}$ when $p^\nu \equiv -1 \pmod 3$ and $p^{\lambda+\nu} \| R_{mp^\nu}$ when $p^\nu \equiv -1 \pmod 3$. If $2 | R_m$, then $4 | S_{2m}$; if $2 S_m$, then $4 | R_{2m}$.*

Proof. From the definitions of R_n and S_n it is easy to show that

$$\rho^2 S_{mp} - \rho R_{mp} = (\rho^2 S_m - \rho R_m)^p ,$$
$$\rho S_{mp} - \rho^2 R_{mp} = (\rho S_m - \rho^2 R_m)^p .$$

Suppose $p \neq 2$. If $p^\lambda \| R_m$, then

$$\rho^2 S_{mp} - \rho R_{mp} \equiv \rho^{2p} S_m^p - p\rho^{2p-1} R_m S_m^{p-1} \pmod{p^{\lambda+2}},$$
$$\rho S_{mp} - \rho^2 R_{mp} \equiv \rho^p S_m^p - p\rho^{p+1} R_m S_m^{p-1} \pmod{p^{\lambda+2}};$$

therefore,

$$R_{mp} \equiv pR_m S_m^{p-1} \pmod{p^{\lambda+2}} \qquad \text{when} \quad p \equiv 1 \pmod 3$$

and

$$S_{mp} \equiv pR_m S_m^{p-1} \pmod{p^{\lambda+2}} \qquad \text{when} \quad p \equiv -1 \pmod 3 .$$

We get similar results when $p^\lambda \| S_m$. Thus the theorem is true for $\nu = 1$. That it is true for a general ν can be easily shown by induction on ν. When $p = 2$ we prove the theorem by using the identities (2.2).

When $p \neq 3$, we see that $\omega_1(p^n)$ and $\omega_2(p^n)$ both exist when $\omega_1(p)$ and $\omega_2(p)$ exist. We need now only consider the problem of when $\omega_1(p)$, $\omega_2(p)$ exist. Since $3 \mid T_3$, we see that $\omega_1(3^n)$ exists only if $3^n \mid R_1$ or $3^n \mid S_1$ and similarly for $\omega_2(3^n)$.

Let $p (\neq 3)$ be a prime. If $p \equiv 1 \pmod 3$, let

$$\pi = r + s\rho ,$$

where $r \equiv -1 \pmod 3$, $3 \mid s$ and $N(\pi) = \pi\bar{\pi} = r^2 - sr + s^2 = p$; if $p \equiv -1 \pmod 3$, let $\pi = \bar{\pi} = p$, $N(\pi) = p^2$. We have π a prime in the Eisenstein field $Q(\rho)$ and we define $[\mu \mid \pi]$ to the cubic character of $\mu \in Q[\rho]$ modulo π. That is

$$\mu^{(N(\pi)-1)/3} \equiv \left[\frac{\mu}{\pi}\right] \pmod{\pi}$$

and

$$\left[\frac{\mu}{\pi}\right] = 1 , \qquad \rho, \quad \text{or} \quad \rho^2 .$$

THEOREM 6. *If* $p \equiv \varepsilon \pmod 3$, *where* $|\varepsilon| = 1$, *and* $[H\alpha \mid \pi] = \rho^\eta$, *then* $p \mid R_{(p-\varepsilon)/3}$ *when* $\eta = 2$, $p \mid S_{(p-\varepsilon)/3}$ *when* $\eta = 1$, *and* $\rho \mid T_{(p-\varepsilon)/3}$ *when* $\eta = 0$.

Proof. We consider two possible cases.

Case 1. $\varepsilon = +1$. In this case $N(\pi) = p$,

$$\alpha^p \equiv \alpha \pmod p , \quad \text{and} \quad (\alpha H)^{(p-1)/3} \equiv \rho^\eta \pmod{\pi} ;$$

hence,

$$\alpha^{2(p-1)/3}\beta^{(p-1)/3} \equiv \rho^{\eta} \pmod{\pi}$$

and

$$\alpha^{(p-1)/3} \equiv \rho^{2\eta}\beta^{(p-1)/3} \pmod{\pi} .$$

The theorem follows easily from this result and the definition of R_n, S_n and T_n.

