MATHEMATICS OF COMPUTATION
VOLUME 48, NUMBER 177
JANUARY 1987, PAGES 385–403

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 $2 \cdot 10^n - 1$.

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 $k \geqslant 1$

$$S_{k+1} \equiv S_k^2 - 2 \pmod{N}.$$

(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 $A \equiv 4, 7, 8, 10, 11, 12 \pmod{13}$, 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 rth 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.

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 α, β be the zeros of $x^2 - Px + Q$. We define the Lucas functions $V_n(P, Q)$, $U_n(P, Q)$ ($n \in \mathbf{Z}$) by

$$V_n(P, Q) = \alpha^n + \beta^n, \qquad U_n(P, Q) = (\alpha^n - \beta^n)/(\alpha - \beta).$$

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.

$$V_n^2 - \Delta U_n^2 = 4Q^n, \tag{2.1}$$

$$V_{2n} = V_n^2 - 2Q^n, \qquad U_{2n} = V_n U_n, \tag{2.2}$$

$$V_{3n} = V_n\left(V_n^2 - 3Q^n\right), \qquad U_{3n} = U_n\left(V_n^2 - Q^n\right), \tag{2.3}$$

$$V_{m+n} = V_n V_m - Q^n V_{m-n}, \qquad U_{m+n} = V_n U_m - Q^n U_{m-n}, \tag{2.4}$$

$$2V_{m+n} = V_n V_m + \Delta U_n U_m, \qquad 2U_{m+n} = U_n V_m + V_n U_m. \tag{2.5}$$

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

$$\delta \alpha^n U_m = V_n \alpha^m - Q^m V_{n-m}. \tag{2.6}$$

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

$$\frac{x^{2s+1} - 1}{x - 1} = x^s G_s\left(x + x^{-1}\right).$$

Also, $G_s(-2) = (-1)^s$, and when $3 \mid s$, $G_s(-1) = 1$. If we put $r = 2s + 1$ and $x = -(\alpha/\beta)^n$, we get

(2.7) $$V_{nr} = (-1)^s Q^{ns} G_s(-V_{2n}/Q^n) V_n;$$

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

(2.8) $$U_{nr} = Q^{ns} G_s(V_{2n}/Q^n) U_n.$$

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

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

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

$$-\delta^r\beta^{nr}U_m^r\beta^k = (V_n\beta^m - Q^m V_{n-m})^r\beta^k,$$

$$\delta^r\alpha^{nr}U_m^r\alpha^k = (V_n\alpha^m - Q^m V_{n-m})^r\alpha^k.$$

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

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

for odd r. If we had added the two identities above we would get a similar identity for $\Delta^{(r+1)/2} U_{nr+k} U_m^r$. If r is even, we can also get identities for $\Delta^{r/2} V_{nr+k} U_m^r$ and $\Delta^{r/2} U_{nr+k} U_m^r$. 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) (mod N) for large values of n, it is convenient to introduce the function

$$W_m \equiv V_{2m} Q^{-m} \pmod{N}.$$

(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

(2.10) $$W_{2n} \equiv W_n^2 - 2 \pmod{N}$$

and

(2.11) $$W_{m+n} \equiv W_m W_n - W_{m-n} \pmod{N}.$$

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

(2.12) $$W_{2n+1} \equiv W_n W_{n+1} - W_1 \pmod{N},$$

where

$$W_1 \equiv P^2 Q^{-1} - 2 \pmod{N}.$$

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 $t = [\log_2 m]$. Using the notation $\{A, B\} \equiv \{C, D\}$ (mod N) to mean $A \equiv C$, $B \equiv D$ (mod N), set $\mathscr{P}_0 \equiv \{W_1, W_2\}$ (mod N) and deduce $\mathscr{P}_{i+1}$ from $\mathscr{P}_i = \{A, B\}$ by

$$\mathscr{P}_{i+1} \equiv \begin{cases} \{A^2 - 2,\ AB - W_1\} \pmod{N} & \text{when } b_{i+1} = 0, \\ \{AB - W_1,\ B^2 - 2\} \pmod{N} & \text{when } b_{i+1} = 1. \end{cases}$$

