Effective Primality Tests for Some Integers of the Forms $A5^n - 1$ and $A7^n - 1$

By H. C. Williams*

To Daniel Shanks on the occasion of his 70th birthday

Abstract. It is shown how polynomial time prime tests, which are both fast and deterministic, can be developed for many numbers of the form $Ar^n - 1$ ($r = 5, 7; A < r^n$). These tests, like the Lucas-Lehmer test for the primality of the Mersenne numbers, are derived by using the properties of the Lucas functions. We exemplify these ideas by using numbers of the form $2 - 10^n - 1$.

1. Introduction. If $N$ is an integer of the form $2^n - 1$ ($n$ odd, $n > 2$), the Lucas-Lehmer test for the primality of $N$ may be given in terms of the following 3 steps:

1. Put $S_1 = 4$.
2. Define for $k \geq 1$
   \[ S_{k+1} = S_k^2 - 2 \pmod{N}. \]
3. $N$ is a prime if and only if
   \[ S_{n-1} \equiv 0 \pmod{N}. \]

This is an effective primality test for $N$ which executes in $O(\log N)$ operations.** In [7] Lehmer showed, by changing the value of $S_1$, that tests like this could be developed for numbers of the form $A2^n - 1$ whenever $A < 2^n$. The difficulties which arise when $3 \mid A$ have been discussed by Inkeri [5] and Riesel [10], [11].

Williams [13], [14] described $O(\log N)$ tests for the primality of integers of the form $A3^n - 1$ ($A < 3^n$). The test in [13] is effective for those values of $N$ for which we know a small prime $q$ such that $N$ is a cubic nonresidue of $q$. For certain values of $A$ such a $q$ is easy to find; for example, if $A = 4, 7, 8, 10, 11, 12 \pmod{13}$, then $q = 13$. In [12] Williams extended his ideas for $N = A3^n - 1$ to $N = Ar^n - 1$, where $r$ is an odd prime and $A < r^n$. However, in order for these tests, which again execute in $O(\log N)$ operations, to be effective, it is first necessary to have a small prime $q$ such that $N$ is an $r$th power nonresidue of $q$, and it is also necessary to have a solution $R$ of a certain polynomial congruence of degree $(r - 1)/2$. It was shown in [12] how this latter problem could be dealt with when $A$ is very small or

---

Received January 24, 1986; revised March 21, 1986.

1980 Mathematics Subject Classification. Primary 10A25, 10A35.

* Research supported by NSERC of Canada Grant #A7649.

** An operation here means addition, subtraction, multiplication or division of integers the size of $N$. 

©1987 American Mathematical Society

0025-5718/87 $1.00 + $.25 per page

385
when \( r = 5 \). In Williams [15] it was shown that for certain values of \( A \), when \( r = 7 \) or 11, an effective \( O(\log N) \) method could be developed to find \( R \). In all of these cases, however, when \( A \) is large it is first necessary to find \( R \), then employ it in the primality test.

In this paper we show how the tests for the primality of \( N = A5^n - 1 \) or \( A7^n - 1 \) for certain \( A \)-values can be made more efficient than those described earlier. We do this by first providing a noneffective \( O(\log N) \) primality test for \( N \). Should this test fail to determine whether or not \( N \) is a prime, it will still provide a value for \( R \), which can subsequently be used in an effective \( O(\log N) \) test for the primality of \( N \). In order to do this, we must first develop some simple properties of the Lucas functions and also show how the Lucas functions can be utilized in the problem of solving certain quadratic and cubic congruences.

As an example of our new tests, we mention here that by using the ideas of [12] it is possible to develop an effective \( O(\log N) \) test for the primality of integers of the form

\[
N = 2 \cdot 10^n - 1
\]

when \( n \) is odd (Zarnke and Williams [17]). By using the ideas presented here we are now able to provide an effective \( O(\log N) \) test for the primality of \( N \) when \( n \) is even and 138007919535942456000 does not divide \( n \).

2. Some Identity Properties of the Lucas Functions. Let \( P, Q \) be two coprime integers and let \( \alpha, \beta \) be the zeros of \( x^2 - Px + Q \). We define the Lucas functions \( V_n(P, Q), U_n(P, Q) \) \( (n \in \mathbb{Z}) \) by

\[
V_n(P, Q) = \alpha^n + \beta^n, \quad U_n(P, Q) = (\alpha^n - \beta^n)/(\alpha - \beta).
\]

Also, if we put \( \delta = \alpha - \beta \) and \( \Delta = \delta^2 \), we have \( \Delta = P^2 - 4Q \). (We assume here that \( \delta \neq 0 \).) When dealing with the Lucas functions modulo \( N \) it is sufficient to insist that \( \gcd(N, Q) = 1 \) rather than \( \gcd(P, Q) = 1 \).

There are many identities which are satisfied by the Lucas functions and, as we will need several of them in our later work, we present a number of these identities below. Unless there is some ambiguity concerning the values of the arguments \( P, Q \) of \( V_n(P, Q) \) and \( U_n(P, Q) \), we often omit them. The identities (2.1) to (2.5) below are well known and can be easily verified by using the definitions of \( V_n \) and \( U_n \).

\[
\begin{align*}
(2.1) \quad V_n^2 - \Delta U_n^2 &= 4Q^n, \\
(2.2) \quad V_{2n} &= V_n^2 - 2Q^n, \quad U_{2n} = V_n U_n, \\
(2.3) \quad V_{3n} &= V_n(V_n^2 - 3Q^n), \quad U_{3n} = U_n(V_n^2 - Q^n), \\
(2.4) \quad V_{m+n} &= V_m V_n - Q^n V_{m-n}, \quad U_{m+n} = V_n U_m - Q^n U_{m-n}, \\
(2.5) \quad 2V_{m+n} &= V_n V_m + \Delta U_n U_m, \quad 2U_{m+n} = U_n V_m + V_n U_m.
\end{align*}
\]

The identity (2.6) can also be verified by direct substitution.

\[
(2.6) \quad \delta \alpha^n U_m = V_n \alpha^m - Q^m V_{n-m}.
\]

If we define the Sylvester polynomial \( G_m(x) \) by \( G_{-1}(x) = -1, \ G_0(x) = 1, \) and \( G_{k+1}(x) = xG_k(x) - G_{k-1}(x) \) \( (k = 0, 1, 2, \ldots) \), then

\[
\frac{x^{2^k} + 1}{x - 1} = x^k G_s(x + x^{-1}).
\]
Also, \( G_s(-2) = (-1)^s \), and when \( 3 | s \), \( G_s(-1) = 1 \). If we put \( r = 2s + 1 \) and \( x = -(\alpha/\beta)^n \), we get

\[
V_{nr} = (-1)^s Q^n G_s(-V_{2n}/Q^n) V_n;
\]

if we put \( x = (\alpha/\beta)^n \), we get

\[
U_{nr} = Q^n G_s(V_{2n}/Q^n) U_n.
\]

These identities generalize the identities (2.3).

It is also convenient to have identities for \( V_{nr+k} \), \( U_{nr+k} \). Such identities may be obtained by using (2.6) to see that we must also have

\[
-\delta \beta^m U_m = V_n \beta^m - Q^m V_{n-m}.
\]

If we raise this identity and (2.6) to the odd power \( r \) and then multiply the first by \( \beta^k \) and the second by \( \alpha^k \), we get

\[
-\delta \beta^m U_m \beta^k = (V_n \beta^m - Q^m V_{n-m}) \beta^k,
\]
\[
\delta \alpha^m U_m \alpha^k = (V_n \alpha^m - Q^m V_{n-m}) \alpha^k.
\]

If we subtract these, expand by the binomial theorem, and use the fact that \( U_{m+j+k} = (\alpha^m \beta^k + \beta^m \alpha^k) / \delta \), we get

\[
\Delta^{(r-1)/2} V_{nr+k} U_m = \sum_{j=0}^{r} \binom{r}{j} (-1)^{r-j} Q^{m(r-j)} V_n V_{n-m} U_{m+j+k}
\]

for odd \( r \). If we had added the two identities above we would get a similar identity for \( \Delta^{(r+1)/2} U_{nr+k} U_m \). If \( r \) is even, we can also get identities for \( \Delta^{(r+1)/2} V_{nr+k} U_m \) and \( \Delta^{(r+1)/2} U_{nr+k} V_m \). None of these identities, in spite of the ease by which they may be derived, seems to occur in the extensive literature on the Lucas functions. They are similar to identities discovered by Siebeck (see [3, p. 394]), Jarden and Motzkin (see [6, pp. 79–80]), Halton [4], and Carlitz and Ferns [2].

