PACIFIC JOURNAL OF MATHEMATICS
Vol. 98, No. 2, 1982

A CLASS OF PRIMALITY TESTS FOR TRINOMIALS WHICH INCLUDES THE LUCAS-LEHMER TEST

H. C. WILLIAMS

When n is an odd prime, the well-known Lucas-Lehmer test gives a necessary and sufficient condition for primality of 2^n-1. In this paper,primality tests of a similar character are developed for certain integers of the form $Ab^{2n}+Bb^n-1$ and a criterion which generalizes the Lucas-Lehmer test is obtained.

1. Introduction. Let $N = 2^n - 1$ where n is an odd prime. The Lucas-Lehmer test for the primality of N reads as follows:

If we put $T_0 = 4$ and define $T_h \pmod N$ by setting $T_{k+1} \equiv T_k^2 - 2 \pmod N$ for $k \geqq 0$, then N is prime if and only if $N \mid T_{n-2}$.

(For proof, see [10, p. 443] or [13, p. 194]. This very elegant test has attracted a great deal of attention (see Williams [17] for a bibliography.) It is also the means by which the largest known primes have been found over the past twenty years.

While the Lucas-Lehmer criterion would only be used when n is a prime, it should be noted that it holds for any odd $n \geqq 3$. When viewed in this way, it falls into a class of primality tests characterized by the following three properties.

(i) The test is restricted to values of N given by some function involving an exponent n which usually belongs to some fixed congruence class and exceeds a certain bound.

(ii) A sequence $\{T_h: h \geqq 0\}$ is employed, where T_0 is an easily calculated integer and T_{k+1} is defined $\pmod N$ for $k \geqq 0$ by $T_{k+1} \equiv f(T_k) \pmod N$ where f is some polynomial such that $f(Z) \subseteqq Z$.

(iii) Write $T[k]$ for T_k where $k = m_i$. Then N is prime if and only if $h(T[m_i]: 1 \leqq i \leqq \ell) \equiv 0 \pmod N$ where h is a Z-valued polynomial over Z^ℓ for some $\ell \geqq 1$ and the m_i depend on n.

We say that any test with the properties i) through iii) is a primality test of Lucas-Lehmer (or LL) type. Such tests have been given for integers of the form $Ac^n - 1$ with $c = 2$ (Lehmer [10, p. 445]; Riesel [11], [12]; Inkeri [5]; Stechkin [14] and with $c = 3$ (Williams [16]). In this paper, we develop some tests of LL type for integers of the form $Ab^2 + B^n b^n - 1$ and in particular a criterion (Theorem 2) is obtained when $b = 2$ which yields a large number of examples including of original LL test ($A = 2$, $B = 0$) and the new case $A = 2$, $B = \pm 3$. Further, we are able to show that an LL primality test exists even for integers of the form

$$10^{2n} \pm 10^n - 1 .$$

2. The Lucas functions: congruence and divisibility properties. We define the Lucas functions to be

$$(2.1) \qquad U_n = U_n(P, Q) = (\alpha^n - \beta^n)/(\alpha - \beta) , \quad V_n = U_{2n}/U_n ,$$

where α and β are roots of the auxiliary quadratic

$$x^2 - Px + Q = 0$$

and exclude the case $\alpha\beta = 0$, i.e. $Q = 0$. (Here and in the sequel all latin letters denote integers unless stated otherwise.) U_n and V_n are defined in the obvious manner when $\alpha = \beta$ or $\alpha^n = \beta^n$ so that $V_0 = 2$.

REMARK. By virtue of Theorems 1, 2, 4, we can also exclude the case $\alpha = \beta$ which holds if and only if $P^2 = 4Q$

In employing these functions (mod N) we frequently use the following lemma connecting $U_n(P, Q)$, $V_n(P, Q)$ and related Lucas functions with second argument unity.

LEMMA 1. *We have* $U_{tm}/U_m \in Z$ *if* $t, m > 0$. *In particular* U_n, $V_n \in Z$ *for* $n > 0$ (*and for* $n = 0$). *If* $QP' \equiv P^2 - 2Q \pmod N$ *and* $(Q, N) = 1$ *we have*

$$(2.2) \qquad U_{2tm}/U_{2m} \equiv Q^{(t-1)m} U'_{tm}/U'_m \quad \textit{and} \quad V_{2m} \equiv Q^m V'_m (t, m > 0)$$

where $U_{2k} = U_{2k}(P, Q)$, $U'_k = U_k(P', 1)$ *and likewise for the* V's.

(Until further notice, all congruences hold (mod N).)

REMARK. When $U_h = 0$, and in particular $h = 0$, we interpret U_{th}/U_h in the natural manner, i.e. as $t\alpha^{(t-1)}$.

Proof. We have $U_{th}/U_h \in Z[P, Q]$ since it is symmetric in α and β, so by (2.1) it remains only to consider the first part of (2, 2). Determine γ, δ by the conditions $\gamma + \delta = P'$, $\gamma\delta = 1$, so that our congruence is of the form $A(\alpha^2, \beta^2) \equiv A(Q\gamma, Q\delta)$, where $A(x, y)$ is a symmetric Z-polynomial in x and y. Hence it can be expressed as $B(V_2, Q^2) \equiv B(QP', Q^2)$ with $B(x, y) \in Z[x, y]$. Since $V_2 = P^2 - 2Q$, this completes the proof.