From (2.10) and (2.12) it is clear that

$$\mathscr{P}_t \equiv \{W_m, W_{m+1}\} \pmod N.$$

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

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

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

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

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

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

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

$$P\Delta U_{2n}Q^{-n} \equiv 2QW_{n+1} - (P^2 - 2Q)W_n \pmod N. \tag{2.16}$$

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

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

and if we put $n = 2m + 2$, we get

$$P^2\Delta W_{3m+1} \equiv Q^2W_{m+1}^3 - 3Q^2W_{m+1}W_m^2 + Q(P^2 - 2Q)W_m^3 \pmod N. \tag{2.17}$$

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

$$V_{p-\varepsilon} \equiv 2Q^{(1-\varepsilon)/2}, \qquad U_{p-\varepsilon} \equiv 0 \pmod p. \tag{3.1}$$

Further, in [7] Lehmer proves

THEOREM 3.1. *If $p \nmid \Delta Q$, then $p \nmid U_{(p-\varepsilon)/2}$ 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*

$$V_{(N+1)/2}(P, Q) \equiv 0 \pmod N. \quad \square$$

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

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

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* $N = Ar^n - 1$ $(A < r^n)$, *where* r *is an odd prime. If* $(\Delta/N) = -1$ *and*

$$G_s(W_{(N+1)/2r}) \equiv 0 \pmod{N},$$

where $s = (r-1)/2$, *then* N *is a prime.* □

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

$$P \equiv \sum_{i=0}^{s-1} C(i, r, q) R^i, \qquad Q \equiv q^{r-2} \pmod{p},$$

then

$$G_s(W_{(p+1)/2r}) \equiv 0 \pmod{p}. \quad \square$$

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

$$P \equiv \sum_{i=0}^{s-1} C(i, r, q) R^i, \qquad Q \equiv q^{r-2} \pmod{N},$$

then N *is a prime if and only if*

$$G_s(W_{(N+1)/2r}) \equiv 0 \pmod{N}. \quad \square$$

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 $p - \varepsilon$, and $t = (p - \varepsilon)/m$, then $U_{ct} \equiv 0 \pmod p$ if and only if $V_{ct} \equiv 2\eta^c Q^{ct/2} \pmod p$.*

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

If $U_{ct} \equiv 0 \pmod p$, by (2.2) we have $U_t \equiv 0 \pmod p$ or, possibly in the case of $c = 2$, $V_t \equiv 0 \pmod p$. 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)

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

where $k = (m-1)/2$, we have $V_{mt} \equiv 2\theta Q^{mt/2} \equiv 2Q^{(1-\varepsilon)/2} \pmod p$ 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),

$$0 \equiv U_{p-\varepsilon} = U_{tm} = Q^{kt} G_k\left(V_{2t}/Q^t\right) U_t \pmod p;$$

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 $V_{cA} \not\equiv 2(Q/N)^c Q^{Ac/2} \pmod N$, then by (2.1) we have $U_{cA} \not\equiv 0 \pmod N$ and by (3.1) and (2.2), $U_{cAr^n} \equiv 0 \pmod N$. It follows that there must be a minimal m $(0 \leqslant m < n)$ such that

$$U_{cAr^m} \not\equiv 0 \pmod N \quad \text{and} \quad U_{cAr^{m+1}} \equiv 0 \pmod N.$$

By (2.8) we must have

$$G_s\left(V_{2cAr^m} Q^{-cAr^m}\right) \equiv 0 \pmod N \quad (m < n). \tag{3.2}$$

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

$$W_{cAr^{m+1}/2} \equiv 2\eta^c \pmod N \quad (m < n). \tag{3.3}$$

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

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

By (2.8) this means that either (3.2) holds or $N \mid U_{cAr^m}$. If $N \mid U_{cAr^m}$, then by Lemma 3.1 we get $W_{cAr^m/2} \equiv 2\eta^c \pmod N$, 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 $V_{cA} \not\equiv 2(Q/N)^c Q^{Ac/2} \pmod N$. 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) $$x^2 \equiv a \pmod{p},$$

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 $x \equiv a^{(p+1)/4}$ 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 $(\Delta/p) = -1$. 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

$$-\Delta U_{2k}^2 \equiv 4Q^{2k} \pmod{p} \quad \text{and} \quad \left(2^{-1}\Delta U_{2k}Q^{-k}\right)^2 \equiv -\Delta \pmod{p}.$$