Case 2. $\varepsilon = -1$. In this case $N(\pi) = p^2$, $\alpha^p \equiv \beta \pmod{p}$,

$$(\alpha H)^{(p^2-1)/3} \equiv \alpha^{(p^2-1)/3} \equiv (\alpha^{p-1})^{(p+1)/3} \equiv (\beta/\alpha)^{(p+1)/3} \pmod{p} .$$

It follows that

$$\alpha^{(p+1)/3} \equiv \rho^{2\eta}\beta^{(p+1)/3} \pmod{p} .$$

If $\eta = 0$ and $p \not\equiv \varepsilon \pmod{9}$, then $\omega_1(p)$ and $\omega_2(p)$ can not exist; for, in this case, $\omega \mid (p - \varepsilon)/3$ and $3 \nmid \omega$. If, on the other hand, $\eta \neq 0$, then ω_1 and ω_2 do exist and

$$\omega_1 \equiv 2\eta(p - \varepsilon)/3 \pmod{3^\nu}$$
$$\omega_2 \equiv \eta(p - \varepsilon)/3 \pmod{3^\nu}$$

where $3^\nu \| p - \varepsilon$. The question of whether $\omega_1 = 2\omega_2$ or $\omega_1 = \omega_2/2$ seems to be rather difficult. We can give some simple results on this but we first require

THEOREM 7. *If p is a prime such that $p \equiv \varepsilon \pmod{6}$, $|\varepsilon| = 1$, $\lambda = (p - \varepsilon)/6$, and $\sigma = (H|p)$ (Legendre symbol), then one and only one of W_λ, X_λ, Y_λ, R_λ, S_λ, T_λ is divisible by p and that one is given in the table below according to the value of σ and η.*

σ \ η	0	1	2
-1	W_λ	X_λ	Y_λ
1	T_λ	R_λ	S_λ

Proof. If $\varepsilon = 1$, $\alpha^{p-\varepsilon} \equiv \beta^{p-\varepsilon} \equiv 1 \pmod{p}$; if $\varepsilon = -1$, $\alpha^{p-\varepsilon} \equiv \beta^{p-\varepsilon} \equiv \alpha\beta = H \pmod{p}$; hence, we easily obtain the result that

$$R_{6\lambda} \equiv H^{(1-\varepsilon)/2} , \qquad S_{6\lambda} \equiv -H^{(1-\varepsilon)/2} , \qquad T_{6\lambda} \equiv 0 \pmod{p} .$$

Thus, $W_{6\lambda} \equiv 2H^{(1-\varepsilon)/2}$ and

$$2H^{(1-\varepsilon)/2} \equiv W_{3\lambda}^2 - 2H^{(p-\varepsilon)/2} \equiv W_{3\lambda}^2 - 2\sigma H^{(1-\varepsilon)/2} \pmod{p} .$$

If $\sigma = -1$, then $p \mid W_{3\lambda}$ and since

$$W_n^2 + 3T_n^2 = 4H^n ,$$

$p \nmid T_{3\lambda}$. Now $p | W_\lambda X_\lambda Y_\lambda$ and the prime p can divide only one of W_λ, X_λ or Y_λ; for, if it divided any two of these it would divide the third. It follows that it would also divide R_λ, S_λ, and T_λ, which is impossible. If $p | W_\lambda$, then $p | T_{2\lambda}$ and $\eta = 0$; if $p | X_\lambda$, then $p | S_{2\lambda}$ and $\eta = 1$; if $p | Y_\lambda$, then $p | R_{2\lambda}$ and $\eta = 2$.

If $\sigma = 1$, then $p \nmid W_{3\lambda}$ and since $T_{6\lambda} \equiv 0 \pmod p$, we must have $p | T_{3\lambda}$; thus, $p | T_\lambda S_\lambda R_\lambda$. If $p | T_\lambda$, then $p | T_{2\lambda}$ and $\eta = 0$; if $p | S_\lambda$ then $p | R_{2\lambda}$ and $\eta = 2$; if $p | R_\lambda$, then $p | S_{2\lambda}$ and $\eta = 1$.