To compute \( V_n \) (and \( U_n \)) \((\text{mod} \ N)\) for large values of \( n \), it is convenient to introduce the function

\[
W_m = V_{2m} Q^{-m} \pmod{N}.
\]

(We assume here that \( \gcd(Q, N) = 1 \).) If we replace \( n \) by \( 2n \) and \( m \) by \( 2m \) in (2.2) and (2.4), we get

\[
W_{2n} = W_n^2 - 2 \pmod{N}
\]

and

\[
W_{m+n} = W_m W_n - W_{m-n} \pmod{N}.
\]

If we put \( m = n + 1 \) in (2.11), we get

\[
W_{2n+1} = W_n W_{n+1} - W_1 \pmod{N},
\]

where

\[
W_1 = P^2 Q^{-1} - 2 \pmod{N}.
\]

Now let \((b_0 b_1 b_2 \cdots b_t)_2\) be the binary representation of \( m \), where \( b_0 = 1 \), \( b_i = 0 \) or \( 1 \) when \( i = 1, 2, 3, \ldots, t \), and \( t = \lfloor \log_2 m \rfloor \). Using the notation \( \{ A, B \} \equiv \{ C, D \} \pmod{N} \) to mean \( A \equiv C, B \equiv D \pmod{N} \), set \( \mathcal{P}_0 = \{ W_1, W_2 \} \pmod{N} \) and deduce \( \mathcal{P}_{i+1} \) from \( \mathcal{P}_i = \{ A, B \} \pmod{N} \) by

\[
\mathcal{P}_{i+1} \equiv \begin{cases} 
\{ A^2 - 2, AB - W_1 \} \pmod{N} & \text{when } b_{i+1} = 0, \\
\{ AB - W_1, B^2 - 2 \} \pmod{N} & \text{when } b_{i+1} = 1.
\end{cases}
\]
From (2.10) and (2.12) it is clear that
\[ \mathcal{P}_i \equiv \{ W_m, W_{m+1} \} \pmod{N}. \]

This furnishes us with a computationally efficient method for computing the values of \( W_m \) and \( W_{m+1} \pmod{N} \).

We have already seen that some identities like (2.2) and (2.4) simplify when converted to congruences involving the \( W \)-functions. We should also point out here that (2.7) becomes

\[ (2.13) \quad W_{nr} \equiv (-1)^s G_s (-W_{2n}) W_n \pmod{N}. \]

Also, by putting \( m = 2n + 1 \) and \( n = 1 \) in (2.4), we get

\[ (2.14) \quad PV_{2n+1}Q^{-n} \equiv Q(W_{n+1} + W_n) \pmod{N}. \]

If we put \( n = 1 \) and \( m = 2n + 1 \) in (2.5) and (2.4), we get

\[ (2.15) \quad \Delta U_{2n+1}Q^{-n} \equiv Q(W_{n+1} - W_n) \pmod{N}. \]

If we put \( m = 2n \) and \( n = 2 \) in (2.5), we also have

\[ (2.16) \quad PDU_{2n}Q^{-n} \equiv 2QW_{n+1} - (P^2 - 2Q)W_n \pmod{N}. \]

Finally, on putting \( r = 3, k = -4, m = 2 \) in (2.9), we get

\[ P^2V_{3n-4} = V_n^3 - 3Q^2V_nV_{n-2}^2 + Q^2(P^2 - 2Q)V_{n-2}^3, \]

and if we put \( n = 2m + 2 \), we get

\[ (2.17) \quad P^2W_{3m+1} \equiv Q^2W_m^3 - 3Q^2W_{m+1}W_m^2 + Q(P^2 - 2Q)W_m^3 \pmod{N}. \]

3. Some Number-Theoretic Properties of the Lucas Functions. Let \( p \) be an odd prime such that \( p \nmid \Delta Q \) and let \( \epsilon, \eta \) equal the values of the Legendre symbols \( (\Delta/p) \) and \( (Q/p) \), respectively. It is well known that

\[ (3.1) \quad V_{p^{-\epsilon}} = 2Q^{(1-\epsilon)/2}, \quad U_{p^{-\epsilon}} = 0 \pmod{p}. \]

Further, in [7] Lehmer proves

**Theorem 3.1.** If \( p \nmid \Delta Q \), then \( p \nmid U_{(p^{-\epsilon})/2} \) if and only if \( \eta = -1 \). □

By using this result, Lehmer essentially proves

**Theorem 3.2.** Let \( N = A2^n - 1 \), where \( A < 2^n \). If the Jacobi symbols \( (\Delta/N) = (Q/N) = -1 \), then \( N \) is a prime if and only if

\[ V_{(N+1)/2}(P, Q) \equiv 0 \pmod{N}. \] □

For example, if we put \( P = 2, Q = -2 \), then \( \Delta = 12 \) and \( (\Delta/N) = (Q/N) = -1 \) when \( N = 2^n - 1 \) \((n \geq 2)\). Hence, \( -W_1 = 4 \), and if \( S_1 = -W_1 \), we have \( S_k \equiv W_{2k} \pmod{N} \) by (2.10) and

\[ S_{n-1} \equiv W_{(N+1)/4} \equiv V_{(N+1)/2}Q^{-\frac{(N+1)/2}{2}} \pmod{N}. \]

Thus, \( N \mid S_{n-1} \) if and only if \( N \mid V_{(N+1)/2} \) and we have the Lucas-Lehmer test for the primality of Mersenne numbers.

By using the results in [12] and [15] we can also prove the following sufficiency test for the primality of numbers of the form \( Ar^n - 1 \) \((A < r^n)\).
THEOREM 3.3. Let \( N = A r^n - 1 \) \((A < r^n)\), where \( r \) is an odd prime. If \((\Delta/N) = -1\) and
\[
G_s \left( W_{(N+1)/2r} \right) \equiv 0 \pmod{N},
\]
where \( s = (r - 1)/2 \), then \( N \) is a prime. \( \Box \)

In order to convert this into a necessary and sufficient primality test, we need to derive a theorem like Theorem 3.1. In [12] and [16] it is shown that if \( q \) is a prime such that \( q \equiv 1 \pmod{r} \), and \( p \) is a prime such that \( p \equiv -1 \pmod{r} \) and
\[
p^{(q-1)/r} \not\equiv 1 \pmod{q},
\]
then we can compute \( s = (r - 1)/2 \) coefficients \( C(i, r, q), \) \( i = 0, 1, 2, \ldots, s - 1 \), independently of \( p \), such that the following theorem holds.

**THEOREM 3.4.** Let \( R \) be any integer such that
\[
G_s(R) \equiv 0 \pmod{p}.
\]
If
\[
P \equiv \sum_{i=0}^{s-1} C(i, r, q) R^i, \quad Q \equiv q^{r-2} \pmod{p},
\]
then
\[
G_s \left( W_{(P+1)/2r} \right) \equiv 0 \pmod{p}. \quad \Box
\]

Notice that Theorem 3.4 is somewhat similar to Theorem 3.1 in that we can specify in advance \( P, Q \) such that \( U_{(P+1)/r}(P, Q) \not\equiv 0 \pmod{p} \). By using Theorem 3.4 we can easily deduce the following result from Theorem 3.3.

**THEOREM 3.5.** Let \( N = Ar^n - 1 \), where \( A < r^n, 2 \mid A \), and suppose that \( q \) is a prime such that \( q \equiv 1 \pmod{r} \) and
\[
N^{(q-1)/r} \not\equiv 0, 1 \pmod{q}.
\]
If \( R \) is any integer such that
\[
G_s(R) \equiv 0 \pmod{N}
\]
and
\[
P \equiv \sum_{i=0}^{s-1} C(i, r, q) R^i, \quad Q \equiv q^{r-2} \pmod{N},
\]
then \( N \) is a prime if and only if
\[
G_s \left( W_{(N+1)/2r} \right) \equiv 0 \pmod{N}. \quad \Box
\]

Thus, in order to make this an effective primality test, we need to be able to determine \( q, C(i, r, q) \) \((i = 0, 1, 2, \ldots, s - 1)\), and \( R \). In Section 5 we discuss how \( q \) can be determined for certain values of \( A \), and we give some tables of \( C(i, r, q) \) for \( r = 5 \) and 7.

In many cases we can find a value for \( R \) by performing the sufficiency test given as Theorem 3.3. Before we indicate how this may be done, we need
Lemma 3.1. Let $p$ be an odd prime such that $p \nmid \Delta Q$. If $c = 1$ or $2$, $m$ is any odd divisor of $p - 1$, and $t = (p - t)/m$, then $U_{ct} \equiv 0 \pmod{p}$ if and only if $V_{ct} \equiv 2\eta^tQ^{t/2} \pmod{p}$.

Proof. By (2.1) it is clear that $p | U_{ct}$ when $V_{ct} \equiv 2\eta^tQ^{t/2} \pmod{p}$.