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) $$x^2 \equiv 5 \pmod{p}.$$

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

$$\left(2^{-1}Q^{-k}V_{2k+1}\right)^2 \equiv Q \pmod{p};$$

if $p \mid V_t$, then

$$-\Delta\left(2^{-1}Q^{-k}U_{2k+1}\right)^2 \equiv Q \pmod{p}.$$

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

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

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

$$x^3 - ax + b \equiv 0 \pmod p \tag{4.3}$$

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's. 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

$$z^3 \equiv \alpha/\beta \pmod p,$$

when

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

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

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

Thus we may assume the existence of some t such that $t \mid (p - \varepsilon)/3$ and $U_t \equiv 0 \pmod p$. Suppose further that $3 \nmid t$ (this is certainly the case if $p \not\equiv \varepsilon \pmod 9$) and that $(p - \varepsilon)/3t$ is odd. We have $V_t \equiv 2\eta Q^{t/2} \pmod p$ by Lemma 3.1. We now select c such that $3 \mid ct + 1$ ($c = 1$ or 2) and note that

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

Thus, by (2.5), we have

$$2V_{ct+1} \equiv V_{ct}V_1 + \Delta U_{ct}U_1 \equiv 2P\eta^c Q^{tc/2} \pmod{p}. \tag{4.4}$$

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

$$\eta^c P Q^{tc/2} \equiv V_k^3 - 3Q^k V_k \pmod{p}$$

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 $p \nmid a$ and $3 \nmid t$, 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

$$G_3(x) \equiv 0 \pmod{p}, \tag{4.5}$$

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 $3 \nmid (p - \varepsilon)/3$. 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

$$N^{(q-1)/r} \not\equiv 0, 1 \pmod{q}. \tag{5.1}$$

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 $\mathscr{S}(u, r, q)$ 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 $L(u, r, q) = |\mathscr{S}(u, r, q)|$. If g is a fixed primitive root of q, $A \equiv g^a \pmod{q}$ and $u \equiv g^j \pmod{q}$, 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, $\nu = (q-1)/k$ 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

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

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

By using (5.4) it is a simple matter to compute $\mathscr{S}(u, r, q)$ as the set of those integers (mod 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 $n = 0, 2, 3, \ldots, \nu - 1$. 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 $q \leqslant 15000$. Note that there are many instances of $L(u, r, q) > 0$ when $\nu > r$. In Tables 2 and 3 we give the elements in selected sets $\mathscr{S}(u, r, q)$.

TABLE 1

$u = 5$, $r = 5$			$u = 10$, $r = 5$			$u = 7$, $r = 7$		
q	$\nu(u, r, q)$	$L(u, r, q)$	q	$\nu(u, r, q)$	$L(u, r, q)$	q	$\nu(u, r, q)$	$L(u, r, q)$
11	5	5	11	2	8			
31	3	18	41	5	10	29	7	7
71	5	20	101	4	40	43	6	24
191	19	19	271	5	90	281	20	20
521	10	70	3541	20	40	911	14	168
601	12	36	7841	56	56	2801	5	1225
1741	15	75	9091	10	900	4733	7	1554
6271	19	76	9901	12	816			
8971	23	23						
9161	20	180						

TABLE 2

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

On evaluating $1 - (1 - 5/11)(1 - 18/31)(1 - 20/71)(1 - 19/191) \approx \cdot 852$, 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 rth 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 $\pmod{101}$, 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 $\pmod{41}$. If $N \equiv 32 \pmod{41}$, then $n \equiv 4 \pmod 5$ and $N \equiv 216 \pmod{271}$; but, $216^5 \not\equiv 1 \pmod{271}$. 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

$$k = 13800791953594245600 0$$

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

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 $N \equiv -1 \pmod 4$, 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 $N \equiv 0$ or $1 \pmod 3$; 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 $N \equiv 1, 2, 4 \pmod 7$, then we can use $X = 3$, $Y = 1$.