When p is a prime, $p \equiv 1 \pmod{12}$, and $(H | p) = 1$, we can obtain a further refinement of the results of Theorem 7. We first require

LEMMA 4. *If $p \equiv 1 \pmod{12}$, $\alpha = a + b\rho$, $p \nmid a^2 - ab + b^2$, $\pi_p = r + s\rho$ and $\tau = (as - br | p)$ (Legendre symbol), then in $Q(\rho)$*

$$\alpha^{(p-1)/2} \equiv \tau \pmod{\pi_p} .$$

Proof. The proof of this result is completely analogous to the proof given by Dirichlet [1] of a similar result concerning the value of $\alpha^{(p-1)/2} \pmod{\pi}$, when $\alpha, \pi \in Q(i)$, $i^2 = 1$.

THEOREM 8. *Let p be a prime such that $p \equiv 1 \pmod{12}$, $(H | p) = 1$, $\pi_p = r + s\rho$. If $\tau = (as - br | p)$, $\nu = \tau(H | p)_4$, and $\mu = (p - 1)/12$, then one and only one of W_μ, X_μ, Y_μ, R_μ, S_μ, T_μ is divisible by p and that one is given in the table below according to the value of ν and η.*

$\nu \backslash \eta$	0	1	2
-1	W_μ	Y_μ	X_μ
1	T_μ	S_μ	R_μ

Proof. Since $W_{(p-1)/2} = \alpha^{(p-1)/2} + \beta^{(p-1)/2}$ and $\alpha^{(p-1)2}\beta^{(p-1)/2} \equiv 1 \pmod p$, we see that $W_{(p-1)/2} \equiv 2\tau \pmod{\pi_p}$ and consequently $W_{(p-1)/2} \equiv 2\tau \pmod p$.

Now

$$W_{(p-1)/2} = W_{(p-1)/4}^2 - 2H^{(p-1)/4} ;$$

thus, $p | W_{3\mu}$ when $\nu = -1$ and $p | T_{3\mu}$ when $\nu = 1$.

The remainder of the theorem follows by using reasoning similar to that used in the proof of Theorem 7.

Using Theorem 7, we see that if $\eta \neq 0$, $\sigma = -1$, and if $(p - \varepsilon)/3$ has no prime divisors which are of the form $6t - 1$, then $\omega_1 = \omega_2/2$

when $\eta = 2$ and $\omega_2 = \omega_1/2$ when $\eta = 1$. For suppose $\eta = 2$, $\sigma = -1$ and $2\lambda = (p - \varepsilon)/3$. Since $Y_\lambda \equiv 0 \pmod p$ we see that $S_\lambda \not\equiv 0 \pmod p$ and $R_{2\lambda} \equiv 0 \pmod p$.
Hence

$$2\lambda = \omega_1(3k + 1) ,$$

or

$$2\lambda = \omega_2(6k - 1) , \qquad \text{where} \quad \omega_1 = 2\omega_2 .$$

Since no prime factor of the form $6t - 1$ divides λ, we must have

$$2\lambda = \omega_1(3k + 1) .$$

If $\omega_1 = 2\omega_2$, $\lambda = (3k + 1)\omega_2$ and $p \mid S_\lambda$ which is not so; thus, $\omega_1 = \omega_2/2$.

5. Primality testing and pseudoprimes. In this section we require the symbol $[A + B\rho \mid C + D\rho]$ of Williams and Holte [7]. In [7] it is shown how this symbol may be easily evaluated. It is also pointed out that if $C + D\rho$ is a prime of $Q(\rho)$, then $[A + B\rho \mid C + D\rho]$ is the cubic character of $A + B\rho$ modulo $C + D\rho$. We are now able to give the main result of this paper.