It is convenient to prove now the following result which is used in §3. We have

PROPOSITION 1. *The following three assertions are equivalent*:
(i) $U_h(P, Q)$ *or* $U_h(P', 1) = 0$ *for some* (*minimal*) $h > 0$;

(ii) *$\alpha^2 = Q\rho$ or $\gamma = \rho$ respectively, where ρ is a primitive hth root of 1 with $h|4$ or 6, $h \geqq 2$;*

(iii) *$P^2 = cQ$ with $c \leqq 3$, or $-2 \leqq P' \leqq '1$ respectively.*

For $(Q, N) = 1$ set $P' + 2 = c$, $0 \leqq c < N$ so that $P^2 \equiv cQ \pmod N$. Then the two inequalities in (iii) are equivalent.

REMARK. Let $\alpha \neq \beta$. Then U_n and V_n are bounded if and only if α and β are roots of 1, this being an easy consequence of the partial-fraction expansion of the respective generating functions.

REMARK. Since U_n and V_n are here of the form $Q^{n/2}B(n)$, where $B(n)$ is uniformly bounded, it is intuitive on examining the later Theorems and LL-type tests (§§ 3–5) that this case will be useless therein. Hence it seems desirable to enumerate these "degenerate" Lucas sequences in this paper. We will see that this case is excluded in Theorem 2, but not in Theorems 1 and 4.

Proof. Set $\alpha^2 = Q\rho$ so that $\beta^2 = Q\rho^{-1}$, $\rho + \rho^{-1} = P^2/Q - 2 =: a$, and $P^2 = (a + 2)Q$. (The discussion for γ and δ is the same so we omit it.) We first show that (i) implies (ii) and (ii) implies (iii). We have $\rho^h = 1$ so that ρ has degree $\leqq \min(2, \phi(h))$ over Z and $h|4$ or 6. We require that $\alpha \neq \beta$ which holds if and only if $\rho \neq 1$, i.e. $h \geqq 2$. Moreover $a \in Z$ so that $-2 \leqq a \leqq 2$ and $c \leqq 3$. We now show that (iii) implies (i). For each a above there exists a $\rho + \rho^{-1} = a$ and $\rho^h = 1$ with $h \geqq 2$.

The last assertion is trivial so the proof is complete.

REMARK. The discussion here is like that in [1, 35–36] but more general.

In the sequel we use the following expansion of V_{nm} in terms of V_m when $Q = 1$ or $m = 1$. (We suppress the parameters P and Q of the Lucas functions when their values are obvious from or irrelevant to the context.)

LEMMA 2. *Define $F_n = F_n(x)$ by setting $F_0 = 2$, $F_1 = x$ and $F_k = xF_{k-1} - F_{k-2}$ for all k. Then*

(i) *$F_{-n} = F_n$ for all n;*

(ii) *$V_{nm} = Q^{nm/2}F_n(V_mQ^{-m/2})$ for all n, m, where $Q^{1/2}$ is fixed;*

(iii) *$F_n(x) = \sum_0^j (-1)^r(n/(n-r))\binom{n-r}{r}x^{n-2r}$ for $n \geqq 1$, where $j = [n/2]$.*

(iv) *$F_n(x) = 2\cos nz$ for all n, where $x = 2\cos z$.*

Proof. (i) Set $F_1(x)(=x) = t + t^{-1}$ as a formal equality. Then the above recurrence gives $F_n(x) = t^n + t^{-n}$ and (i) follows at once.

(ii) Choose any square roots of α and β and set $\theta = (\alpha/\beta)^{1/2}$. Then $V_{nm}Q^{-nm/2} = \theta^{nm} + \theta^{-nm} = F_n(\theta^m + \theta^{-m})$ which gives (ii).

(iii) We find without difficulty that $\sum_{n=1}^{\infty} F_n(x)y^{n-1} = \sum_{k=0}^{\infty}(x - 2y)(xy - y^2)^k$ as a formal identity or as an absolutely convergent series when $|xy| + |y^2| < 1$, from which (iii) follows after term-by-term integration in y.

(iv) This follows at once on setting $t = e^{iz}$ above (and is of course well-known).

The following lemma will play a crucial role in the later work. We have.

LEMMA 3. *Set* $W_t(P, Q) = W_t = (U_{t(m-\ell)}U_{t(m+\ell)})/(U_{m+\ell})$ *and* $J_t(x, y) = ((F_t(x) - F_t(y))/(x - y) \in Z[x, y]$.

(i) *For* $Q = 1$ *we have*

$$W_t = J_t(V_{2m}, V_{2\ell}) \ . \tag{2.3}$$

(*We define* W_t *and* J_t *by the above convention when a zero denominator occurs.*)

(ii) *For* $(Q, N) = 1$ *set* $L_n = V_n(P', 1)$ *for* P' *as in Lemma* 1 *and take* $t \geqq 1$. *Then*

$$J_t(L_m, L_\ell) \equiv Q^{m(1-t)}W_t(P, Q) \quad \text{if} \quad 2\,|\,(m, \ell) \ , \tag{2.4}$$

where Q^{-k} *has the usual meaning* (mod N) *for* $k > 0$.

REMARK. The expansion of $J_t(x, y)$ in x and y is obtainable at once from (ii) of Lemma 2.

Proof. Our two formulas follow without difficulty from (2.1) and (2.2) respectively.

In the rest of this section we present some divisibility and congruence properties of the U_n and V_n. Though these results are known (see [10] or [1]) we supply proofs for the reader's convenience. For a given $m \geqq 1$ such that $(m, Q) = 1$ we define $\omega = \omega(m)$ to be the least positive k such that $m\,|\,U_k$.