When $N \equiv 1 \pmod 4$ 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

q	Elements of $\mathscr{S}(7, 7, q)$
29	1, 7, 16, 20, 23, 24, 25
43	3, 4, 9, 10, 11, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 32, 33, 34, 39, 40
281	10, 17, 32, 57, 58, 70, 72, 118, 119, 125, 156, 162, 163, 209, 211, 223, 224, 249, 264, 271

TABLE 4

q	C(0,5,q)	C(1,5,q)
11	-57	-25
31	-142	125
41	503	25
61	418	-275
71	563	1025
101	-377	-1025
131	-2242	-475
151	-652	-1900
181	-417	-2525
191	-1272	-3875
211	2718	4475
241	-2222	-1100
251	-4252	500
271	-6612	-3625
281	-3942	-2225
311	3693	3025
331	4383	2225
401	6348	11225
421	16238	725
431	-9892	-10100
461	-14507	1525
491	28	6275
521	-8937	-10525
541	12628	11275
571	20788	-2900
601	1073	18875
631	-20867	-10475
641	7378	-15500
661	-17107	-27225
691	-31197	3025
701	7973	27275
751	-16827	-33275
761	-25732	-7625
811	22943	2525
821	-15437	-25475
881	133	32275
911	-3732	26900
941	-18472	23225
971	14088	46100
991	28903	47275
1021	-8687	-4275
1031	-49692	8275
1051	31673	4275
1061	-38432	-45725
1091	38278	43625
1151	-50502	9025
1171	-67012	-6525
1181	67458	12100
1201	20098	-38975
1231	26708	33275
1291	-53497	-35725
1301	16773	-21025
1321	-7062	-25475
1361	-38107	-50275
1381	48858	80975
1451	-7652	-70475
1471	-40637	24525
1481	51458	16775
1511	-8432	-69775
1531	-51942	11275
1571	-13062	2525
1601	100748	10475
1621	42288	18775
1721	-128537	-17525
1741	-108372	-7025
1801	142398	16475
1811	-4932	-46100
1831	-7242	51475
1861	96968	-8875
1871	-64862	-139525
1901	-29777	26725
1931	107833	98725
1951	128073	2225
2011	-148932	-49900
2081	-3717	-30725
2111	102043	148025
2131	103633	-54225
2141	32553	-57025
2161	200743	225
2221	-11262	68275
2251	204948	4775
2281	29783	-112275
2311	23293	93475
2341	199953	-9025
2351	87648	-34100
2371	-102612	52225
2381	62558	165500
2411	98768	206900
2441	-141697	42775
2521	-230362	12375
2531	-57717	-114025
2551	113423	-75475
2591	128953	-36025
2621	-142912	68875
2671	-262487	5275
2711	-76032	-142525
2731	-104192	-134900
2741	155078	-26125
2791	45628	-150975
2801	-87352	-153775
2851	84823	214875
2861	134293	264025
2971	275363	-28225
3001	-146952	-294025
3011	219843	-63475
3041	-263897	-27275
3061	94118	105500
3121	212338	58000
3181	108858	230275
3191	-133847	-229525
3221	183338	96100
3251	181448	299900
3271	-213562	-228775
3301	276798	60400
3331	97408	49900
3361	-12082	5900
3371	129138	-152275
3391	-178572	-338900
3461	-244332	-207625
3491	261753	241975
3511	-199057	-262525
3541	64378	-115100
3571	47563	116275
3581	393708	-16375
3631	-434192	-2375
3671	-74387	-118775
3691	417278	15975
3701	152398	166375
3761	-133182	-365900
3821	-51462	59600
3851	-144352	-33725
3881	-451142	-48400
3911	-313382	108475
3931	-422792	-79775
4001	-281127	-331375
4021	-281912	-10475
4051	-222352	-422775
4091	-354922	-142525
4111	-193732	150975
4201	406523	-46125
4211	-386532	-157900
4231	296808	118975
4241	284878	-165275
4261	-284357	-416375
4271	130138	87625
4391	463553	191225
4421	-263562	200125
4441	-245097	-313525
4451	-109402	284525
4481	270333	525775
4561	382568	-51475
4591	204028	-251375
