SOME PROPERTIES OF A SPECIAL SET OF RECURRING SEQUENCES

HUGH C. WILLIAMS
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 $2^nA - 1$ ($A < 2^{n+1}3^n - 1$) 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 $2^n3^nA - 1$ to be prime when $A < 2^{n+1}3^n - 1$. 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

$$R_{n+1} = GR_{n+1} - HR_n,$$
$$S_{n+2} = GS_{n+1} - HS_n,$$
$$T_{n+2} = GT_{n+1} - HT_n.$$ (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
$U=(a^n-\beta^n)/(a-\beta)$; 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

$$R_{m+n} = R_m R_n - T_m T_n,$$
(2.1)
$$S_{m+n} = T_m T_n - S_m S_n,$$
$$T_{m+n} = S_m S_n - R_m R_n = T_m R_n - S_m T_n = R_m T_n - T_m S_n.$$

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

$$R_{2n} = -S_n(2R_n + S_n), \quad S_{2n} = R_n(2S_n + R_n),$$
$$T_{2n} = T_n(R_n - S_n);$$
(2.2)

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

$$R_{3n} = S_n^2 - 3S_n R_n^2 - R_n^3, \quad S_{3n} = R_n^3 - 3S_n^2 R_n - S_n^3,$$
$$T_{3n} = -3R_n S_n T_n = -(R_n^3 + S_n^3 + T_n^3).$$  (Use $-R_n^3 = (S_n + T_n)^3$.)

Since

$$H^* R_n = -S_n, \quad H^* S_n = -R_n, \quad H^* T_n = -T_n,$$

it follows that

$$H^* R_{n-m} = T_m T_n - S_m R_n, \quad H^* S_{n-m} = R_m S_n - T_m T_n,$$
$$H^* T_{n-m} = S_m R_n - R_m S_n = R_m T_n - T_m R_n = T_m S_n - R_m T_n.$$

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

(2.4)  $$T_n^2 - R_n S_n = R_n^2 - T_n S_n = S_n^2 - T_n R_n = H^*,$$
$$T_n^2 + R_n T_n + R_n^2 = R_n^2 + S_n R_n + S_n^2 = S_n^2 + T_n S_n + T_n^2 = H^*,$$
$$T_n S_n + S_n R_n + R_n T_n = -H^*.$$  

More generally, we have
We have

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

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

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

We also have

\[
R_{n+m}^2 - H^{2m}R_{n-m}^2 = T_{2m}S_{2m}, \hspace{1cm} S_{n+m}^2 - H^{2m}S_{n-m}^2 = T_{2m}R_{2m}, \\
T_{n+m}^2 - H^{2m}T_{n-m}^2 = T_{2m}T_{2n}.
\]

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

\[ R_n + S_n + T_n = 0, \hspace{1cm} R_nS_n + S_nT_n + R_nT_n = -H^n, \]

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

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

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

for \(m > 0\). From these we deduce the rather interesting identities

\[
R_n^4 + S_n^4 + T_n^4 = 2H^{2n}, \\
R_n^6 + S_n^6 + T_n^6 = 7H^{2n}R_nS_nT_n, \\
R_n^8 + S_n^8 + T_n^8 = 2H^{5n} + 15H^{2n}R_nS_n^2T_n, \\
R_nS_n^5 + R_n^5T_n + S_n^5T_n = 5H^{2n}R_nS_n^2T_n^2 - H^{2n}.
\]

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 \(R_n^i + S_n^i + T_n^i\) 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
\[ W_n + X_n + Y_n = 0 , \]
\[ 3R_n = W_n - Y_n , \quad 3S_n = X_n - W_n , \quad 3T_n = Y_n - X_n \]
\[ R_{2n} = S_n Y_n , \quad S_{2n} = R_n X_n , \quad T_{2n} = T_n W_n . \]

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
\[ W_{2n} = (W_n^2 + 2X_n Y_n)/3 = X_n Y_n + H^* = W_n^2 - 2H^n , \]
\[ Y_{2n} = (X_n^2 + 2W_n Y_n)/3 = W_n Y_n + H^* = X_n^2 - 2H^n , \]
\[ X_{2n} = (Y_n^2 + 2X_n W_n)/3 = W_n X_n + H^* = Y_n^2 - 2H^n , \]
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) \( a \not\equiv -b (\text{mod } 3) \).