Define

$$\varDelta = P^2 - 4Q = (\alpha - \beta)^2 \tag{2.5}$$

Then we have

LEMMA 4. (i) *If* $2 \nmid m$ *and* $m\,|\,U_n (n > 0)$ *then* $\omega(m)\,|\,n$.

(ii) $\omega(p)\,|\,p-(\Delta\,|\,p)$ *where* p *is an odd prime (here and below) and* $(\Delta\,|\,p)$ *denotes the Legendre symbol.*

(iii) *If* $(\Delta\,|\,p) = -1$ *we have*

$$V_{p+1+k} \equiv QV_k \equiv Q^{k+1}V_{-k} \pmod{p} . \tag{2.6}$$

REMARK. The conclusion of (i) hold also if $2\,|\,m$ but we will not need that case.

In the proof we use the following simple identities:

$$2Q^k U_{n-k} = U_n V_k - U_k V_n , \tag{2.7}$$

$$2U_{n+k} = U_n V_k + U_k V_n , \tag{2.8}$$

$$2V_{n+k} = V_n V_k + \Delta U_n U_k . \tag{2.9}$$

(Observe that (2.7) becomes (2.8) on multiplying by Q^{-k} and replacing $-k$ by k in the result, and that (2.8) and (2.9) are essentially the same.)

Proof of (i). In (2.7) take $k = h\omega > 0$ where $n-k = r(0 \leqq r < \omega)$. It follows by Lemma 1 that $m\,|\,U_r$ so $r = 0$ by definition ω.

Proof of (ii). By definition of α and β we assume that $2\alpha = P + \sqrt{\Delta}, 2\beta = P - \sqrt{\Delta}$ for a fixed square root of Δ. It follows by a standard congruence for binomial coefficients and Euler's criterion that $2^p U_p \equiv 2(\Delta\,|\,p)$ or $U_p \equiv (\Delta\,|\,p)$ and $V_p \equiv P = V_1$. (All congruences hold (mod p) in this proof.) We thus obtain (ii) at once if $p\,|\,\Delta$. Next by (2.7) and (2.8) with $n = p, k = 1$ we get $2QU_{p-1} \equiv V_1(U_p - U_1) \equiv P((\Delta\,|\,p) - 1)$ and $2U_{p+1} \equiv P((\Delta\,|\,p) + 1)$. Hence the assertion follows when $p \nmid \Delta$ since $p \nmid Q$.

Proof of (iii). By (2.7) we get $-2Q \equiv U_{p+1}V_1 - V_{p+1}$ so that $V_{p+1} \equiv 2Q$ by (ii). Suppose now that $k \geqq 0$. Then by (2.9) we obtain the first part of (2.6) and the second part follows trivially. If $k < 0$ the result follows in the same way on interpreting $Q^k \pmod{p}$ for $k < 0$ as in (2.4).

In Theorems 2 and 4 we use the following simple corollary. We have

LEMMA 5. [10, pp. 441]. *If* $(\Delta\,|\,p) = (Q\,|\,p) = -1$, *then* $p\,|\,V_m$ *where* $m = (p+1)/2$.

Proof. Square V_m and apply (2.6) with $k = 0$.

LEMMA 6. *If* $r, s \geqq 1$, *we have* $(U_{rs}/U_s, U_s)\,|\,rQ^{sm}$ *where* $m = [r/2]$.

(*We recall that this quotient is an integer by Lemma* 1.)

Proof. Though we only need the case r a prime, the proof is no more difficult for arbitrary r. Set $C_k = C_k(x, y) = (x^k - y^k)/(x - y)$ $(x \neq y)$ and $C_k(x, x) = kx^{k-1}$ so that $C_k(\alpha, \beta) = U_k$ by (2.1), and determine $A = A(x, y)$ by the condition

$$C_{\varepsilon s+1}(C_{rs}/C_s) - AC_s = r(xy)^{sm} \qquad (2\varepsilon = 1 + (-1)^r) . \tag{2.10}$$

The proof of our Lemma will clearly follow as soon as we show that $A(\alpha, \beta) \in Z$. On setting $t = x^s$, $u = y^s$ we get $(t - u)A = (x - y)AC_s = xD(t, u) - yD(u, t)$ where $D(t, u) = t^\varepsilon C_r(t, u) - r(tu)^m$. Since $\varepsilon + r - 1 = 2m$ we have $D(t, t) = 0$ so that $A(x, y) \in Z[x, y]$. By (2.10) we have $A(x, y) = A(y, x)$ and the assertion follows.

REMARK. If $(P, Q) = 1$ we can replace rQ^{sm} above by r, but this refinement is not required. Carmichael [1, p. 51] proves this latter assertion for r prime only and by a different method.

From this we derive a lemma similar to Theorem 5.3 of [10].

LEMMA 7. *If r is a prime such that $(r, N) = 1$ and $U_{rs}/U_s \equiv 0 \pmod N$ where $s > 0$ and $(Q, N) = 1$, then any odd prime divisor p of N is $\equiv \pm 1 \pmod{r^{j+1}}$ where $r^j \mid s$.*

Proof. Let $p \mid N$ so that $p \nmid U_s$ by Lemma 6 and define $\omega(m)$ as in Lemma 4. Then $\omega(p) \mid rs$ and $\omega(p) \nmid s$ which gives $r^{k+1} \mid \omega(p)$ if $r^k \| s$ where $k \geqq j$. The result now follows form (ii) of Lemma 4.