4621	265788	552025
4651	276348	131225
4691	-13347	-58525
4721	-280162	-339275
4751	-412452	-143900
4801	-28577	-425475
4831	-525967	-94975
4861	-636282	2000
4871	-34112	-71900
4931	308108	206900
4951	-612277	-81225
5011	234468	397525
5021	-190662	208400
5051	494473	-131375
5081	544383	203975
5101	-490477	-26725
5171	-361737	-456475
5231	-50417	-84725
5261	420468	554525
5281	-381892	-559375
5351	-608752	-6275
5381	599258	86900
5431	-514767	151525
5441	-283822	268400
5471	-200712	-60500
5501	-265177	288025
5521	690213	51775
5531	-205842	-184525
5581	492258	180100
5591	507653	525625
5641	-691322	-92900
5651	421248	339025
5701	88473	-443725
5711	634668	359500
5741	-813472	-65725
5791	258603	324725
5801	76523	47225
5821	83938	-439100
5851	-72477	-586225
5861	540018	-208400
5881	-554867	-147725
5981	871308	65225
6011	281843	627775
6091	108353	-326475
6101	-641602	-362225
6121	-329362	-769525
6131	-548367	126025
6151	219373	126775
6211	584668	443125
6221	911338	-40400
6271	-683112	-443125
6301	-292102	-796275
6311	146168	709225
6361	813018	-124400
6421	584188	-136125
6451	129073	-517775
6481	-286792	195525
6491	-466747	-913525
6521	-101287	-341975
6551	-1032727	-34525
6571	213788	790100
6581	423458	-362000
6661	-908357	-68225
6691	-142472	575725
6701	-218602	363625
6761	876068	-38275
6781	701283	-256775
6791	-657572	-420500
6841	-234647	-196475
6871	1069788	47900
6911	551118	902975
6961	-584207	-896375
6971	-347212	-927625
6991	-734672	-100125
7001	1026298	-34025
7121	-810362	19225
7151	-1032327	-43625
7211	-291907	-935275
7321	1113288	120725
7331	-208342	-789725
7351	-633752	-741275
7411	-398107	382775
7451	41723	765025
7481	546683	810725
7541	574728	-209275
7561	-599682	-1155475
7591	262978	942525
7621	-681462	232525
7681	602483	779525
7691	719353	858625
7741	213903	970525
7841	1039728	-204725
7901	-562702	-438625
7951	305948	-442525
8011	-623307	-1113025
8081	513408	1069525
8101	628648	1226025
8111	-1288107	-100025
8161	173518	-767600
8171	-198237	330775
8191	757428	278900
8221	-1007012	-722975
8231	-840067	-1054525
8291	-41522	690475
8311	270568	-662225
8431	696608	793025
8461	-1485882	16400
8501	-48202	931100
8521	-665787	-1363225
8581	539083	-36875
8641	377428	1131475
8681	727158	1142000
8731	1375383	33875
8741	-1168347	-652475
8761	148443	898225
8821	-1037837	171475
8831	-1457992	96100
8861	1518843	225625
8941	748553	-369475
8951	-602852	-540125
8971	-1525587	-272375
9001	1688073	-11975
9011	1043018	-3125
9041	-447522	49100
9091	-336772	-864100
9151	1145998	918025
9161	-416757	418225
9181	-1145017	-917725
9221	-1296962	288875
9241	880878	233225
9281	1152033	-198025
9311	791118	1576375
9341	1174778	892375
9371	880288	488275
9391	-886072	-836275
9421	-56387	425475
9431	865608	-564100
9461	-1288282	-892900
9491	1329828	532625
9511	687968	1154900
9521	1517938	-172400
9551	-1694202	-204725
9601	-772502	-427025
9631	517183	-771125
9661	-1546807	-49375
9721	-433662	885725
9781	1718158	-16400
9791	454103	-765775
9811	-725582	-1188275
9851	-1372427	358625
9871	-470712	-1300225
9901	-243277	-849025
9931	528858	1543525
9941	1346403	907475