If $U_{ct} \equiv 0 \pmod{p}$, by (2.2) we have $U_t \equiv 0 \pmod{p}$ or, possibly in the case of $c = 2$, $V_q \equiv 0 \pmod{p}$. Suppose $U_t \equiv 0 \pmod{p}$. By (2.1) we must have $V_t \equiv 2\theta Q^{t/2} \pmod{p}$, where $\theta = \pm 1$; hence $V_{2t} \equiv 2Q^t \pmod{p}$. Since $G_k(-2) = (-1)^k$ and by (2.7)

$$V_{mt} \equiv (-1)^k Q^{k/2} G_k(-2) V_t \pmod{p},$$

where $k = (m - 1)/2$, we have $V_{mt} \equiv 2\theta Q^{m/2} \equiv 2Q^{(t-r)/2} \pmod{p}$ by (3.1). It follows that $\theta = \eta$.

If $c = 2$ and $V_t \equiv 0 \pmod{p}$, then $V_{2t} \equiv -2Q^t \pmod{p}$. Now by (3.1) and (2.8),

$$0 = U_{p-\varepsilon} = U_{im} = Q^{k/2} G_k(V_{2t}/Q^t)U_t \pmod{p};$$

thus, $U_t \equiv 0 \pmod{p}$. However, by (2.1) we see that we cannot have both $U_t \equiv 0 \pmod{p}$ and $V_t \equiv 0 \pmod{p}$.

Now if $N = Ar^n - 1$ is a prime, $P, Q$ are chosen such that $(\Delta/N) = -1$, $\eta = (Q/N) \neq 0$ and $V_{cA} \neq 2(Q/N)A^{c/2} \pmod{N}$, then by (2.1) we have $U_{cA} \neq 0 \pmod{N}$ and by (3.1) and (2.2), $U_{cA^m} \equiv 0 \pmod{N}$. It follows that there must be a minimal $m (0 \leq m < n)$ such that $U_{cA^m} \neq 0 \pmod{N}$ and $U_{cA^{m+1}} \equiv 0 \pmod{N}$.

By (2.8) we must have

$$G_k(V_{2cA^m}Q^{-cA^m}) \equiv 0 \pmod{N} \quad (m < n).$$

Further, if (3.2) holds, then by (2.8) and Lemma 3.1 we have

$$W_{cA^{m+1/2}} \equiv 2\eta^c \pmod{N} \quad (m < n).$$

On the other hand, if $m$ is the least nonnegative integer such that (3.3) holds, then

$$U_{cA^{m+1}} \equiv 0 \pmod{N}.$$

By (2.8) this means that either (3.2) holds or $N | U_{cA^m}$. If $N | U_{cA^m}$, then by Lemma 3.1 we get $W_{cA^{m+1/2}} \equiv 2\eta^c \pmod{N}$, which contradicts the minimality of $m$. Thus, if $m$ is the least nonnegative integer for which (3.3) holds, then $m$ is the least nonnegative integer for which (3.2) holds.

Under the assumption, then, that $N$ is a prime, we can find a value for $R$ by attempting to use our sufficiency test for the primality of $N$. Our only problem here is our assumption that $V_{cA} \neq 2(Q/N)A^{c/2} \pmod{N}$. We can certainly select $P, Q$ to ensure that this will not happen when $A$ is very small, but for larger values of $A$ we have no a priori method for doing this. In Sections 4 and 6 we will show how, for certain values of $A$, when $r = 5$ or $7$, we can, under the assumption that $N$ is a prime, find a value for $R$, even when $A$ is large. Also we will deduce this $R$-value from an attempt to use our sufficiency test to prove $N$ a prime.

4. Solution of Quadratic and Cubic Congruences. In order to find $R$ when $r = 5$ or $7$, we must be able to solve $G_2(x) \equiv 0 \pmod{N}$ or $G_3(x) \equiv 0 \pmod{N}$. Now $G_2(x) = x^2 + x - 1$ and $G_3(x) = x^3 + x^2 - 2x - 1$; hence, we must develop methods involving Lucas functions for solving quadratic and cubic congruences.
modulo \( N \). Since we may assume that \( N \) is a prime, we will first discuss the solution of
\[
(4.1) \quad x^2 \equiv a \pmod{p},
\]
where \( p \) is a prime and \( (a/p) = 1 \). We will divide our discussion into two cases, depending on the congruence class of \( p \) modulo 4.

If \( p \equiv -1 \pmod{4} \), then \( x \equiv a^{(p+1)/2} \) is certainly a solution of (4.1); however, the problem of testing \( N \) for primality and deducing \( a^{(N+1)/4} \pmod{N} \) are not usually related (but see the remarks in Section 6). What we wish to do here is find a method for solving
\[
x^2 \equiv a \pmod{N},
\]
which we can integrate into a single sufficiency test for the primality of \( N \). This means that we must use the Lucas functions to solve (4.1), and, specifically, Lucas functions such that \( (a/p) = -1 \). In fact, since the computation of \( W_m \) can be done efficiently, we will attempt to solve (4.1) by making use of these \( W \)-functions.

Let \( (\Delta/p) = (Q/p) = -1 \). We have
\[
V_{(p+1)/2} \equiv 0 \pmod{p}
\]
by (3.1), Theorem 3.1, and (2.2). Thus, we may assume that there exists a \( k \) such that
\[
V_{2k} \equiv 0 \pmod{p}.
\]
By (2.1) we must have
\[
-\Delta U_{2k}^2 \equiv 4Q^{2k} \pmod{p} \quad \text{and} \quad (2^{-1}\Delta U_{2k}Q^{-k})^2 \equiv -\Delta \pmod{p}.
\]
Since \( V_{2k} \equiv 0 \pmod{p} \), we have \( W_k \equiv 0 \pmod{p} \); hence, by (2.16), we have
\[
\Delta U_{2k}Q^{-k} \equiv 2QW_{k+1}P^{-1} \pmod{p}.
\]
Thus, if we find \( P, Q \) such that \( \Delta = P^2 - 4Q \equiv -a \pmod{p} \) and \( (Q/p) = -1 \), then
\[
x \equiv P^{-1}QW_{k+1} \pmod{p}
\]
is a solution of (4.1).

For the case under consideration here we put \( a = 20Y^2, P = 2X, Q = X^2 + 5Y^2 \), where \( (X^2 + 5Y^2/p) = -1 \). We see that
\[
x \equiv (4XY)^{-1}(X^2 + 5Y^2)W_{k+1} \pmod{p}
\]
is a solution of
\[
(4.2) \quad x^2 \equiv 5 \pmod{p}.
\]
Hence \( y \equiv (-1 + x)2^{-1} \pmod{p} \) is a solution of \( G_2(y) \equiv 0 \pmod{p} \).

If \( p \equiv 3 \pmod{8} \) and \( (\Delta/p) = -1, (Q/p) = 1 \), then \( U_{(p+1)/2} \equiv 0 \pmod{p} \), and there must exist some odd \( t = 2k + 1 \) such that
\[
U_{2t} \equiv 0 \pmod{p}.
\]
By (2.2), this means that either \( p \mid V_t \) or \( p \mid U_t \). If \( p \mid U_t \), then by (2.1) we have
\[
(2^{-1}Q^{-k}U_{2k+1}^2) \equiv Q \pmod{p};
\]
if \( p \mid V_t \), then
\[
-\Delta(2^{-1}Q^{-k}U_{2k+1}^2) \equiv Q \pmod{p}.
\]
Thus, if we can find $X$, $Y$ such that $a = X^2 + Y^2$, we can put $P = 2X$, $Q = X^2 + Y^2$, $\Delta = -4Y^2$. It follows from (2.14) and (2.15) that we either have

$$x \equiv (4X)^{-1}(X^2 + Y^2)(W_{k+1} + W_k) \pmod{p}$$

or

$$x \equiv (4Y)^{-1}(X^2 + Y^2)(W_{k+1} - W_k) \pmod{p}$$

as a solution of (4.1). If $a = 5$, we can put $X = 1$, $Y = 2$, $P = 4$, $Q = 5$, and $\Delta = -16$.

The problem of solving (4.1) when $p \equiv 1 \pmod{4}$ by using Lucas functions has been discussed by Cipolla (see [3, p. 218]) and Lehmer [8]. If, as in [3], we put $a = Q$ and select $P$ such that $(\Delta/p) = -1$ and $(Q/p) = +1$, then

$$V_{(p+1)/2} \equiv 0 \pmod{p}.$$ 

Thus, there must exist some $k$ such that

$$V_{2k+1}^2 \equiv 4Q^{2k+1} \pmod{p}.$$ 

By (2.14),

$$x \equiv (2P)^{-1}Q(W_{k+1} + W_k) \pmod{p}$$

is a solution of (4.1). If we find $X$ and $Y$ such that $(X^2 - 5Y^2/p) = -1$ and put $P = 2X$, $Q = 5Y^2$, we find that

$$x \equiv 5Y(4X)^{-1}(W_{k+1} + W_k) \pmod{p}$$

is a solution of (4.2).

Of course, in the cases of $p \equiv -1 \pmod{8}$ and $p \equiv 1 \pmod{4}$, we must search for $X$ and $Y$; and, as a consequence of this, we see that these algorithms are not effective. However, for many numbers it is easy to find such an $X$ and $Y$. We discuss this problem at greater length in Section 5.