3. Some primality criteria for quadratic polynomials in powers of an integer. We shall be concerned in what follows with primality criteria for the numbers N such that

$$N = N_n =: Ab^{2n} + Bb^n - 1;\ 2 \nmid N;\ b \geqq 2;\ A, n, N \text{ all} > 0 , \tag{3.1}$$

Here A and B are fixed parameters and we can assume that Ab^{-2} and Bb^{-1} are not both integers. In the following theorem we will take $b = ar$ where r is a (fixed) prime. (The references in §1 deal with "linear polynomials" of this type, i.e. numbers of the form $Ab^n - 1$.) We exclude the following two cases since N is then composite or trivial: $B^2 + 4A$ a square; $B = 0$, $A = b \geqq 3$. Other exclusions will be presented later.

We being with some sufficient conditions for N to be prime.

LEMMA 8. *Suppose that $b = ar$ with $r^n > Aa^{2n} + |B|a^n$. (Here and later we take $r > 0$.) If some prime factor of N is $\equiv \pm 1 \pmod{r^n}$ then N is prime.*

Proof. Set $e = r^n$, $C = Aa^{2n}$, $D = Ba^n$ (so that $e > 1$). Let $p \mid N$ with $p \equiv \pm 1 (\bmod e)$ and assume that N is composite. We show that $e \leqq C + |D|$. Since $N \equiv -1 \pmod e$ we have $N = (he - 1)(je + 1) = Ce^2 + De - 1$ for some $h, j > 0$, so that $Ce + D = hje + h - j$ and $|C - hj|e = |h - j - D| \leqq hj - 1 + |D|$ as is easily seen. Set $C - hj = t$ so that $t \neq 0$ since $D^2 + 4C$ is non-square. Then $|t|e \leqq C - t - 1 + |D| < C + |D| + |t|$ and the assertion follows.

(The reader can now pass on to the proofs of Theorem 1 and 2.) Somewhat better results can be obtained for special classes of N as follows, where N has a prime factor $\equiv \pm 1 \pmod e$. We note that our hypotheses give $e > 1$ below, as can be easily verified.

LEMMA 9. *Suppose that r is odd $n \geqq 2$. Then N is prime if*
(i) $e \geqq (C - 3)/2 + |D|$,
(ii) $2 \mid a, e > (C + 2|D|)/8$.
(Here and in the next Lemma we use the notation introduced above.)

Proof. We assume that N is composite and follow the proof of Lemma 8. Since e and N are odd, we have $2 \mid (h, j)$. On setting $h = 2k$, $j = 2m$ we get $(C - 4km)e = 2(k - m) - D$. For t as above this gives $e - 1/2 \leqq (e - 1/2)|t| \leqq C/2 + |D| - 2$, which gives (i). If now $2 \mid a$ and $n \geqq 2$ we have $4 \mid (C, D)$ and (ii) follows in the same way.

REMARK. The bounds for e in the preceding Lemmas and in the following one are exact, as can be shown without difficulty.

LEMMA 10. *N is prime if* $2|a$, $e \equiv 1 (\bmod 4)$, $n \geqq 5$ *and* $e \geqq (C + 6|D| - 16)/24$.

Proof. Assume N is composite. By hypothesis we can write $C = 32E$, $D = 32F$ with $E \geqq 32$. (We only need $E \geqq 7$ in the following proof.) The assertion to be proved can now be written as

$$e \leqq (4E - 5)/3 + 8|F| \,. \tag{3.2}$$

As in the proof of Lemmas 8 and 9 we find that

$$(8E - km)e = (k - m)/2 - 8F \tag{3.3}$$

for suitable k and $m > 0$. Set $8E - km = u$, $v = |u|$ so that $u = (C - hj)/4 \neq 0$ and $e - 8|F| \leqq ((k - m)\operatorname{sgn} u)/2v$. Hence (3.2) holds if

$$((k - m)\operatorname{sng} u)/v \leqq (8E - 10)/3 \,. \tag{3.4}$$

We have $u \equiv 0, 1 \pmod 4$ by (3.3) since e is odd and consider 3 cases, namely $v \geqq 4$, $u = 1$, $u = -3$.

(i) $v \geqq 4$. have $|k - m| \leqq km - 1 \leqq 8E + v - 1$, so (3.4) holds if $(8E - 1)/4 \leqq (8E - 13)/3$ and this is so for $E = 7$, hence for $E \geqq 7$.

(ii) $u = 1$. Since $e \equiv 1 \pmod 4$ we have $u \equiv (k-m)/2 \pmod 4$ for all u by (3.3). For $u = 1$ the left side of (3.4) increases with k and $k \equiv 8E - 1$. The choice $k = 8E - 1$ contradicts the last congruence so (3.4) holds if $(8E - 1)/3 - 3 \leqq (8E - 10)/3$ which is true.

(iii) $u = -3$. We maximize m in this case and argue as in (ii).

We are now ready to prove two related theorems, the second of which will yield a large class of LL-type tests. It is convenient to isolate part of the argument as the following

LEMMA 11. *For any $N > 0$ and a, b, P determine $T_k \pmod N$ for $k \geqq 0$ by*

$$T_0 \equiv F_a(P),\ T_{j+1} \equiv F_b(T_j) \tag{3.5}$$

for $F_n(x)$ as in Lemma 2. If $d = gb^k (k \geqq 0)$ write $V[d]$ for $V_d = V_d(P, 1)$ (here and later) to avoid subscripts with exponents. Then

$$F_c(T_k) \equiv V[cab^k] \pmod N . \tag{3.6}$$

Proof. By (2.1) we have $P = V_1$ so (3.6) follows by Lemma 2 and induction.

Let $(.|.)$ denote the Jacobi symbol and define Δ by (2.5). We present first a sufficient condition for primality, namely.