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 \( p | R_1 \). If \( p | R_1 \) and \( p | H \), then \( R_0 = 1 \) and \( p | G \), which is impossible. In the same way we see that \( (S_n , H) = 1 \). Also, if \( p | (T_n , H) \), 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 a 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 $m/n = 1 \pmod{3}$, then $R_n \mid R_m$ and $S_n \mid S_m$; if $m/n = -1 \pmod{3}$, then $R_n \mid S_m$, $S_n \mid R_m$; if $m/n = 0 \pmod{3}$, then $R_n \mid T_m$, $S_n \mid T_m$.

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

$$R_{(3k \pm 1)n} = R_{3kn} R_{tn} - T_{3kn} T_{tn} \equiv R_{3kn} R_{tn} \pmod{R_n S_n}.$$  

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

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

$$T_1, T_2, T_3, \ldots, T_m,$$

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 $R_{\omega_1}$ and $S_{\omega_2}$ are respectively the first term of the sequences

$$\{R_k\}_{k=1}^\infty \text{ and } \{S_k\}_{k=1}^\infty$$

which $m$ 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 $\omega_1$ only; however, analogous results involving $S_n$ and $\omega$, for each of these are also true and their proofs are similar.

**Theorem 2.** If $(m, H) = 1$ and $\omega_1$ exists, then $\omega_2$ exists, $3 \mid \omega$, $\omega_1 = \omega_2$ or $2 \omega_3$, and $\omega_1 + \omega_2 = \omega$. 

Proof. Suppose \( \omega_1 \geq \omega \). We have

\[ \omega_1 = q\omega + r \quad (0 \leq r < \omega \leq \omega_1) \]

and

\[ 0 = R_{\omega_1} = R_{q_\omega}R_r - T_{q_\omega}T_r \equiv R_{q_\omega}R_r \pmod{m} . \]

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

\[ H^\omega S_{\omega-\omega_1} = S_\omega R_{\omega_1} - T_\omega T_{\omega_1} \equiv 0 \pmod{m} ; \]

thus, \( m \mid S_{\omega-\omega_1} \) and \( \omega_2 \leq \omega - \omega_1 < \omega \). Since as with \( \omega_1 \), \( m \mid T_{3\omega_2} \), 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 \( m \mid T_\omega \), 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 \( \omega_1 \) exists and either \( \omega_1 \mid n \) and \( n/\omega_1 \equiv 1 \pmod{3} \) or \( w_2 \mid n \), \( \omega_2 = \omega/2 \) and \( n/\omega_2 \equiv -1 \pmod{6} \).

**Proof.** Let \( n = 3\omega_1q + r \quad (0 \leq r < 3\omega_1) \); then

\[ 0 = R_n = R_{3\omega_1q}R_r - T_{3\omega_1q}T_r \equiv R_{3\omega_1q}R_r \pmod{m} \]

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 \( m \mid T_r \), we see that \( 3r = \omega \) or \( 2\omega \). 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 \( n/\omega_1 \equiv 1 \pmod{3} \).

**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 \( \omega, 2\omega, 4\omega, 5\omega \). If \( 3r = \omega \) or \( 4\omega \), then \( r = \omega_3 \) or \( 4\omega_3 \). 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 \( n/\omega_1 \equiv 1 \pmod{3} \); if \( r = \omega + \omega_1 \), then \( n = 3\omega_1q + \omega + \omega_1 = 6\omega_1q + 3\omega_2 + 2\omega_2 = (6q + 5)\omega_2 \).

**Corollary.** Under the conditions of Theorem 3, we must have \( n \equiv \omega_1 \pmod{3^{\nu+1}} \), where \( 3^{\nu} \mid \omega_1 \), \( \nu \geq 0 \).

**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 \( \omega_1(m) \equiv \omega_1(n) \pmod{3^{\nu+1}} \), where \( 3^{\nu} \mid \omega_1(m), \nu \geq 0 \).
Proof. Suppose \( \Omega = \omega_i(mn) \) exists; then clearly \( \omega_i = \omega_i(m) \) and \( \omega_i^* = \omega_i(n) \) exist and
\[
\begin{align*}
\Omega &\equiv \omega_i \pmod{3^{v+1}} \quad (3^v || \omega_i), \\
\Omega &\equiv \omega_i^* \pmod{3^{v^*+1}} \quad (3^{v^*} || \omega_i^*).
\end{align*}
\]
It follows that \( v = v^* \) and \( \omega_i = \omega_i^*(\pmod{3^{v+1}}) \).
If \( \omega_i \) and \( \omega_i^* \) exist and \( \omega_i \equiv \omega_i^*(\pmod{3^{v+1}}) \) (3^v || \omega_i), put \( \Omega = [\omega_i, \omega_i^*] \). We see that
\[
\frac{\Omega}{\omega_i} \equiv \frac{\Omega}{\omega_i^*} \not\equiv 0 \pmod{3}.
\]
If \( \Omega/\omega_i \equiv 1 \pmod{3} \), then \( R_\Omega \equiv 0 \pmod{mn} \); if \( \Omega/\omega \equiv -1 \pmod{3} \), then \( S_\Omega \equiv S_{2\Omega} \equiv 0 \pmod{mn} \). In either case we see that \( \omega_i(mn) \) must exist.