For our discussion of the cubic congruence modulo $p$ we will assume that $p > 3$, $p \nmid a$ and that we wish to solve

$$x^3 - ax + b \equiv 0 \pmod{p}$$

when such a congruence has a solution. Cailler [1] gave a method which utilized the Lucas functions for solving (4.3); however, he obtained his solution as a ratio of two of the $U$-functions. We will instead obtain a solution, when possible, in terms of the $W$-functions. As does Cailler, we first note that if $Q \equiv 3^{-1}a$, $P \equiv 3ba^{-1} \pmod{p}$ and $y$ is a solution of (4.3), then if $p \nmid \Delta$, we get

$$z^3 \equiv a/\beta \pmod{p},$$

when

$$z \equiv (y - \alpha)/(y - \beta) \pmod{p}.$$ 

It follows that, since $z^{p-\epsilon} \equiv 1 \pmod{p}$, we have

$$p \mid U_{(p-\epsilon)/3}(P, Q).$$

Thus we may assume the existence of some $t$ such that $t \mid (p - \epsilon)/3$ and $U_t \equiv 0 \pmod{p}$. Suppose further that $3 \nmid t$ (this is certainly the case if $p \neq \epsilon \pmod{9}$) and that $(p - \epsilon)/3t$ is odd. We have $V_t \equiv 2\eta Q^{t/2} \pmod{p}$ by Lemma 3.1. We now
select \( c \) such that \( 3 \mid ct + 1 \) \((c = 1 \text{ or } 2)\) and note that

\[
V_{ct} = 2\eta^c Q^{ct}/2 \quad \text{and} \quad U_{ct} \equiv 0 \pmod{p}.
\]

Thus, by (2.5), we have

\[
2V_{ct+1} \equiv V_{ct}V_1 + \Delta U_{ct}U_1 \equiv 2\eta^c Q^{ct}/2 \pmod{p}.
\]

If we put \( k = (ct + 1)/3 \), we get

\[
\eta^c PQ^{ct}/2 \equiv V_k^3 - 3Q^k V_k \pmod{p}
\]

from (4.4) and (2.3). Since \( 2 \mid t \), we must have \( k = 2m + 1 \), and we get

\[
(V_k Q^{-m})^3 - 3Q(V_k Q^{-m}) \equiv \eta^c PQ \pmod{p}
\]

or

\[
(-\eta^c V_k Q^{-m})^3 - a(-\eta^c V_k Q^{-m}) + b \equiv 0 \pmod{p}.
\]

By using (2.14), we see that

\[
x \equiv -\eta^c P^{-1}Q(W_{m+1} + W_m) \pmod{p}
\]

is a solution of (4.3).

We emphasize here that we have not solved the general cubic congruence by this technique. We needed here that \( p \not\equiv a \) and \( 3 \not\mid t \), conditions that do not occur for every cubic congruence; nevertheless, for our immediate problem this technique works in many cases. If we put \( y = 3x + 1 \) in

\[
G_3(x) \equiv 0 \pmod{p},
\]

we get

\[
y^3 - 21y - 7 \equiv 0 \pmod{p},
\]

and we can put \( Q = 7, \ P = -1, \ \Delta = -27 \). We have \( \varepsilon = (-3/p) \), and a solution of (4.5) is given by

\[
x \equiv (-1 + \eta^c 7(W_{m+1} + W_m))3^{-1} \pmod{p}.
\]

whenever \( 3 \not\equiv (p - \varepsilon)/3 \). This is a more general result than that obtained by a different technique in [15] for the case of \( r = 7 \).

5. Determination of \( q, X \) and \( Y \). When \( N = Ar^n - 1 \) we need to be able to find a small prime \( q \) such that \( q \equiv 1 \pmod{r} \) and

\[
N^{(q^{-1})/r} \not\equiv 0, 1 \pmod{q}.
\]

In general, this appears to be a difficult problem; however, in many cases it is not at all difficult to find a suitable \( q \). We will consider this problem from the point of view of asking for a given \( r \) and \( q \), what values of \( A \) exist such that (5.1) holds for any \( n \). For example, if \( N = A5^n - 1 \), and \( q = 11 \), then, if \( A \equiv 3 \pmod{11} \), (5.1) holds for any value of \( n \).

Let \( \mathcal{S}(u, r, q) \) be the set of those values of \( A \pmod{q} \) such that

\[
(Au^n - 1)^{(q^{-1})/r} \not\equiv 1, 0 \pmod{q}
\]

for any \( n \), and set \( L(u, r, q) = |\mathcal{S}(u, r, q)| \). If \( g \) is a fixed primitive root of \( q \), \( A \equiv g^u \pmod{q} \) and \( u \equiv g^i \pmod{q} \), in order to determine \( L(u, r, q) \) we wish to count those values of \( a \pmod{q-1} \) such that for all \( n \) there exists some \( i \) where
0 < i < q - 1 and

\[ g^{a + nj} - 1 \equiv g^{rh + i} \pmod{q}. \tag{5.2} \]

Notice that if \( k = \gcd(j, q - 1) \), we can replace (5.2) by

\[ g^{a + nk} \equiv g^{rh + i} + 1 \pmod{q}. \tag{5.3} \]

Also, \( v = (q - 1)/k \) is the least \( t (> 0) \) such that

\[ u^t \equiv 1 \pmod{q}. \]

If there does exist an \( n \) with \( i = 0 \), such that (5.3) holds, we have

\[ A = g^a \equiv (g^{rh} + 1)g^{-nk} \pmod{q}. \tag{5.4} \]

Since \( g^{rh} + 1 \) will generate \((q - 1)/r \) distinct values \( \pmod{q} \), we see that \( L(u, r, q) \) > 0 whenever \( v \leq r \). Also, (5.3) holds when we replace \( a \) by \( a + kt \) \( (t = 0, 2, 3, \ldots, v - 1) \) and \( n \) by \( n - t \), hence \( \nu | L(u, r, q) \).

By using (5.4) it is a simple matter to compute \( \mathcal{S}(u, r, q) \) as the set of those integers \( \pmod{q} \) which do not have any representation of the form

\[ (g^{rh} + 1)g^{-nk}, \]

where \( h = 0, 1, 2, \ldots, (q - 1)/r - 1 \) and \( n = 0, 2, 3, \ldots, v - 1 \). For further information on the problem of computing numbers like \( L(u, r, q) \), we refer the reader to Lehmer and Vandiver [9].

We give in Table 1 below for \((u, r) = (5, 5), (7, 7), (10, 5)\), the values of \( \nu(u, r, q) \) and \( L(u, r, q) \) when \( L(u, r, q) \neq 0 \) and \( q \leq 15000 \). Note that there are many instances of \( L(u, r, q) > 0 \) when \( v > r \). In Tables 2 and 3 we give the elements in selected sets \( \mathcal{S}(u, r, q) \).

**Table 1**

<table>
<thead>
<tr>
<th>( u )</th>
<th>( r )</th>
<th>( \nu(u, r, q) )</th>
<th>( L(u, r, q) )</th>
<th>( u )</th>
<th>( r )</th>
<th>( \nu(u, r, q) )</th>
<th>( L(u, r, q) )</th>
<th>( u )</th>
<th>( r )</th>
<th>( \nu(u, r, q) )</th>
<th>( L(u, r, q) )</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>5</td>
<td>11</td>
<td>5</td>
<td>2</td>
<td>8</td>
<td>11</td>
<td>2</td>
<td>10</td>
<td>29</td>
<td>7</td>
<td>7</td>
</tr>
<tr>
<td>31</td>
<td>3</td>
<td>18</td>
<td>41</td>
<td>5</td>
<td>10</td>
<td>281</td>
<td>20</td>
<td>20</td>
<td>281</td>
<td>20</td>
<td>20</td>
</tr>
<tr>
<td>71</td>
<td>5</td>
<td>20</td>
<td>101</td>
<td>4</td>
<td>40</td>
<td>2801</td>
<td>5</td>
<td>20</td>
<td>2801</td>
<td>5</td>
<td>20</td>
</tr>
<tr>
<td>191</td>
<td>19</td>
<td>19</td>
<td>271</td>
<td>5</td>
<td>90</td>
<td>2801</td>
<td>5</td>
<td>20</td>
<td>2801</td>
<td>5</td>
<td>20</td>
</tr>
<tr>
<td>521</td>
<td>10</td>
<td>70</td>
<td>3541</td>
<td>20</td>
<td>40</td>
<td>2801</td>
<td>5</td>
<td>20</td>
<td>2801</td>
<td>5</td>
<td>20</td>
</tr>
<tr>
<td>601</td>
<td>12</td>
<td>36</td>
<td>7841</td>
<td>56</td>
<td>56</td>
<td>2801</td>
<td>5</td>
<td>20</td>
<td>2801</td>
<td>5</td>
<td>20</td>
</tr>
<tr>
<td>1741</td>
<td>15</td>
<td>75</td>
<td>9091</td>
<td>10</td>
<td>900</td>
<td>4733</td>
<td>7</td>
<td>1554</td>
<td>4733</td>
<td>7</td>
<td>1554</td>
</tr>
<tr>
<td>6271</td>
<td>19</td>
<td>76</td>
<td>9901</td>
<td>12</td>
<td>816</td>
<td>4733</td>
<td>7</td>
<td>1554</td>
<td>4733</td>
<td>7</td>
<td>1554</td>
</tr>
<tr>
<td>8971</td>
<td>23</td>
<td>23</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>9161</td>
<td>20</td>
<td>180</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Table 2**