THEOREM 1. *Let $N = Ab^{2n} + Bb^n - 1 > 0$ be odd where $A, b, n > 0$, $b = ar$ with r prime and $B^2 + 4A \neq \square$ (here and in the sequel). Define $T_k \pmod N$ by (3.5). Assume that $r^n > Aa^{2n} + Ba^n$ and find P such that $(\Delta | N) = -1$ with $Q = 1$. If*

$$J_r =: J_r(F_{2A}(T_{2n-1})\ ,\quad F_{2B}(T_{n-1})) \equiv 0$$

where J_r is given by (2.3), then N is prime. (Recall that $F_0(x) = 2$.) If

$$F_{rA}(T_{2n-1}) \not\equiv F_{rB}(T_{n-1})$$

then N is composite. (All congruences hold $\pmod N$ in the rest of this section.)

REMARK. We have $F_{2c} = F_c^2 - 2$ and $F_{rc} = F_r(F_c)$ by Lemma 2.

REMARK. We prove in Proposition 3 below that the required P always exists when N is a non-square, and likewise for P and Q in the following Theorem 2.

Proof. By (3.6) we get $J_r \equiv W_r$ for W_r as in Lemma 3 with $U_k = U_k(P, 1)$, $m = Aab^{2n-1}$ and $\ell = Bab^{n-1}$, so if $N \mid J_r$, any prime factor of N is $\equiv \pm 1 \pmod{r^n}$ by Lemma 7. Hence N is prime by Lemma 8. (We note that $m > |\ell|$ by the inequality for r^n.)

If N is prime we have $V_{rm} \equiv V_{r\ell}$ by by (2.6) so that $F_{rA}(T_{2n-1}) \equiv F_{rB}(T_{n-1})$.

REMARK. It is easy to see by Proposition 1 that if $W_r = 0$, then $N < C$ as we would expect, where C is a universal constant. Thus the above test when applied to a sequence $\{N_n : n > n_0\}$ satisfying (3.1), and with P so chosen that $W_r = 0$, yields no information in this trivial case, a fact which may be considered as a partial check on the above proof.

We now employ Lemma 5 and the argument used to derive the first part of Theorem 1 to obtain a necessary and sufficient condition for the primality of N when $b = r = 2$ which includes the Lucas-Lehmer test.

THEOREM 2. *Let $N = A \cdot 2^{2n} + B \cdot 2^n - 1$ where $2^n > A + |B|$. Determine P and Q such that $(Q \mid N) = (\Delta \mid N) = -1$ and set $QT_0 \equiv P^2 - 2Q$ so that $T_0 = F(P') = P'$ for P' as in Lemma* 1. *If we define T_k by* (3.4) *with $a = 1, b = 2$ and P' for P so that*

$$T_{j+1} \equiv T_j^2 - 2 \qquad (j \geqq 0)\,,$$

then N is prime if and only if

$$J =: F_A(T_{2n-1}) + F_B(T_{n-1}) \equiv 0 (\operatorname{mod} N)\,,$$

where $F_c(x) = F_{-c}(x)$ by (i) *of Lemma* 2.

REMARK. The Lucas-Lehmer test (see §1) is obtained by taking $A = 2, B = 0, Q = -2, P = 2$ and observing that (N prime if and only if $N \mid T_{2n-1}^2$) implies that (N prime if and only if $N \mid T_{2n-1}$). (We must assume $N \geqq 31$; the case $N = 7$ is not covered.)

Proof. Write L_k and V_k for $V_k(P', 1)$ and $V_k(P, Q)$ respectively. By (3.6) with P' for P we have $F_c(T_k) \equiv L[c \cdot 2^k]$. Set $m = A \cdot 2^{2n-1}$, $\ell = B \cdot 2^{n-1}$. By Lemma 3 and (2.1) it follows that $J \equiv L_m + L_\ell = J_2(L_m, L_\ell) \equiv Q^{-m} V_{m-\ell} V_{m+\ell}$, since $(Q, N) = 1$. Thus if $N \mid J$ then N is prime as in Theorem 1. (We have $2 \mid (m, \ell)$ since $n = 1$ gives $2 > A + |B|$ so $A = 1, B = 0$, and $B^2 + 4A$ is a square.)

If N is prime then $V_{m+\ell} \equiv 0$ by Lemma 5 so $N \mid J$.

REMARK. In §5 we use Theorem 2 to construct further LL-type tests.

We now show the case $U_h(P, Q)$ or $U_h(P', 1) = 0$ for some h never occurs in the above proof if $n \geqq 3$ so that the problem of zero denominators does not occur. By Proposition 1 it suffices to verify.

PROPOSITION 2. *Let N, P, Q be given by Theorem 2 with $n \geqq 3$ or $N \equiv -1 \pmod 8$. Then $P^2 \not\equiv cQ \pmod N$ for $0 \leqq c \leqq 3$.*

Proof. Since $(Q, N) = 1$ we can find c such that $P^2 \equiv cQ$. Then $(c \mid N) = -1$, and $(c - 4 \mid N) = 1$ by (2.5). Since $(2 \mid N) = 1$, the assertion follows.

REMARK. Suppose now that $n = 2$ so that $N = 16A + 4B - 1 \leqq 12A + 12 - 1 \leqq 47$. Since $47 \equiv -1 \pmod 8$ and $N \equiv -1 \pmod 4$ we have $P^2 \not\equiv cQ$ if $N > 43$.

We close this section by showing that Theorems 1 and 2 are "effective" in that the required P or P and Q can always be found if a nonsquare. Note that in Theorem 2 it suffices to find P such that $(P^2 + 4 \mid N) = -1$, since we can then take $Q = -1$. We will actually prove the following more general.