THEOREM 9. *Let* $N = 2^n 3^m A - 1$, *where* $n > 1$, A *is odd, and* $A < 2^{n+1}3^m - 1$. *If* $(H \mid N) = -1$ *(Jacobi symbol),* $[a + b\rho \mid N] = \rho^\eta$ $(\eta \neq 0)$, *then* N *is a prime if and only if*

$$X_L \equiv 0 \pmod N \qquad \textit{when} \quad \eta = 1$$

or

$$Y_L \equiv 0 \pmod N \qquad \textit{when} \quad \eta = 2 .$$

Here $L = (N + 1)/6$.

Proof. If N is a prime, $[a + b\rho \mid N]$ is the cubic character of αH modulo N; hence, $N \mid X_L$ when $\eta = 1$ and $N \mid Y_L$ when $\eta = 2$.

If $N \mid X_L$, then $N \mid T_{6L}$. If p is any prime divisor of T_{2L} or T_{3L}, then p must divide one of T_L, W_L, R_L, S_L. From the simple identities which relate R_k, S_k, T_k to W_k, X_k, Y_k, we see that if $p \mid X_L$, then p must divide two of R_L, S_L, and T_L, which is impossible; hence $(N, T_{2L}) = (N, T_{3L}) = 1$. Let p be any prime divisor of N and let $\omega = \omega(p)$. We have $\omega \mid 6L$ but $\omega \nmid 2L$ and $\omega \nmid 3L$; thus, $2^n \mid \omega$ and $3^m \mid \omega$. Since $\omega \mid p \pm 1$, we have

$$p = 2^n 3^m u \pm 1 .$$

Since $N = pS$ for some S, we have $S = 2^n 3^m v \pm 1$ and $A = 2^n 3^m uv \pm$

$(v - u)$. Now A is odd and $n > 1$; hence, one of u, v must be even and $A \geqq 2^{n+1}3^m - 1$, which is not possible; thus, N is a prime. Similarly, it can be shown that if $N \mid Y_L$, then N is a prime.

This criterion for the primality of N can be easily implemented on a computer by making use of the identities

$$\begin{aligned} R_{2k} &= -S_k(2R_k + S_k) \\ S_{2k} &= R_k(2S_k + R_k) \\ R_{k+1} &= aR_k + bS_k \\ S_{k+1} &= (a - b)S_k - bR_k \,. \end{aligned}$$

The values of a, b can be easily found by trial and then R_L, S_L determined modulo N by using the above identities in conjunction with a power technique such as that of Lehmer [3].

It is of some interest to determine whether there exist composite values of $N = 2^n3^mA - 1$ such that $A \geqq 2^{n+1}3^m - 1$, $[a + b\rho \mid N] = \rho^\eta$, $\eta \neq 0$, $(H \mid N) = -1$, and

$$X_L \equiv 0 \pmod N \qquad \text{when} \quad \eta = 1$$

or

$$Y_L \equiv 0 \pmod N \qquad \text{when} \quad \eta = 2 \quad (L = (N+1)/6) \,.$$

Such values of N can be considered as a type of pseudoprime. In fact, if $N \equiv -1 \pmod 3$, $[H(a + b\rho) \mid N] = \rho^\eta$, $\sigma = (H \mid N)$, we define N to be an *α-pseudoprime* to base $a + b\rho$ if it divides the appropriate entry of Table 1 with $\lambda = (N + 1)/6$. For example, if $\sigma = -1$, $\rho = 2$, N is an α-pseudoprime if

$$Y_{(N+1)/6} \equiv 0 \pmod N \,.$$

A systematic search of all composite α-pseudoprimes ($<10^6$) to base $2 + 3\rho$ produced the following:

$$\begin{aligned} &N = 5777 = 53 \cdot 109 && \eta = 1\,, && \sigma = 1\,, \\ &N = 31877 = 127 \cdot 251 && \eta = 0\,, && \sigma = -1\,, \\ &N = 513197 = 41 \cdot 12517 && \eta = 0\,, && \sigma = -1\,, \\ &N = 915983 = 47 \cdot 19489 && \eta = 1\,, && \sigma = 1\,. \end{aligned}$$