<table>
<thead>
<tr>
<th>( q )</th>
<th>Elements of ( \mathcal{S}(5, 5, q) )</th>
</tr>
</thead>
<tbody>
<tr>
<td>11</td>
<td>1, 3, 4, 5, 9</td>
</tr>
<tr>
<td>31</td>
<td>1, 3, 5, 8, 9, 12, 13, 14, 15, 16, 17, 18, 21, 22, 23, 25, 28, 29</td>
</tr>
<tr>
<td>71</td>
<td>1, 3, 4, 5, 9, 11, 12, 15, 16, 20, 25, 26, 29, 45, 54, 55, 57, 59, 60, 62</td>
</tr>
<tr>
<td>191</td>
<td>8, 9, 13, 34, 40, 45, 48, 49, 54, 65, 78, 79, 86, 92, 97, 103, 133, 134, 170</td>
</tr>
</tbody>
</table>

License or copyright restrictions may apply to redistribution; see http://www.ams.org/journal-terms-of-use
On evaluating $1 - (1 - 5/11)(1 - 18/31)(1 - 20/71)(1 - 19/191) = -1/852$, we see that we have $q$ equal to one of 11, 31, 71, or 191 for over 85% of all $N$ of the form $A5^n - 1$. Similarly, we have a $q = 29, 43$ or 281 for over 68% of all $N$ of the form $A7^n - 1$. If we were to use the values of the $q$'s given in Table 1, we could change these figures to 88% and 90%, respectively. There are, however, values for $A$ for which we can never expect to find a single $q$-value that will work for all $Au^n - 1$. This is certainly the case if $A - 1$ is a perfect $r$th power.

Consider, for example, numbers of the form $N = 2 \cdot 10^n - 1$. We find that if $q = 101$, then $N \equiv 1, 19, 98, 80 \pmod{101}$. Since none of 19$^{20}$, 98$^{20}$, 80$^{20}$ is 1 (mod 101), we can use $q = 101$ as long as $4 \nmid n$. If $q = 41$, then $N \equiv 1, 19, 35, 31, 32 \pmod{41}$. Of these only 1$^8$ and 32$^8$ are 1 (mod 41). If $N \equiv 32 \pmod{41}$, then $n \equiv 4 \pmod{5}$ and $N = 216 \pmod{271}$; but, 216$^2 \neq 1 \pmod{271}$. Thus, if $20 \nmid n$ one of 41, 101, or 271, can be used as a value for $q$. The process we have begun here can be easily continued on a computer. We found that if

$$k = 138007919535942456000$$

$$= 2^6 \cdot 3^5 \cdot 5^3 \cdot 7^2 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \cdot 37 \cdot 41$$

and $k \nmid n$, then one of 31, 41, 101, 131, 181, 191, 251, 271, 281, 331, 401, 521, 541, 571, 641, 751, 811, 821, 881, 1021, 1151, 1231, 1361, 1451, 1471, 1741, 1861, 2531, 2591, 3001, 3331, 3701, 4481, 4861 can be used for $q$.

Once we have found a value for $q$ we also need to know the values of the coefficients $C(i, r, q)$. In Table 4 we give the values of $C(i, 5, q)$ for all $q < 10000$ and in Table 5 we give the values of $C(i, 7, q)$ for all $q < 5000$. A description of how these numbers can be computed is given in [12].

When $r = 5$ we need to know how to compute $X$ and $Y$. For a general $A$ this is a very difficult problem, but for certain values of $A$ it can be easily solved. If $N = 1 \pmod{4}$, we see from the results in Section 4 that we need only consider the case where $8 \mid A$. In this case, if $A \equiv \pm 1 \pmod{3}$, then $N \equiv 0 \pmod{1} \pmod{3}$; thus, if $3 \nmid N$ and $3 \nmid A$, we have $(6/N) = -1$ and we can put $X = Y = 1$. For the case of $24 \mid A$, we must search for some odd $m$ such that $(N/m) = 1$ and $2m = X^2 + 5Y^2$ or $(N/m) = -1$ and $m = X^2 + 5Y^2$. For example, if $N = 1, 2, 4 \pmod{7}$, then we can use $X = 3, Y = 1$.

When $N = 1 \pmod{4}$ it is more difficult to find values of $A$ for which we can easily find $X$ and $Y$. If $m = X^2 - 5Y^2$, $|m| > 1$, $m \mid A$ and $m \equiv -1 \pmod{4}$, then $(m/N) = (N/m) = (-1/m) = -1$. Thus, if $11 \mid A$ we can use $X = 4, Y = 1$. If we do not know any such divisor of $A$, then we must search for $m$ such that $m = X^2 - 5Y^2$ and $(N/m) = -1$.