PROPOSITION 3. *Let m be odd, >0 and a nonsquare and take $d \not\equiv 0 \pmod m$. Then there exists k such that $(k^2 - d \mid m) = -1$.*

Proof. Set $C_d(m) = \#\{k \pmod m) : (k^2 - d \mid m) = -1\}$. We prove that $C_d(m) > 0$ and begin with the case $m = p$, a prime. In $GF(p)$ we have $k^2 - d = j^2$ for some j if and only if $2k = e + d/e$ for some e, so that $\min(C_d(p), p - C_d(p)) = (p - 1)/2 > 0$. Next let $m = h^2 \prod_{i=1}^{s} p_i$, where the p_i are distinct primes and $s \geqq 1$. By the Chinese Remainder Theorem we can thus determine k such that $(k^2 - d \mid p_i) = -1$ or 1 according as $i = 1$ or $2 \leqq i \leqq s$, which completes the proof.

4. LL-type tests when $b = ar$, r an odd prime, and the theory of cyclotomy.

There is, unfortunately, no simple analogue of Lemma 5 which holds for U_{rk}/U_k with $rk = p + 1$ where p and r are odd primes. However, we can use the theory of cyclotomy to obtain an analogue of Theorem 2 that will be useful when $r = 3$ or 5. We employ here the method of Williams [15].

Let $p, q, r(=2s + 1)$ be odd primes such that $p \equiv -1$, $q \equiv 1 \pmod r$ and let $K = GF(p^{q-1})$. As is customary write $t = \operatorname{ind} m =: \operatorname{ind}_g m$ where $m = g^t$, $0 \leqq t \leqq q - 2$ and g is a fixed primitive root of q. (Herein equality holds in K and Roman letters denote elements of Z or $GF(p)$ unless stated otherwise.) We use the well-known Gauss sum (or Lagrange resolvent)

$$(\xi,\,\omega)=\sum_{1}^{q-1}\xi^{\operatorname{ind}k}\omega^{k}\,,\tag{4.1}$$

where ξ, ω are primitive rth and qth roots of 1 in K respectively.

We require the following three lemmas.

LEMMA 12 [8, p. 278]. *We have*

$$(\xi,\,\omega^{m})=(\xi,\,\omega)\xi^{-\operatorname{ind}m}\quad(m,\,q)=1\tag{4.2}$$

and

$$(\xi,\,\omega)(\xi^{-1},\,\omega)=q\;.\tag{4.3}$$

Proof. We use the fact that $r\mid(q-1)/2$ which gives (4.2) at once since $\operatorname{ind}km\equiv\operatorname{ind}k+\operatorname{ind}m\pmod{q-1}$. Next write the left member of (4.3) as a double summation whose general term is $\xi^{\operatorname{ind}a-\operatorname{ind}b}\omega^{a+b}$ for $1\leqq a,\,b\leqq q-1$. Set $a\equiv bc\pmod q$ and then sum first on b, then c to complete the proof.

LEMMA 13. *Set* $\psi_i(\xi)=\sum_1^{q-2}\xi^{\operatorname{ind}j-(i+1)\operatorname{ind}(j+1)}$. *Then we have*

$$(\xi,\,\omega)^{r}=q\sum_{1}^{r-2}\psi_i(\xi)=:q\alpha=q\sum_{1}^{r-1}a_i\xi^{i}\,,\tag{4.4}$$

so that $\alpha=\alpha(\xi)$ *is independent of* p *and the* a_i *are uniquely determined. If* $\beta=\alpha(\xi^{-1})$ *we have*

$$\alpha\beta=q^{r-2}\;.\tag{4.5}$$

Proof. For the proof of (4.4) see [8, p. 279] or [6, Chap. 8]. We get (4.5) at once form (4.3).

REMARK. In [8], (4.1)-(4.4) are presented as formulas in C, however they clearly remain valid in K. (These functions ψ_i are often called the Jacobi Functions.)

Define $G_s(x)$ by setting

$$y^{s}G(y+y^{-1})=(y^{r}-1)/(y-1)$$

so that $G_s(x)=1+\sum_1^s F_n(x)\in Z[x]$ (or $K[x]$), where $F_n(x)$ is defined as in Lemma 2. On setting $G_{-1}(x)=-1,\,G_0(x)=1$, it follows easily that

$$G_n(x)=xG_{n-1}(x)-G_{n-2}(x)\qquad\text{for}\quad n\geqq 1\;.\tag{4.6}$$

We temporarily let p be an arbitrary odd prime and prove

LEMMA 14. (i) *p is a prime divisor of $G_s(x)$ if and only if* $p\equiv$

$0, \pm 1 (\bmod r)$ [7, p. 199]. (ii) *If* $p \equiv \pm 1 (\bmod r)$ *we have* $G_s(x) = \prod_1^s (x - \rho_i)$ *in* $GF(p)$ *where* $\rho_i = \xi^i + \xi^{-i}$, *and* ξ *is a fixed primitive* rth *root of* 1 *in* K, i.e. *in* $GF(p^2)$. [2]

Proof. If $p = r$ we have $p = G_s(2)$. Suppose now that $p \neq r$ and let ξ be a primitive rth root of 1 in $H =: GF(p^{r-1})$. Then we have $(y^r - 1)/(y - 1) = \prod_1^{r-1} (y - \xi^i) = \prod_1^s (y^2 - \rho_i y + 1) = y^{-s} \prod_1^s (x - \rho_i) = y^{-s} G_x(x)$ over H where $\rho_i = \xi^i + \xi^{-i}$. Next, if $\rho = \rho_i \in GF(p)$ then $y^2 - \rho y + 1$ splits over $GF(p^2)$ so that $r \mid p^2 - 1$. Conversely if this condition holds we have $\rho^{p-1} = 1$ in $GF(p^2)$ and $\rho \in GF(p)$.