TABLE 5

q	C(0,7,q)	C(1,7,q)	C(2,7,q)	q	C(0,7,q)	C(1,7,q)	C(2,7,q)	q	C(0,7,q)	C(1,7,q)	C(2,7,q)	q	C(0,7,q)	C(1,7,q)	C(2,7,q)
29	5199	-2597	-5831	1163	-51990108	69471612	30063460	2647	858603576	193450726	-378971831	4243	1306286203	55871711	196147931
43	8265	-7889	343	1289	-57494369	14383509	-10310727	2689	-19853983	69190107	153738431	4271	-1547008584	-262417736	-324669296
71	-35093	47971	34643	1303	84758490	-28573125	-44954756	2731	-533629140	-281358980	67785228	4327	1856308431	3793237	172125877
113	99594	-144403	-111230	1373	114110953	-92555365	-82380417	2801	399937620	84815325	179507678	4397	-2671539271	484910419	1881282627
127	-209568	173509	204330	1429	10122138	54386717	20399288	2843	-791644835	320577453	448411593	4481	-3078426822	-641541712	1353967069
197	-201147	88053	-179291	1471	104047921	-98830501	-94092789	2857	611717594	-4992708	-237239380	4523	2645905554	-67022935	-340461898
211	1405689	107261	-719173	1499	-65300139	-29473647	-26232983	2927	-884872	369507726	-49905471	4621	2607160323	-1648959613	-2218974457
239	1434998	213934	-820015	1583	-105126142	-52518102	-5390931	2969	292961352	383098758	-152727659	4649	2070808878	547282715	-331072910
281	1135251	164297	203399	1597	-31948338	127974378	27495027	3011	807688453	-641289607	-522537029	4663	2623307622	-1378242355	-1349704902
337	-1621230	1923446	2135861	1667	-107556521	-10916269	-39682503	3067	727907647	-95506635	38713381	4691	-2502433901	721430969	653283337
379	-5130477	2995125	4487959	1709	-128888538	-19650568	61256860	3109	-321401838	-75951764	143668392	4733	-3640717978	-897543633	1157111970
421	5998291	900081	73255	1723	-251830686	-6875288	23281125	3137	-684688860	642265540	481997075	4789	2503258315	-1288303051	-2306029131
449	109674	-4578021	-1250284	1877	213712889	-67891215	-103662489	3221	1032304089	13046789	-630416213	4817	2392716723	-1804998839	-972636721
463	7170357	-5701003	-2821959	1933	-325960798	121787785	265261402	3319	1594734174	478436049	-602508214	4831	3297127440	-913128181	-2380050148
491	11305523	2322257	-4927685	2003	-356330368	76001548	257413856	3347	410454063	-774625369	-343842751	4943	2078861097	-1566888729	-2251794265
547	-7279477	-1790019	1725731	2017	-120735498	278730179	84069986	3361	1006353381	-909797259	-751471595	4957	3369667635	-605577231	-911286761
617	-14976453	-5617605	5786263	2087	-368547223	-3340379	87440745	3389	-981389334	-546310212	279347432	4999	-778583052	-1738072336	-172038412
631	15175284	2170504	-118188	2129	-376912419	161860671	264240977	3529	-1269418404	580125210	264208147				
659	-9476315	7532525	11847661	2143	217740192	-101841208	-52949008	3557	725591711	-9791915	23750741				
673	-12282174	12600252	12905228	2213	-448102587	135107063	245219765	3571	633784653	-1001872963	-341350611				
701	10792521	-2656241	-1863617	2269	336702399	-363165901	-216692259	3613	1332480441	-730397871	-1203852629				
743	-7228076	17252753	4856782	2297	474106148	-113971305	-158732658	3697	800419548	83590864	301799575				
757	11733531	-22794261	-7669137	2311	-605685852	-179377681	203273462	3739	1112087268	-1205587180	-695845276				
827	-23656481	16263737	27354397	2339	-160779075	-187582241	-15710821	3767	1823330703	109364325	-167699903				
883	-12154305	19328295	3384381	2381	-452527980	93027725	73591042	3823	165647046	-627189710	117497149				
911	47995260	-3388203	-6742988	2423	-549704451	30978045	27607727	3851	-484284145	-359801169	496884843				
953	-42151818	38409924	17261524	2437	665456181	134229277	-211190343	3907	-1160308123	1354052427	562632161				
967	-22156752	28839440	21113169	2521	623176846	130163600	-102839877	4019	-1880121329	-75053545	80430217				
1009	50636066	-39230282	-40569893	2549	672228303	-130070451	-420202195	4159	-1905773823	-247612729	125148009				
1051	-74745981	-5541655	10374231	2591	24336324	-385760193	-73912286	4201	-2162483465	250456983	168340333				
1093	69239721	-10283777	-25456725	2633	-551928288	185022922	285335183	4229	1296278415	-29007461	-742607299				