In order to continue our discussion of the existence of \( \omega_i(m) \) and \( \omega_i(m) \) it is necessary to consider the question of the existence of \( \omega_i(p^n), \omega_i(p^*) \), 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 \( p^i > 2 \), and \( p^i || T_n \) then \( p^{i+v} || T_{np^v} \); also, if \( p^i = 2 \) 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 \( 3^v || R_m \) when \( v \geq 1 \), then \( 3^v || R_{mn} \) when \( n \equiv 1 \pmod{3} \); otherwise, \( 3 \nmid R_{mn} \).

**Proof.** Certainly \( 3^v || R_m \) when \( n \equiv 1 \pmod{3} \) (Theorem 1); suppose \( 3^v+1 || R_m \). Now \( 3^{v+2} || T_{3m} \) and \( 3^{v+2} || T_{3m} \); hence, \( 3^{v+2} || T_{3m} = (T_{2m}, T_{3m}) \), which is impossible. If \( 3 | R_{mn} \) when \( n \equiv 1 \pmod{3} \), 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 \( p^i \neq 2 \) and \( p^i || R_m \), then \( p^{i+v} || R_{mp^v} \) when \( p^v \equiv 1 \pmod{3} \) and \( p^{i+v} || S_{mp^v} \) when \( p^v \equiv -1 \pmod{3} \). If \( p^i \neq 2 \) and \( p^i || S_m \), then \( p^{i+v} || S_{mp^v} \) when \( p^v \equiv -1 \pmod{3} \) and \( p^{i+v} || R_{mp^v} \) when \( p^v \equiv -1 \pmod{3} \). If \( 2 | R_m \), then \( 4 | S_m \); if \( 2 | S_m \), then \( 4 | R_{2m} \).

**Proof.** From the definitions of \( R_n \) and \( S_n \) it is easy to show that
\[
\begin{align*}
\rho^2 S_{mp} - \rho R_{mp} &= (\rho^2 S_m - \rho R_m)^p, \\
\rho S_{mp} - \rho^2 R_{mp} &= (\rho S_m - \rho^2 R_m)^p.
\end{align*}
\]
Suppose $p \neq 2$. If $p^i || R_m$, then
\[
\rho^2 S_{mp} - \rho R_{mp} \equiv \rho^2 p^2 S_m^2 - p \rho^{p-1} R_m S_{mp}^{-1} (\text{mod } p^{i+2}) ,
\]
\[
\rho S_{mp} - \rho^2 R_{mp} \equiv \rho^p S_m^2 - p \rho^{p+1} R_m S_{mp}^{-1} (\text{mod } p^{i+2}) ;
\]

therefore,
\[
R_{mp} \equiv p R_m S_{mp}^{-1} (\text{mod } p^{i+2}) \quad \text{when } p \equiv 1 \pmod{3}
\]
and
\[
S_{mp} \equiv p R_m S_{mp}^{-1} (\text{mod } p^{i+2}) \quad \text{when } p \equiv -1 \pmod{3} .
\]

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

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

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

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

**Proof.** We consider two possible cases.

**Case 1.** $\varepsilon = +1$. In this case $N(\pi) = p$,
\[
\alpha^p \equiv \alpha \pmod{p} , \quad \text{and} \quad (\alpha H)^{(p-1)/3} \equiv \rho^\gamma \pmod{\pi} ;
\]
hence,
\[ \alpha^{2(p-1)/3} \beta^{(p-1)/3} \equiv \rho^\eta \pmod{\pi} \]

and

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

The theorem follows easily from this result and the definition of \( R_\eta, S_\eta \) and \( T_\eta \).