**Table 3**

<table>
<thead>
<tr>
<th>$q$</th>
<th>Elements of $\mathcal{Y}(7, 7, q)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>29</td>
<td>1, 7, 16, 20, 23, 24, 25</td>
</tr>
<tr>
<td>43</td>
<td>3, 4, 9, 10, 11, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 32, 33, 34, 39, 40</td>
</tr>
<tr>
<td>281</td>
<td>10, 17, 32, 57, 58, 70, 72, 118, 119, 125, 156, 162, 163, 209, 211, 223, 224, 249, 264, 271</td>
</tr>
<tr>
<td>q</td>
<td>C(0.5, q)</td>
</tr>
<tr>
<td>---</td>
<td>-----------</td>
</tr>
<tr>
<td>0.5</td>
<td>361</td>
</tr>
<tr>
<td>1.0</td>
<td>1417</td>
</tr>
<tr>
<td>1.5</td>
<td>152398</td>
</tr>
<tr>
<td>2.0</td>
<td>51462</td>
</tr>
<tr>
<td>2.5</td>
<td>145452</td>
</tr>
<tr>
<td>3.0</td>
<td>45142</td>
</tr>
<tr>
<td>3.5</td>
<td>312882</td>
</tr>
<tr>
<td>4.0</td>
<td>227929</td>
</tr>
<tr>
<td>4.5</td>
<td>218129</td>
</tr>
<tr>
<td>5.0</td>
<td>222355</td>
</tr>
<tr>
<td>5.5</td>
<td>354832</td>
</tr>
<tr>
<td>6.0</td>
<td>193732</td>
</tr>
<tr>
<td>6.5</td>
<td>368552</td>
</tr>
<tr>
<td>7.0</td>
<td>248608</td>
</tr>
<tr>
<td>7.5</td>
<td>284975</td>
</tr>
<tr>
<td>8.0</td>
<td>284357</td>
</tr>
<tr>
<td>8.5</td>
<td>130138</td>
</tr>
<tr>
<td>9.0</td>
<td>463553</td>
</tr>
<tr>
<td>9.5</td>
<td>262362</td>
</tr>
<tr>
<td>10.0</td>
<td>245097</td>
</tr>
<tr>
<td>10.5</td>
<td>109402</td>
</tr>
<tr>
<td>11.0</td>
<td>270333</td>
</tr>
<tr>
<td>11.5</td>
<td>362568</td>
</tr>
<tr>
<td>12.0</td>
<td>276788</td>
</tr>
<tr>
<td>12.5</td>
<td>276348</td>
</tr>
<tr>
<td>13.0</td>
<td>281042</td>
</tr>
<tr>
<td>13.5</td>
<td>485204</td>
</tr>
<tr>
<td>14.0</td>
<td>278578</td>
</tr>
<tr>
<td>14.5</td>
<td>278916</td>
</tr>
<tr>
<td>15.0</td>
<td>222352</td>
</tr>
<tr>
<td>15.5</td>
<td>-368552</td>
</tr>
<tr>
<td>16.0</td>
<td>248608</td>
</tr>
<tr>
<td>16.5</td>
<td>284975</td>
</tr>
<tr>
<td>17.0</td>
<td>284357</td>
</tr>
<tr>
<td>17.5</td>
<td>130138</td>
</tr>
<tr>
<td>18.0</td>
<td>463553</td>
</tr>
<tr>
<td>18.5</td>
<td>262362</td>
</tr>
<tr>
<td>19.0</td>
<td>245097</td>
</tr>
<tr>
<td>19.5</td>
<td>109402</td>
</tr>
<tr>
<td>20.0</td>
<td>270333</td>
</tr>
<tr>
<td>20.5</td>
<td>362568</td>
</tr>
<tr>
<td>21.0</td>
<td>276788</td>
</tr>
<tr>
<td>21.5</td>
<td>276348</td>
</tr>
<tr>
<td>22.0</td>
<td>281042</td>
</tr>
<tr>
<td>22.5</td>
<td>485204</td>
</tr>
<tr>
<td>23.0</td>
<td>278578</td>
</tr>
<tr>
<td>23.5</td>
<td>278916</td>
</tr>
<tr>
<td>24.0</td>
<td>222352</td>
</tr>
<tr>
<td>24.5</td>
<td>-368552</td>
</tr>
<tr>
<td>25.0</td>
<td>248608</td>
</tr>
<tr>
<td>25.5</td>
<td>284975</td>
</tr>
<tr>
<td>26.0</td>
<td>284357</td>
</tr>
<tr>
<td>26.5</td>
<td>130138</td>
</tr>
<tr>
<td>27.0</td>
<td>463553</td>
</tr>
<tr>
<td>27.5</td>
<td>262362</td>
</tr>
<tr>
<td>28.0</td>
<td>245097</td>
</tr>
<tr>
<td>28.5</td>
<td>109402</td>
</tr>
<tr>
<td>29.0</td>
<td>270333</td>
</tr>
<tr>
<td>29.5</td>
<td>362568</td>
</tr>
<tr>
<td>30.0</td>
<td>276788</td>
</tr>
<tr>
<td>30.5</td>
<td>276348</td>
</tr>
<tr>
<td>31.0</td>
<td>281042</td>
</tr>
<tr>
<td>31.5</td>
<td>485204</td>
</tr>
<tr>
<td>32.0</td>
<td>278578</td>
</tr>
<tr>
<td>32.5</td>
<td>278916</td>
</tr>
<tr>
<td>33.0</td>
<td>222352</td>
</tr>
<tr>
<td>33.5</td>
<td>-368552</td>
</tr>
<tr>
<td>34.0</td>
<td>248608</td>
</tr>
<tr>
<td>34.5</td>
<td>284975</td>
</tr>
<tr>
<td>35.0</td>
<td>284357</td>
</tr>
<tr>
<td>35.5</td>
<td>130138</td>
</tr>
<tr>
<td>36.0</td>
<td>463553</td>
</tr>
<tr>
<td>36.5</td>
<td>262362</td>
</tr>
<tr>
<td>37.0</td>
<td>245097</td>
</tr>
<tr>
<td>37.5</td>
<td>109402</td>
</tr>
<tr>
<td>38.0</td>
<td>270333</td>
</tr>
<tr>
<td>38.5</td>
<td>362568</td>
</tr>
<tr>
<td>39.0</td>
<td>276788</td>
</tr>
<tr>
<td>39.5</td>
<td>276348</td>
</tr>
<tr>
<td>40.0</td>
<td>281042</td>
</tr>
<tr>
<td>40.5</td>
<td>485204</td>
</tr>
<tr>
<td>41.0</td>
<td>278578</td>
</tr>
<tr>
<td>41.5</td>
<td>278916</td>
</tr>
<tr>
<td>42.0</td>
<td>222352</td>
</tr>
<tr>
<td>42.5</td>
<td>-368552</td>
</tr>
<tr>
<td>43.0</td>
<td>248608</td>
</tr>
<tr>
<td>43.5</td>
<td>284975</td>
</tr>
<tr>
<td>44.0</td>
<td>284357</td>
</tr>
<tr>
<td>44.5</td>
<td>130138</td>
</tr>
<tr>
<td>45.0</td>
<td>463553</td>
</tr>
<tr>
<td>45.5</td>
<td>262362</td>
</tr>
<tr>
<td>46.0</td>
<td>245097</td>
</tr>
<tr>
<td>46.5</td>
<td>109402</td>
</tr>
<tr>
<td>47.0</td>
<td>270333</td>
</tr>
<tr>
<td>47.5</td>
<td>362568</td>
</tr>
<tr>
<td>48.0</td>
<td>276788</td>
</tr>
<tr>
<td>48.5</td>
<td>276348</td>
</tr>
<tr>
<td>49.0</td>
<td>281042</td>
</tr>
<tr>
<td>49.5</td>
<td>485204</td>
</tr>
<tr>
<td>50.0</td>
<td>278578</td>
</tr>
<tr>
<td>50.5</td>
<td>278916</td>
</tr>
<tr>
<td>q</td>
<td>C(0,1,q)</td>
</tr>
<tr>
<td>----</td>
<td>----------</td>
</tr>
<tr>
<td>29</td>
<td>5199</td>
</tr>
<tr>
<td>43</td>
<td>8265</td>
</tr>
<tr>
<td>71</td>
<td>-35093</td>
</tr>
<tr>
<td>113</td>
<td>99959</td>
</tr>
<tr>
<td>127</td>
<td>-206568</td>
</tr>
<tr>
<td>197</td>
<td>-201147</td>
</tr>
<tr>
<td>211</td>
<td>1405689</td>
</tr>
<tr>
<td>239</td>
<td>1434998</td>
</tr>
<tr>
<td>281</td>
<td>1135251</td>
</tr>
<tr>
<td>337</td>
<td>-1621230</td>
</tr>
<tr>
<td>377</td>
<td>-5130477</td>
</tr>
<tr>
<td>421</td>
<td>5988291</td>
</tr>
<tr>
<td>449</td>
<td>106674</td>
</tr>
<tr>
<td>463</td>
<td>7110379</td>
</tr>
<tr>
<td>481</td>
<td>11059523</td>
</tr>
<tr>
<td>547</td>
<td>-2729477</td>
</tr>
<tr>
<td>617</td>
<td>-1497453</td>
</tr>
<tr>
<td>631</td>
<td>15175284</td>
</tr>
<tr>
<td>659</td>
<td>-9473615</td>
</tr>
<tr>
<td>673</td>
<td>-12282174</td>
</tr>
<tr>
<td>701</td>
<td>10792521</td>
</tr>
<tr>
<td>743</td>
<td>-7220706</td>
</tr>
<tr>
<td>757</td>
<td>11733531</td>
</tr>
<tr>
<td>827</td>
<td>-23656481</td>
</tr>
<tr>
<td>883</td>
<td>-12154306</td>
</tr>
<tr>
<td>947</td>
<td>4995590</td>
</tr>
<tr>
<td>953</td>
<td>-42151818</td>
</tr>
<tr>
<td>967</td>
<td>-22156752</td>
</tr>
<tr>
<td>1005</td>
<td>50636066</td>
</tr>
<tr>
<td>1051</td>
<td>-74745881</td>
</tr>
<tr>
<td>1083</td>
<td>69239721</td>
</tr>
</tbody>
</table>
We can also regard this problem as being similar to our preceding problem; that is, we search for primes \( q \) and values of \( A \) such that

\[
(5.5) \quad (A^5 - 1)^{(q - 1)/2} \not\equiv 1 \pmod{q}
\]

for all \( n \). As we also need that \( q = X^2 - 5Y^2 \), we must further restrict \( q \equiv \pm 1 \pmod{5} \). Unfortunately, such primes seem to be very rare. When \( q = 31 \), we have \( A \equiv 0, 16, 18, 28 \pmod{31} \) as solutions of (5.5) for all \( n \); when \( q = 19531 \), there are 127 such values of \( A \). These can be found by computing \( 5^k \pmod{19531} \) \((i = 0, 1, 2, \ldots, 8)\), where \( k \in \{0, 66, 576, 652, 772, 1348, 1492, 1677, 1891, 2108, 2301, 2552, 2893, 3372, 3466, 3593, 3624, 5453\} \). Also, if \( k = 66, 652, 5453 \), then \( 5^k \in \mathcal{O}(5, 5, 19531) \). We also have \( 19531 = 156^2 - 5 \cdot 31^2 \), \( C(0, 5, 19531) = -2590642 \) and \( C(1, 5, 19531) = -4403875 \). The primes 31 and 19531 are the only values of \( q \) known to the author such that these special values of \( A \) with \( q \nmid A \) exist.

We also point out that if \( A \equiv 5j \pmod{31} \), where \( j \in \{5, 11, 17, 20\} \) and \( n \equiv -i \pmod{3} \), then if \( 31 \nmid N \), we have \( (31/N) = -1 \). For each value of \( i \) there exist 99 values of \( A \pmod{829} \) \((829 = 57^2 - 5 \cdot 22^2)\) such that if \( 829 \nmid N \), then \( (829/N) = -1 \) when \( n \equiv -i \pmod{3} \). For example, if \( A \equiv 17 \pmod{31} \) and \( A \equiv 23 \pmod{829} \), then \( (31/N) = -1 \) or \( (829/N) = -1 \). Many other results of this type can be derived.

6. The Primality Tests. We now assume that we wish to test \( N = Ar^n - 1 \), where \( A < r^n \) and \( r = 5 \) or 7, for primality. We further assume that \( N \) is odd. We emphasize here that it is only for those values of \( A \) such that we have \textit{a priori} values for \( q \), the coefficients \( C(i, r, q) \) and \( X, Y \) (when needed), that the tests given below are effective; however, as we have seen in Section 5, we can certainly provide such values for many values of \( A \).