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

$$(5.5) \qquad (A5^n - 1)^{(q-1)/2} \not\equiv 1 \pmod{q}$$

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 $5^i k \pmod{19531}$ ($i = 0, 1, 2, \ldots, 8$), where $k \in \{0, 66, 576, 652, 676, 772, 1348, 1492, 1677, 1891, 2108, 2301, 2552, 2893, 3372, 3466, 3593, 3624, 5453\}$. Also, if $k = 66, 652, 5453$, then $5^i k \in \mathcal{S}(5, 5, 19531)$. We also have $19531 = 156^2 - 5.31^2$, $C(0, 5, 19531) = -2590642$ 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 $A \equiv 5^i j \pmod{31}$, where $j \in \{5, 11, 17, 20\}$ and $n \not\equiv -i \pmod 3$, 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 *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 $P = 2X$, $Q = 5Y^2$ 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

$$V_A \equiv V_{A/2}^2 - 2Q^{A/2} \not\equiv 2Q^{A/2} \pmod N.$$

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 ($0 < m \leqslant n$) such that

$$W_{Ar^m/2} \equiv 2\eta \pmod{N} \tag{6.1}$$

and

$$G_2(W_{Ar^{m-1}}) \equiv 0 \pmod{N}.$$

If (6.1) holds for any N, then we know that if p is any prime divisor of N, we must have $p \mid U_{Ar^m}$ and $p \nmid U_{Ar^{m-1}}$. 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 $L \equiv 5Y(4X)^{-1}(W_{k+1} + W_k) \pmod{N}$.

(3) If $L^2 \equiv 5 \pmod{N}$, put $R \equiv (-1 + L)2^{-1} \pmod{N}$ 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 $m \leqslant n + 1$ 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 $W_k \not\equiv 0 \pmod{N}$, then $V_{A/2} \not\equiv 0 \pmod{N}$ and

$$V_A \not\equiv -2Q^{A/2} = 2\eta Q^{A/2} \pmod{N}.$$

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 $W_k \equiv 0 \pmod{N}$, put

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

where $L \equiv (4XY)^{-1}QW_{k+1} \pmod{N}$ and go to step (6).

(4) If $W_k \not\equiv 0 \pmod{N}$, put

$$S_1 = W_{2k} \equiv W_k^2 - 2 \pmod{N}.$$

(5) Determine $S_{i+1} \equiv G_2(2 - S_i^2)S_i \pmod{N}$ for $i = 1, 2, \ldots$ until we find some $m \leqslant n + 1$ such that $S_m \equiv 2\eta \pmod{N}$. 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) 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 $N = A5^n - 1 = 2 \cdot 10^n - 1$ $(n \geqslant 3)$, 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 $138007919535942456000 \nmid n$.

(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

$$\begin{aligned} Y_{j+1} &= Y_j^2 - 2 \quad \pmod{N}, \\ Z_{j+1} &\equiv Z_jY_j \qquad \pmod{N}, \qquad j = 0, 1, 2, \ldots, n-1. \end{aligned}$$

(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 $S_1 \equiv Y_{n-1}^2 - 2 \pmod{N}$.

(4) Compute

$$S_{i+1} \equiv G_2(2 - S_i^2)S_i \pmod{N}$$

until we find some $m \leqslant n + 1$ such that $S_m \equiv -2 \pmod{N}$. If no such m exists, N is composite; if $m \geqslant 3n/4$, N is a prime; if $m < 3n/4$, put $R \equiv S_{m-1}^2 - 2$.

(5) Select q from the list given in Section 5 and find $C(0, 5, q)$, $C(1, 5, q)$ from Table 4. Compute

$$P \equiv C(0, 5, q) + C(1, 5, q)R, \qquad Q \equiv q^3 \pmod{N}.$$

(6) Compute $Y_0 \equiv P^2Q^{-1} - 2 \pmod N$ and determine $S_1 \equiv Y_n \pmod N$ from

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

(7) Use

$$S_{i+1} \equiv G_2(2 - S_i^2)S_i \pmod N \quad (i = 1, 2, 3, \dots, n-1)$$

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

Test 2 can be used when $N \equiv 3 \pmod 8$; 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 $V_{A/2} \not\equiv 4Q^{A/4} \pmod N$ and $V_A \not\equiv 2\eta Q^{A/2} \pmod N$. Thus, in the case where $N \equiv 3 \pmod 8$, 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, $W_{k+1} \pmod N$, 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 $R \equiv (-1 + L)2^{-1} \pmod N$ and go to step 6. Otherwise,

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

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 $9 \nmid A$. We need not, of course, consider the case of $A \equiv 1 \pmod 3$.