We have $\rho_i = F_i(\rho)$ for $\rho = \rho_1$ and $1 \leqq i \leqq s$ by Lemma 2. Set $c_i = a_i = a_{r-i}$. Then by Lemmas 13 and 14 we get

$$(4.7) \quad \gamma =: \alpha + \beta = \sum c_i \rho_i = \sum c_i F_i(\rho) = \sum C(i, r, q) \beta_i \in GF(p)$$

where $B = \{\beta_i\}$ is any (integral) basis of $Z(\rho)$, i runs from 1 to s, and the $C(i, r, q) = C(i, r, q \mid B)$ (which we regard as lying in $GF(p)$) are independent of p. It seems most convenient simply to take $\beta_i = \rho_i$ for all i so that

$$(4.8) \qquad \gamma = \sum_1^s c_i \rho_i \, , \quad c_i = C(i, r, q) = a_i + a_{r-1} \, , \quad \rho_i = F_i(\rho) = \xi^i + \xi^{-i}$$

When $r = 3$ or 5, expressions for the $C(i, r, q)$ in (4.8) in terms of the representations of q by certain quadratic forms will be given in §5.

We use the preceding Lemmas to prove.

THEOREM 3. [15] *Let* p, q, r $(=2s + 1)$ *be odd primes such that* $-p \equiv q \equiv 1 (\bmod r)$ *and* $p^{(q-1)/r} \not\equiv 1 (\bmod q)$, *and put* $P = \sum_1^s C(i, r, q) F_i(R)$, $Q = q^{r-2}$, *where* $G_s(R) \equiv 0 \ (\bmod p)$. *Consider* $U_n = U_n(P, Q)$ *as an element of* $GF(p)$ *and set* $p + 1 = rk$. *Then we have*

$$U_{p+1}/U_k = 0, \text{ i.e. } U_{p+1} = 0 \, , \quad U_k \neq 0 \, .$$

(*Our two assertions are equivalent by Lemma* 6.)

Proof. For some ξ we have $R = \xi + \xi^{-1}$ by Lemma 14. Thus by (4.5) and (4.8) we have $P = \alpha + \beta$ and $Q = \alpha\beta$. We now work with (4.1)-(4.4) as follows and recall that $\beta = \alpha(\xi^{-1})$. Set $j = \operatorname{ind} p$. We have $(q\alpha)^k = (\xi, \omega)^{p+1} = (\xi, \omega)(\xi^{-1}, \omega^p) = q\xi^j$, so that $(q\beta)^k = q\xi^{-j}$. Hence $\alpha^{p+1} = \beta^{p+1}$ and $\alpha^k \neq \beta^k$ since $p^{(q-1)r} \not\equiv 1 (\bmod q)$. The Theorem follows at once by the definition of U_n, i.e. (2.1).

REMARK. Let R be a zero of $G_s(x) \equiv 0 \ (\bmod N)$ for any $N > 0$. Since the zeros of $G_s(x) = 0$ over $\boldsymbol{C}$ are $F_i(\rho)$ for $1 \leqq i \leqq s$ where ρ is a given zero, it follows that $G_s(x)$ has the s zeros $F_i(R)$ $(\bmod N)$.

Moreover if we replace $R = R_1$ by $R_i =: F_i(R)$ for any i, we permute the c_i in $P = P_1$ to give s formally different choices of $P =: P_i$ above and in Theorem 4 below. (See (4.8).) We will not be concerned, here or later, with determining when the R_i and P_i are all distinct $(\bmod N)$ and do not claim that the R_i are *all* the zeros in question, since N may be composite.

We note that the $F_i(R)$ are easily computable by means of the recurrence in Lemma 2 and that P can be written as $\sum_0^{s-1} d_j R^j$ for suitable d_j.

We are now ready to prove the following analogue of Theorem 2.

THEOREM 4. *Let* $N = Ab^{2n} + Bb^n - 1$ *where* A, b, n *are all* > 0, $2 \nmid N$, $b = ar$ *with* r *an odd prime, and set* $e, C, D = r^n, Aa^{2n}, Ba^n$ *respectively as in Lemma* 9. *Suppose that*

(i) $e \geqq (C-3)/2 + |D|$

or

(ii) $2 \mid a$, $e > (C + 2|D|)/8$, $n \geqq 2$.

Let q *be a prime such that* $q \equiv 1 \pmod r$ *and* $N^{(q-1)/r} \not\equiv 0, 1 \pmod q$. *Define* R, P, Q *as in Theorem* 3 *with* p *replaced by* N. *Set*

$$T_0 = F_a(P') \text{ or } F_{a/2}(P'),\ T_{h+1} \equiv F_b(T_h) \pmod N \ \textit{for}\ h \geqq 0$$

according as (i) or (ii) *holds, where* $QP' \equiv P^2 - 2Q \pmod N$. *Then* N *is prime if*

$$J =: J_r(F_{2A}(T_{2n-1}), F_{2B}(T_{n-1})) \equiv 0 \pmod N .$$

(*Recall that* $F_m(x)$ *has the same value for* $m = \pm j$ *by Lemma* 2.)

Proof. Assume that (i) holds. By Lemma 3 and (3.6) we get $J \equiv Q^{m(1-r)} W_r(P, Q)$ with $m = 2Aab^{2n-1}$, $\ell = 2Bab^{n-1}$. Hence if $N \mid J$, then N is prime by Lemmas 7 and 9.