**Case 2.** \( \varepsilon = -1 \). In this case \( N(\pi) = p^5, \alpha^p \equiv \beta \pmod{p}, \)

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

It follows that

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

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

\[ \omega_1 \equiv 2\gamma(p - \varepsilon)/3 \pmod{3^r} \]

\[ \omega_2 \equiv \gamma(p - \varepsilon)/3 \pmod{3^r} \]

where \( 3^r | p - \varepsilon \). 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 \( W_\lambda, X_\lambda, Y_\lambda, R_\lambda, S_\lambda, T_\lambda \) is divisible by \( p \) and that one is given in the table below according to the value of \( \sigma \) and \( \eta \).

<table>
<thead>
<tr>
<th>( \sigma )</th>
<th>( \eta )</th>
<th>0</th>
<th>1</th>
<th>2</th>
</tr>
</thead>
<tbody>
<tr>
<td>-1</td>
<td>( W_\lambda )</td>
<td>( X_\lambda )</td>
<td>( Y_\lambda )</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>( T_\lambda )</td>
<td>( R_\lambda )</td>
<td>( S_\lambda )</td>
<td></td>
</tr>
</tbody>
</table>

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

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

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

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

If \( \sigma = -1 \), then \( p | W_{3\lambda} \) and since
\[ W_n^2 + 3T_n^2 = 4H^4. \]

\( p \mid T_{3\lambda}. \) Now \( p \mid W_3X_3Y_3 \) and the prime \( p \) can divide only one of \( W_3, X_3 \) or \( Y_3; \) for, if it divided any two of these it would divide the third. It follows that it would also divide \( R_3, S_3, \) and \( T_3, \) which is impossible. If \( p \mid W_3, \) then \( p \mid T_{3\lambda} \) and \( \eta = 0; \) if \( p \mid X_3, \) then \( p \mid S_{3\lambda} \) and \( \eta = 1; \) if \( p \mid Y_3, \) then \( p \mid R_{3\lambda} \) and \( \eta = 2. \)

If \( \sigma = 1, \) then \( p \nmid W_{3\lambda} \) and since \( T_{3\lambda} \equiv 0 \pmod{p}, \) we must have \( p \mid T_{3\lambda}; \) thus, \( p \mid T_3S_3R_3. \) If \( p \mid T_3, \) then \( p \mid T_{3\lambda} \) and \( \eta = 0; \) if \( p \mid S_3 \) then \( p \mid R_{3\lambda} \) and \( \eta = 2; \) if \( p \mid R_3, \) then \( p \mid S_{3\lambda} \) and \( \eta = 1. \)

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

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

\[ \alpha^{(p-1)/2} \equiv \tau \pmod{\pi_\rho}. \]

**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 \( \alpha, \pi \in \mathbb{Q}(i), \) \( i^2 = 1. \)

**Theorem 8.** Let \( p \) be a prime such that \( p \equiv 1 \pmod{12}, \) \( (H \mid p) = 1, \) \( \pi_\rho = r + s\rho. \) If \( \tau = (as - br \mid p), \) \( \nu = \tau(H \mid p), \) and \( \mu = (p - 1)/12, \) then one and only one of \( W_\mu, X_\mu, Y_\mu, R_\mu, S_\mu, T_\mu \) is divisible by \( p \) and that one is given in the table below according to the value of \( \nu \) and \( \eta. \)

<table>
<thead>
<tr>
<th>( \nu )</th>
<th>( \eta )</th>
<th>( 0 )</th>
<th>( 1 )</th>
<th>( 2 )</th>
</tr>
</thead>
<tbody>
<tr>
<td>(-1)</td>
<td>( W_\mu )</td>
<td>( Y_\mu )</td>
<td>( X_\mu )</td>
<td></td>
</tr>
<tr>
<td>( 1)</td>
<td>( T_\mu )</td>
<td>( S_\mu )</td>
<td>( R_\mu )</td>
<td></td>
</tr>
</tbody>
</table>

**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 \( W_{(p-1)/2} \equiv 2\tau \pmod{\pi_\rho} \) and consequently \( W_{(p-1)/2} = 2\tau \pmod{p}. \)

Now

\[ W_{(p-1)/2} = W_{(p-1)/4}^2 - 2H^{(p-1)/4}; \]

thus, \( p \mid W_{3\mu} \) when \( \nu = -1 \) and \( p \mid T_{3\nu} \) 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 \( \omega_3 = \omega_3/2 \)
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 \( Y_1 \equiv 0 \pmod{p} \) we see that \( S_1 \not\equiv 0 \pmod{p} \) and \( R_{2} \equiv 0 \pmod{p} \).