We deal first with the case of \( r = 5 \). If \( 4 \nmid A \) and \( N \) is odd, then \( N \equiv 1 \pmod{4} \). If we can find \( X, Y \) such that \( (X^2 - 5Y^2/N) = -1 \), we can put \( P = 2X, \quad Q = 5Y^2 \) and compute \( W_k, W_{k+1} \pmod{N} \), where \( k = (A - 2)/4 \). Set

\[
L \equiv 5Y(W_{k+1} + W_k)(4X)^{-1} \pmod{N}
\]

and note that

\[
L \equiv (2Y)^{-1}Q^{-k}V_{2k+1} \pmod{N}.
\]

Now

\[
V_{2k+1}^2 \equiv 4Q^{2k+1} \pmod{N}
\]

if and only if \( L^2 \equiv 5 \pmod{N} \). If \( L^2 \equiv 5 \pmod{N} \), then we have

\[
R \equiv 2^{-1}(-1 + L) \pmod{N},
\]

and we can use this in the test given as Theorem 3.5. If \( L^2 \not\equiv 5 \pmod{N} \), then

\[
V_{2k+1}^2 \not\equiv 4Q^{2k+1} \pmod{N}
\]

and

\[
V_A \equiv V_{A/2}^2 - 2Q^{4/2} \not\equiv 2Q^{A/2} \pmod{N}.
\]
If \( N \) is a prime, we have \( \eta = 1 \) and
\[ V_A \not\equiv 2\eta Q^{A/2} \pmod{N}. \]
Thus, by the remarks of Section 3 there must exist a least \( m \) (\( 0 < m \leq n \)) such that
\[ W_{A,r^{m/2}} \equiv 2\eta \pmod{N} \]
and
\[ G_2(W_{A,r^{m-1}}) \equiv 0 \pmod{N}. \]
If (6.1) holds for any \( N \), then we know that if \( p \) is any prime divisor of \( N \), we must have \( p \mid U_{A,r^{m}} \) and \( p + U_{A,r^{m-1}} \). Thus \( p \equiv \pm 1 \pmod{r^m} \) (see [7]). If \((2r^m - 1)^2 > N\), then \( N \) must be a prime.

We may now assemble all of this information into a primality test for \( N = A5^n - 1 \equiv 1 \pmod{4}, A < 5^n \).

**Primality Test 1.**

1. Select \( X, Y \).
2. Put \( P = 2X, Q = 5Y^2, k = (A - 2)/4; \) compute \( W_k, W_{k+1} \pmod{N} \) and \( L = 5Y(4X)^{-1}(W_{k+1} + W_k) \pmod{N} \).
3. If \( L^2 \equiv 5 \pmod{N} \), put \( R = (-1 + L)2^{-1} \pmod{N} \) and go to step (6); otherwise,
   4. Compute \( S_1 \equiv W_{A/2} \equiv 4 \cdot 5^{-1}L^2 - 2 \pmod{N} \).
5. Determine \( S_{i+1} \equiv G_2(2 - S_i^2)S_i \pmod{N}, i = 1, 2, \ldots \), until we find some \( m \leq n + 1 \) such that \( S_m \equiv 2 \pmod{N} \). If no such \( m \) exists, \( N \) is composite. If \((2 \cdot 5^{m-1} - 1)^2 > N\), then \( N \) is a prime. If \((2 \cdot 5^{m-1} - 1)^2 < N\), put \( R \equiv S_{m-1}^2 - 2 \pmod{N} \).
6. Find \( q, C(0, 5, q), C(1, 5, q) \) and compute \( P \equiv C(0, 5, q) + C(1, 5, q)R, Q \equiv q^3 \pmod{N} \) and, using these values of \( P, Q \), calculate \( S_1 \equiv W_{A/2} \pmod{N} \).
7. Using \( S_{i+1} \equiv G_2(2 - S_i^2)S_i \pmod{N} \), compute \( S_n \).
8. \( N \) is a prime if and only if
\[ G_2(S_n^2 - 2) \equiv 0 \pmod{N}. \]

In any running of this test it would be found that most prime values of \( N \) would be identified as such in step (5); however, if step (5) failed to determine whether or not \( N \) is a prime (\( m \) is too small), then steps (6) and (7) would settle the question. Thus, for example, if \( A \equiv 16, 18 \) or \( 28 \pmod{31} \), we can use \( X = 6, Y = 1, q = 31 \) and we have an effective necessary and sufficient \( O(\log N) \) test for the primality of \( N \).

When \( N = A5^n - 1 \equiv -1 \pmod{4} \), we select \( X, Y \) such that \((X^2 + 5Y^2/N) = -1 \) and compute \( P = 2Y, Q = X^2 + 5Y^2, W_k, W_{k+1} \pmod{N} \), where \( k = A/4 \). If \( W_k \equiv 0 \pmod{N} \), we then determine
\[ L \equiv (4XY)^{-1}QW_{k+1} \pmod{N}. \]

By our remarks in Section 4 we know that
\[ R \equiv (-1 + L)2^{-1} \pmod{N}. \]
is a solution of \( G_2(x) \equiv 0 \pmod{N} \). If \( N \) is a prime and \( W_k \neq 0 \pmod{N} \), then \( V_{A/2} \neq 0 \pmod{N} \) and

\[
V_A \equiv -2Q^{A/2} = 2\eta Q^{A/2} \pmod{N}.
\]

We now have a test for the primality of \( N = A5^n - 1 \), where \( 8 \mid A \) and \( A < 5^n \) in

**Primality Test 2.**

1. Select \( X, Y \) and put \( \eta = 1 \).
2. Put \( P = 2X, Q = X^2 + 5Y^2 \) and compute \( W_k, W_{k+1} \pmod{N} \), where \( k = A/4 \).
3. If \( W_k = 0 \pmod{N} \), put

\[
S_1 = (-1 + L)^2 \pmod{A'},
\]

where \( L = (4XY)^{-1} QW_{k+1} \pmod{N} \) and go to step (6).
4. If \( W_k \neq 0 \pmod{N} \), put

\[
S_1 = W_{2k} - 2 \pmod{N}.
\]

5. Determine \( S_{i+1} = G_2(2 - S_i^2)S_i \pmod{N} \) for \( i = 1, 2, \ldots \) until we find some \( m \leq n + 1 \) such that \( S_m = 2\eta \pmod{N} \). If no such \( m \) exists, \( N \) is composite. If \((2 \cdot 5^{n-1} - 1)^2 > N\), then \( N \) is a prime. If \((2 \cdot 5^{n-1} - 1)^2 < N\) put \( R \equiv S_{2m-1}^2 - 2 \pmod{N} \).
6. Steps (6), (7), and (8) are the same as those in Test 1.

If, for example, we wish to adapt this test for use on numbers of the form \( N = A5^n - 1 = 2 \cdot 10^n - 1 \) (\( n > 3 \)), we first note that \((6/N) = (3/N) = -1\); hence, we can put \( X = Y = 1 \). By using the formulas in (2.2), we have the following effective test for the primality of numbers of the form \( 2 \cdot 10^n - 1 \) (\( n > 3 \)) where \( 138007919535942456000 \div n \).

1. Put \( P = 2, Q = 6, Y_0 = (2 \cdot 10^n - 11)/3, Z_0 = 2Y_0 + 6 \). (Note that \( Y_0 \equiv P^2Q^{-1} - 2 \equiv V_2Q^{-1}, Z_0 \equiv PQ^{-1} \equiv U_2Q^{-1} \pmod{N} \)).
2. Compute

\[
Y_{j+1} = Y_j^2 - 2 \pmod{N},
\]
\[
Z_{j+1} = Z_jY_j \pmod{N}, \quad j = 0, 1, 2, \ldots, n - 1.
\]

(We have \( Z_{n-1} \equiv U_{A/2}Q^{-A/4} \pmod{N} \)).
3. If \((5Z_{n-1}^2) \equiv 5 \pmod{N} \), put

\[
R \equiv (-1 + 5Z_{n-1})2^{-1} \pmod{N}
\]

and go to step (5); otherwise, put \( S_1 = Y_{n-1}^2 - 2 \pmod{N} \).
4. Compute

\[
S_{i+1} = G_2(2 - S_i^2)S_i \pmod{N}
\]

until we find some \( m \leq n + 1 \) such that \( S_m \equiv -2 \pmod{N} \). If no such \( m \) exists, \( N \) is composite; if \( m \geq 3n/4 \), \( N \) is a prime; if \( m < 3n/4 \), put \( R \equiv S_{2m-1}^2 - 2 \).
5. Select \( q \) from the list given in Section 5 and find \( C(0, 5, q), C(1, 5, q) \) from Table 4. Compute

\[
P \equiv C(0, 5, q) + C(1, 5, q)R, \quad Q \equiv q^3 \pmod{N}.
\]
(6) Compute \( Y_0 = P^2Q^{-1} - 2 \) (mod \( N \)) and determine \( S_1 = Y_n \) (mod \( N \)) from

\[
Y_{j+1} \equiv Y_j^2 - 2 \pmod{N} \quad (j = 1, 2, 3, \ldots, n - 1).
\]

(7) Use

\[
S_{i+1} \equiv G_2(2 - S_i^2)S_i \pmod{N} \quad (i = 1, 2, 3, \ldots, n - 1)
\]
to compute \( S_n \).