Let c ($= 1$ or 2) be such that $cB \equiv 1 \pmod 3$, where $B = A/6$. Since $N \equiv -1 \pmod 3$, we have $\varepsilon = (\Delta/N) = (-3/N) = -1$ 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,

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

must be solvable; thus,

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

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

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

then $N \mid U_A$. If $N \mid U_A$, by (2.3) we have $N \mid U_{A/3}$ 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

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

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

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

is a solution of (6.2).

From (2.16) we get

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

and by (2.3),

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

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

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

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

(3) Put

$$M \equiv 8B^3 7^{3n}\left(91 W_k^3 + 147 W_k^2 W_{k+1} - 49 W_{k+1}^3\right) \pmod N,$$

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

(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 $m \leqslant n + 1$ such that $S_m \equiv 2\eta^c \pmod{N}$. 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 $R \equiv S_{m-1}^2 - 2 \pmod{N}$.

(5) Select q and determine $C(0,7,q)$, $C(1,7,q)$, $C(2,7,q)$. Put

$$\begin{aligned} P &\equiv C(0,7,q) + C(1,7,q)R + C(2,7,q)R^2 \pmod{N}, \\ Q &\equiv q^5 \pmod{N}, \\ S_1 &\equiv W_{A/2} \pmod{N}. \end{aligned}$$

(6) Using

$$S_{i+1} \equiv -G_3(2 - S_i^2)S_i \pmod{N},$$

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 $A \not\equiv 2 - 3n \pmod 9$, 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 $\varepsilon = (\Delta/N) = 1$ 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

1. C. Cailler, "Sur les congruences du troisième degrée," *Enseign. Math.*, v. 10, 1908, pp. 474–487.

2. L. Carlitz & H. H. Ferns, "Some Fibonacci and Lucas identities," *Fibonacci Quart.*, v. 8, 1970, pp. 61–73.

3. L. E. Dickson, *History of the Theory of Numbers*, Vol. 1, Chelsea, New York, 1952.

4. J. H. Halton, "On a general Fibonacci identity," *Fibonacci Quart.*, v. 3, 1965, pp. 31–43.

5. K. Inkeri, "Tests for primality," *Ann. Acad. Sci. Fenn. Ser. A*, No. 279, 1960.

6. Dov Jarden, *Recurring Sequences*, Riveon LeMathematica, Jerusalem, 1966.

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

8. D. H. Lehmer, *Computer Technology Applied to the Theory of Numbers*, MAA Studies in Mathematics, vol. 6, 1969, pp. 117–151.

9. Emma Lehmer & H. S. Vandiver, "On the computation of the number of solutions of certain trinomial congruences," *J. Assoc. Comput. Mach.*, v. 4, 1957, pp. 505–510.

10. H. Riesel, "A note on the prime numbers of the forms $N = (6a+1)2^{2n-1} - 1$ and $M = (6a-1)2^{2n} - 1$," *Ark. Mat.*, v. 3, 1956, pp. 245–253.

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

12. H. C. Williams, "An algorithm for determining certain large primes," *Congressus Numerantium III, Proc. Second Louisiana Conf. on Combinatorics, Graph Theory and Computing*, Utilitas Math., Winnipeg, 1971, pp. 533–556.

13. H. C. Williams, "The primality of $N = 2A3^n - 1$," *Canad. Math. Bull.*, v. 15, 1972, pp. 585–589.

14. H. C. Williams, "Some properties of a special set of recurring sequences," *Pacific J. Math.*, v. 77, 1978, pp. 273–285.

15. H. C. Williams, "The primality of certain integers of the form $2Ar^n - 1$," *Acta Arith.*, v. 39, 1981, pp. 7–17.

16. H. C. Williams, "A class of primality tests for trinomials which include the Lucas-Lehmer test," *Pacific J. Math.*, v. 98, 1982, pp. 477–494.

17. C. R. Zarnke & H. C. Williams, "Computer determination of some large primes," *Congressus Numerantium* III, *Proc. Second Louisiana Conf. on Combinatorics, Graph Theory and Computing*, Utilitas Math., Winnipeg, 1971, pp. 563–570.