Hence

\[
2\lambda = \omega_2(3k + 1),
\]

or

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

Since no prime factor of the form \( 6t - 1 \) divides \( \lambda \), we must have

\[
2\lambda = \omega_2(3k + 1).
\]

If \( \omega_1 = 2\omega_2 \), \( \lambda = (3k + 1)\omega_2 \) and \( p \mid S_1 \) which is not so; thus, \( \omega_1 = \omega_2/2 \).

5. Primality testing and pseudoprimes. In this section we require the symbol \( [A + B\rho | C + D\rho] \) 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 \( [A + B\rho | C + D\rho] \) 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 \( N = 2^n3^mA - 1 \), where \( n > 1 \), \( A \) is odd, and \( A < 2^{n+1}3^m - 1 \). If \( (H | N) = -1 \) (Jacobi symbol), \([a + b\rho | N] = \rho^\gamma \) (\( \gamma \neq 0 \)), then \( N \) is a prime if and only if

\[
X_L \equiv 0 \pmod{N} \quad \text{when} \quad \eta = 1
\]

or

\[
Y_L \equiv 0 \pmod{N} \quad \text{when} \quad \eta = 2.
\]

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

**Proof.** If \( N \) is a prime, \([a + b\rho | N]\) is the cubic character of \( \alpha H \) modulo \( N \); hence, \( N \mid X_L \) when \( \eta = 1 \) and \( N \mid Y_L \) when \( \eta = 2 \).

If \( N \mid X_L \), then \( N \mid T_{2L} \). 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, \( 2^\alpha \mid \omega \) and \( 3^\beta \mid \omega \). Since \( \omega \mid p \pm 1 \), we have

\[
p = 2^\alpha 3^\beta u \pm 1.
\]

Since \( N = pS \) for some \( S \), we have \( S = 2^\alpha 3^\beta v \pm 1 \) and \( A = 2^\alpha 3^\beta uv \pm
(v − u). Now A is odd and n > 1; hence, one of u, v must be even
and \( A \geq 2^{n+1}3^m - 1 \), which is not possible; thus, N is a prime.
Similarly, it can be shown that if \( N|Y_L \), 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

\[
\begin{align*}
R_{k+1} &= aR_k + bS_k \\
S_{k+1} &= (a - b)S_k - bR_k .
\end{align*}
\]

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 \( A \geq 2^n3^m - 1 \), \([a + b\rho|N] = \rho^\eta,\)
\( \eta \neq 0 \), \((H|N) = -1 \), and

\[
X_L \equiv 0 \pmod{N} \quad \text{when } \eta = 1
\]
or

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

Such values of \( N \) can be considered as a type of pseudoprime. In
fact, if \( N \equiv -1 \pmod{3} \), \([H(a + b\rho)|N] = \rho^\sigma, \ \sigma = (H|N) \), we define
\( N \) to be an \( \alpha \)-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 \( \alpha \)-pseudoprime if

\[
Y_{(N+1)/6} \equiv 0 \pmod{N} .
\]

A systematic search of all composite \( \alpha \)-pseudoprimes (<10⁶) to
base \( 2 + 3\rho \) produced the following:

\[
\begin{align*}
N = 5777 &= 53\cdot109 & \eta = 1, & \sigma = 1, \\
N = 31877 &= 127\cdot251 & \eta = 0, & \sigma = -1, \\
N = 513197 &= 41\cdot12517 & \eta = 0, & \sigma = -1, \\
N = 915983 &= 47\cdot19489 & \eta = 1, & \sigma = 1.
\end{align*}
\]

None of these has both \( \sigma = -1 \) and \( \eta \neq 0 \). Such \( \alpha \)-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 \([a + b\rho|p_1] = \rho^\sigma\) and \((H|p_1) = -1 \). 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 \( \alpha \)-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 \(p_1|\gamma_q\) and \(p_2|\gamma_q;\) hence, \(N|\gamma_q.\) We also have \(p_3|R_2, \ p_6 \perp S_q\) and \(p_7 \perp R_2 = \gamma_1 S_7;\) therefore, \(\omega(p_2) = 2q, \ \omega(p_6) = 4q\) and \(\omega(p_7) = 6q.\) Since \(\omega(p_2)|p_2 - 1,\) we see that \(12q|p_2 - 1\) and \((p_2 - 1)/12q = 1 (\text{mod} \ 3);\) consequently, \(R_{(p_2 + 1)/6} = 0 (\text{mod} \ p_2), \ (H|p_2) = +1,\) and \([H(a + b\rho)|\pi_2] = \rho.\) Now \(p_1 p_2 + 1 \equiv 0 (\text{mod} \ 6q)\) and \((p_1 p_2 + 1)/6q = -1 (\text{mod} \ 6);\) hence,

\[ X_{(p_1 p_2 + 1)/6} \equiv 0 (\text{mod} \ p_2), \]