None of these has both $\sigma = -1$ and $\eta \neq 0$. Such α-pseudoprimes seem to be rather rare; however, they do exist. For example, let q, p_1, be primes such that $q \equiv 1 \pmod 3$, $p_1 = 6q - 1$ and select a, b such that $[a + b\rho \mid p_1] = \rho^2$ and $(H \mid p_1) = -1$. If p_2 is prime such that $p_2 \equiv 13 \pmod{36}$, $(p_2, p_1(2b - a)) = 1$ and $Y_q \equiv 0 \pmod{p_2}$, then $N = p_1p_2$ is an α-pseudoprime to base $a + b\rho$ and

$$N \mid X_{(N+1)/6} ,$$

$(N|H) = -1$, $[a + b\rho | N] = \rho$. To prove this we first note that $p_1 | Y_q$ and $p_2 | Y_q$; hence, $N | Y_q$. We also have $p_2 | R_{2q}$, $p_2 \nmid S_q$ and $p_2 \nmid R_2 = Y_1 S_1$; therefore, $\omega_1(p_2) = 2q$, $\omega_2(p_2) = 4q$ and $\omega(p_2) = 6q$. Since $\omega(p_2) | p_2 - 1$, we see that $12q | p_2 - 1$ and $(p_2 - 1)/12q \equiv 1 \pmod 3$; consequently, $R_{(p_2-1)/6} \equiv 0 \pmod{p_2}$, $(H|p_2) = +1$, and $[H(a + b\rho) | \pi_2] = \rho$. Now $p_1 p_2 + 1 \equiv 0 \pmod{6q}$ and $(p_1 p_2 + 1)/6q \equiv -1 \pmod 6$; hence,

$$X_{(p_1 p_2 + 1)/6} \equiv 0 \pmod{p_1 p_2} ,$$

$(H | p_1 p_2) = (H | p_1)(H | p_2) = -1$, and

$$\left[\frac{a + b\rho}{p_1 p_2}\right] = \left[\frac{a + b\rho}{p_1}\right]\left[\frac{H(a + b\rho)}{\pi_2}\right]\left[\frac{H(a + b\rho)}{\bar{\pi}_2}\right] = \left[\frac{(a + b\rho)^2(a + b\rho^2)}{\bar{\pi}_2}\right]$$
$$= \overline{\left[\frac{(a + b\rho^2)^2(a + b\rho)}{\pi_2}\right]} = \left[\frac{(a + b\rho)^2(a + b\rho^2)}{\pi_2}\right]^{-1} = \rho .$$

If we put $q = 5449$, $p_1 = 32693$, $a = 2$, $b = 3$, we have $(H | p_1) = -1$, $[a + b\rho | p_1] = \rho^2$. We also find that the prime 653881 divides Y_{5449}; hence, $N = 32693 \cdot 653881 = 21377331533$ is an α-pseudoprime to base $2 + 3\rho$ and $N | X_{(N+1)/6}$.

6. Acknowledgment. The author gratefully acknowledges the help of the referee in improving the presentation of this material and for correcting many typographical errors.

References

1. G. L. Dirichlet, *Demonstration d'une propriété analogue à la loi de réciprocité qui existe entre deux nombres premiers quelconques*, J. reine angew. Math., **9** (1832), 379–389.

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

3. ———, *Computer technology applied to the theory of numbers*, M.A.A. Studies in Mathematics, **6** (1969), 117–151.

4. P. M. MacMahon, *Combinatory Analysis*, Chelsea Publishing Co., New York, 1960.

5. H. Riesel, *Lucasian criteria for the primality of* $N = h \cdot 2^n - 1$, Math. Comp., **23** (1969), 869–875.

6. H. C. Williams, *The primality of* $N = 2A3^n - 1$, Canad. Math. Bull., **15** (1972), 585–589.

7. H. C. Williams and R. Holte, *Computation of the solution of* $x^3 + Dy^3 = 1$, Math. Comp., **31** (1977).

Received March 29, 1977 and in revised form November 21, 1977.

THE UNIVERSITY OF MANITOBA
WINNIPEG, CANADA R3T 2N2