(8) \( N \) is a prime if and only if

\[
N \mid G_2(S_n^2 - 2).
\]

This test was implemented on an AMDAHL 5850 computer and used to determine the primality of all primes of the form \( 2 \cdot 10^n - 1 \) with \( n < 3400 \). We found that \( 2 \cdot 10^n - 1 \) is prime only for \( n = 1, 2, 3, 5, 7, 26, 27, 53, 147, 236, 248, 386, 401, 546, 785, 1325, 1755, 2906, 3020 \). The author is indebted to Harvey Dubner for identifying the last four numbers in this table as the only likely primes when 1000 < \( n < 3400 \). Indeed, if we are given a large range of values for \( n \) in which to search for the primes of the form \( N = A5^n - 1 \) with \( 4 \mid A \), because very few of the values of \( N \) will be prime, a more practical way of implementing our primality test for \( N \) is (after preliminary trial division by small primes) to first determine whether or not \( N \) is a base 5 probable prime by calculating

\[
R \equiv 5^{(N+1)/4} \pmod{N}.
\]

If \( R^2 \not\equiv 5 \) (mod \( N \)), then \( N \) is not a prime; if \( R^2 \equiv 5 \) (mod \( N \)), we need only execute steps (6), (7), and (8) of Primality Test 1.

Test 2 can be used when \( N \equiv 3 \) (mod 8); however, in this case we can avoid the difficulty of searching for \( X \) and \( Y \) by using \( P = 2, \ Q = 5, \ k = (A - 4)/8 \). If neither

\[
5(W_{k+1} + W_k)4^{-1} \quad \text{nor} \quad 5(W_{k+1} - W_k)8^{-1}
\]
is a solution of (4.2), then when \( N \) is a prime we cannot have

\[
U_{A/2} \equiv 0 \pmod{N}.
\]

It follows that \( V_{A/2} \not\equiv 4Q^{4/4} \) (mod \( N \)) and \( V_A \not\equiv 2\eta Q^{4/2} \) (mod \( N \)). Thus, in the case where \( N \equiv 3 \) (mod 8), we can replace steps (1), (2), (3), (4) of Primality Test 2 by

(1) Select \( P = 2, \ Q = 5, \ \eta = +1 \).

(2) Compute \( W_k, W_{k+1} \) (mod \( N \)), where \( k = (A - 4)/8 \).

(3) If \( 5(W_{k+1} + W_k)4^{-1} \) or \( 5(W_{k+1} - W_k)8^{-1} \) is a solution of (4.2), put \( L \) equal to this solution and put \( R \equiv (-1 + L)2^{-1} \) (mod \( N \)) and go to step 6. Otherwise,

(4) Put \( L \equiv W_{A/4} \equiv 5(W_{k+1} + W_k)2^{-1} - 2 \pmod{N} \). \( S_1 \equiv W_{A/2} \equiv L^2 - 2 \pmod{N} \).

It is rather remarkable that for certain values of \( A \) we can obtain a test similar to Tests 1 and 2 for the primality of \( N = A7^n - 1 \) (\( A < 7^n \)). For, in this case we must integrate the problem of solving a certain cubic congruence into a prime test. We can do this for \( 1/3 \) of the possible values of \( A \); that is, those values of \( A \) for which \( 3 \mid A \) and \( 9 \not\mid A \). We need not, of course, consider the case of \( A \equiv 1 \) (mod 3).
Let $c (= 1 \text{ or } 2)$ be such that $cB \equiv 1 \pmod{3}$, where $B = A/6$. Since $N \equiv -1 \pmod{3}$, we have $e = (\Delta/N) = (-3/N) = -1$ when $P = -1$, $Q = 7$. Also,

$$\eta = (Q/N) = (7/N) = (-1)^{(N+1)/2} = (-1)^B.$$ 

Now if $N$ is a prime, we have $N \equiv -1 \pmod{7}$ and, consequently,

(6.2) $$G_3(x) \equiv 0 \pmod{N}$$

must be solvable; thus,

(6.3) $$U_{(N+1)/3} \equiv 0 \pmod{N}.$$

Also, by the reasoning used at the end of Section 3, we know that if

$$V_{cA} \equiv 2\eta Q^{cA/2} \pmod{N},$$

then $N \mid U_A$. If $N \mid U_A$, by (2.3) we have $N \mid U_{4/3}$ or $V_{A/3}^2 \equiv Q^{A/3} \pmod{N}$. Set $m = 7^n = (N + 1)/A$ and $s = (m - 1)/2$; by (2.8) we have

(6.4) $$U_{(N+1)/3} \equiv Q^{As/3}G_s\left(V_{2A/3}Q^{-A/3}\right)U_{A/3} \pmod{N}.$$ 

If $V_{A/3}^2 \equiv Q^{A/3} \pmod{N}$, then $V_{2A/3}Q^{-A/3} \equiv -1 \pmod{N}$ by (2.2); hence, because $3 \mid s$, we get

$$G_s\left(V_{2A/3}Q^{-A/3}\right) \equiv 1 \pmod{N}.$$ 

It follows from (6.3) and (6.4) that $U_{A/3} \equiv 0 \pmod{N}$.

By the results of Section 4 we see that if $V_{cA} \equiv 2\eta Q^{cA/2} \pmod{N}$, then

$$(-1 + 7\eta (W_{k+1} + W_k))^{3^{-1}} \pmod{N}$$

is a solution of (6.2).

From (2.16) we get

$$27W_{3k+1} = 91W_k^3 + 147W_k^2W_{k+1}^2 - 49W_{k+1}^3 \pmod{N},$$

and by (2.3),

$$W_{cA/2} \equiv V_{cA}Q^{-cA/2} = W_{3cb} = W_{3(3k+1)} \equiv W_{3k+1}\left(W_{2k+2}^2 - 3\right) \pmod{N}.$$ 

We can now give our primality test for numbers of the form $N = A7^n - 1$, where $A = 6B$, $3 \nmid B$, $A < 7^n$ as

**Primality Test 3.**

(1) Using $W_1 = 6B7^{n-1} - 2$, compute $W_k$, $W_{k+1} \pmod{N}$, where $k = (cB - 1)/3$, $cB \equiv 1 \pmod{3}$, $c = 1$ or 2.

(2) Put

$$R \equiv 2B7^n(-1 + (-1)^{cB}7(W_k + W_{k+1})) \pmod{N}.$$ 

If $G_3(R) \equiv 0 \pmod{N}$, go to step (5); otherwise,

(3) Put

$$M \equiv 8B^37^3n(91W_k^3 + 147W_k^2W_{k+1}^2 - 49W_{k+1}^3) \pmod{N},$$

$$S_1 \equiv M(M^2 - 3) \pmod{N}.$$ 

(4) Compute

$$S_{i+1} \equiv -G_3(2 - S_i^2)S_i \pmod{N} \text{ for } i = 1, 2, 3, \ldots$$
until we find some $m \leq n + 1$ such that $S_m \equiv 2a^r \pmod{N}$. If no such $m$ exists, $N$ is composite; if $(2 \cdot 7^{m-1} - 1)^2 > N$, then $N$ is a prime; if $(2 \cdot 7^{m-1} - 1)^2 < N$, put $R = S_{n-1} - 2 \pmod{N}$.

(5) Select $q$ and determine $C(0, 7, q), C(1, 7, q), C(2, 7, q)$. Put
\[
P = C(0, 7, q) + C(1, 7, q)R + C(2, 7, q)R^3 \pmod{N},
\]

\[
Q = q^5 \pmod{N},
\]

\[
S_1 = W_{A/2} \pmod{N}.
\]

(6) Using
\[
S_{r+1} \equiv -G_3(2 - S_r^2)S_r \pmod{N},
\]

compute $S_n$.

(7) $N$ is a prime if and only if
\[
G_3(S_n^2 - 2) \equiv 0 \pmod{N}.
\]

If $A \equiv 2 \pmod{3}$ and $A \neq 2 - 3n \pmod{9}$, we can still solve for $R$ by using the results in Section 4 with $t = (N - 1)/3$; but, because $N \equiv 1 \pmod{3}$, we have $e = (A/N) = 1$ and, therefore, we cannot integrate the problem of solving (6.2) into a sufficiency test for the primality of $N$ as we did above.

Department of Computer Science
University of Manitoba
Winnipeg, Manitoba, Canada R3T 2N2


License or copyright restrictions may apply to redistribution; see http://www.ams.org/journal-terms-of-use