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

\[
\begin{align*}
\left[\frac{a + b\rho}{p_1 p_2}\right] &= \left[\frac{a + b\rho}{p_1}\right] \left[\frac{H(a + b\rho)}{\pi_2}\right] \left[\frac{H(a + b\rho)}{\pi_2}\right] = \left[\frac{(a + b\rho)^{(a + b\rho)}}{\pi_2}\right] \\
&= \left[\frac{(a + b\rho)^{(a + b\rho)}}{\pi_2}\right] = \left[\frac{(a + b\rho)^{(a + b\rho)}}{\pi_2}\right] = \rho.
\end{align*}
\]

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 \(\alpha\)-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


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

THE UNIVERSITY OF MANITOBA
WINNIPEG, CANADA R3T 2N2
<table>
<thead>
<tr>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dan Amir, <em>Chebyshev centers and uniform convexity</em></td>
<td>1</td>
</tr>
<tr>
<td>Lawrence Wasson Baggett, <em>Representations of the Mautner group. I</em></td>
<td>7</td>
</tr>
<tr>
<td>George Benke, <em>Trigonometric approximation theory in compact totally disconnected groups</em></td>
<td>23</td>
</tr>
<tr>
<td>M. Bianchini, O. W. Paques and M. C. Zaine, <em>On the strong compact-ported topology for spaces of holomorphic mappings</em></td>
<td>33</td>
</tr>
<tr>
<td>Marilyn Breen, <em>Sets with ((d - 2))-dimensional kernels</em></td>
<td>51</td>
</tr>
<tr>
<td>J. L. Brenner and Allen Kenneth Charnow, <em>Free semigroups of (2 \times 2) matrices</em></td>
<td>57</td>
</tr>
<tr>
<td>David Bressoud, <em>A new family of partition identities</em></td>
<td>71</td>
</tr>
<tr>
<td>David Fleming Dawson, <em>Summability of matrix transforms of stretchings and subsequences</em></td>
<td>75</td>
</tr>
<tr>
<td>Harold George Diamond and Paul Erdős, <em>A measure of the nonmonotonicity of the Euler phi function</em></td>
<td>83</td>
</tr>
<tr>
<td>Gary Doyle Faulkner and Ronald Wesley Shonkwiler, <em>Kernel dilation in reproducing kernel Hilbert space and its application to moment problems</em></td>
<td>103</td>
</tr>
<tr>
<td>Jan Maksymilian Gronski, <em>Classification of closed sets of attainability in the plane</em></td>
<td>117</td>
</tr>
<tr>
<td>H. B. Hamilton and T. E. Nordahl, <em>Semigroups whose lattice of congruences is Boolean</em></td>
<td>131</td>
</tr>
<tr>
<td>Harvey Bayard Keynes and D. Newton, <em>Minimal ((G, \tau))-extensions</em></td>
<td>145</td>
</tr>
<tr>
<td>Anthony To-Ming Lau, <em>The Fourier-Stieltjes algebra of a topological semigroup with involution</em></td>
<td>165</td>
</tr>
<tr>
<td>B. C. Oltikar and Luis Ribes, <em>On prosupersolvable groups</em></td>
<td>183</td>
</tr>
<tr>
<td>Brian Lee Peterson, <em>Extensions of pro-affine algebraic groups</em></td>
<td>189</td>
</tr>
<tr>
<td>Thomas M. Phillips, <em>Primitive extensions of Aronszajn spaces</em></td>
<td>233</td>
</tr>
<tr>
<td>Mehdi Radjabalipour, <em>Equivalence of decomposable and 2-decomposable operators</em></td>
<td>243</td>
</tr>
<tr>
<td>M. Satyanarayana, <em>Naturally totally ordered semigroups</em></td>
<td>249</td>
</tr>
<tr>
<td>Fred Rex Sinal, <em>A homeomorphism classification of wildly imbedded two-spheres in (S^3)</em></td>
<td>255</td>
</tr>
<tr>
<td>Hugh C. Williams, <em>Some properties of a special set of recurring sequences</em></td>
<td>273</td>
</tr>
</tbody>
</table>