If N is prime, then $N \mid (U_{N+1}/U_k)$ by Theorem 3 so that $N \mid (U_{2(N+1)}/U_{2k})$. Since $2(N+1) = m + \ell$ we have $N \mid J$.

The discussion in case (ii) goes in the same way so we omit the details.

REMARK. We can improve this Theorem in case (ii) when $r \equiv 1 \pmod 4$ by using Lemma 10.

5. Construction of LL-type tests by means of Theorems 2 and 4, and some numerical examples. We deal here with examples only of the many possible different tests of LL-type which can now be derived from the preceding theorems.

We set

$$t = T_{2n-1}\,, \qquad u = T_{n-1}\,. \tag{5.1}$$

and define J as in Theorems 2 and 4. It is convenient to list here the values of $F_n(x)$ to be used in this section, namely

$$F_2(x) = x^2 - 2,\ F_3(x) = x^3 - 3x,\ F_5(x) = x^5 - 5x^3 + 5x \tag{5.2}$$

$r = 2$. Let $N = 2^{2n+1} \pm 3\cdot 2^n - 1 (n \geqq 3)$, then $A = 2$, $B = \pm 3$. Putting $P = -Q = 2$, we get $\Delta = P^2 - 4Q = 12$, and $(Q|N) = (\Delta|N) = -1$. Also $T_0 = 4$ and $J = F_2(t) + F_3(u) = t^2 + u^3 - 3u - 2$.

Thus, if

$$N = 2^{2n+1} \pm 3\cdot 2^n - 1 \qquad (n \geqq 3)$$

and

$$\begin{aligned} &T_0 = 4 \\ &T_{k+1} \equiv T_k^2 - 2 \pmod N\,, \end{aligned}$$

then N is a prime if and only if

$$T_{2n-1}^2 + T_{n-1}^3 - 3T_{n-1} - 2 \equiv 0 \pmod N\,.$$

Before presenting further LL-type tests we give here a general formula for P' (mod N). Let $N \equiv h$ (mod q) where q is defined in Theorem 4 and $(h, q) = 1$. Suppose that $jh = -1$ (mod q).

Then we have

$$P' \equiv P^2((jN + 1)/q)^{r-2} - 2 \pmod N\,. \tag{5.3}$$

$r = 3$. In this case we have α in Theorem 3 equal to $\psi_1(\xi)$ and $P \equiv -C(1, 3, q)$ (mod N). It is well known (see, for example, [4]) that we have $C(1, 3, q) = -x$, where x is determined uniquely from the congruence $x \equiv 1$ (mod 3) and the quadratic partition

$$4q = x^2 + 27y^2\,. \tag{5.4}$$

Take $b = 3$ so that $a = 1$ and (i) of Theorem 4 holds. Set $q = Q = 7$ and take $n = 3m + 1$. Then $N \equiv 9A + (-1)^m 3B - 1$ (mod 7) so that $N^2 \not\equiv 0, 1$ if and only if $3A + (-1)^m B \not\equiv 0, 3, 5$. We now take $A = 1$, $B = \pm 1$ so that the last condition is satisfied. We can set $P = x = 1$. If $B = 1$, then for $n \equiv 1, 4$(mod 6) we have $N \equiv 4, 2$ and $j \equiv 5, 3$ (mod 7) respectively, and likewise if $B = -1$. Next we have $T_0 \equiv (jN + 1)/7 - 2$ (mod N), $T_{k+1} \equiv F_3(T_k)$ and $J = J_3(t^2 - 2, u^2 - 2)$ where $J_3(x, y) = x^2 + xy + y^2 - 3$ by Lemma 3. We thus obtain a set of 4 primality tests according as $n \equiv 1$ or 4(mod 6) and $B = \pm 1$.

For example, let $N = 3^{2n} - 1$, where $n > 1$ and $n \equiv 1$ (mod 6). If

$$T_0 \equiv (4N+1)/7 - 2 = (4\cdot 3^{2n} - 4\cdot 3^n - 17)/7 ,$$
$$T_{k+1} \equiv T_k(T_k^2 - 3) \pmod N ,$$

then N is a prime if and only if

$$T_{2n-1}^4 + T_{n-1}^4 + T_{n-1}^2 T_{2n-1}^2 - 6T_{2n-1}^2 - 6T_{n-1}^2 + 9 \equiv 0 \pmod N .$$

$r = 5$. In this case, we can easily verify by using standard results on Jacobi Functions (see, for example, [3]) that

$$\alpha = \psi_1(\xi)\psi_2(\xi)\psi_3(\xi)$$

in Theorem 3 can be written as

$$\alpha = \psi_1^2(\xi)\psi_1(\xi^2) . \tag{5.5}$$

By using results [4] connecting the values of the a_i in Lemma 13 with the values of x, y, z, w in the representation

$$\begin{cases} 16q = x^2 + 50u^2 + 50v^2 + 125w^2 \\ xw = v^2 - u^2 - 4uv \\ x \equiv 1 \pmod 5 . \end{cases} \tag{5.6}$$

it is a routine matter to deduce that

$$P \equiv c_1 R_i + c_2 R_{3-i} \pmod N , \quad (i = 1, 2) \tag{5.7}$$

where $G_2(R) \equiv 0$ for $R \equiv R_i$ and $R_{3-i} = F_2(R_i) \equiv -R_i - 1$, $c_i =: C(i, r, q)$

$$2c_1 = K + L , \quad 2c_2 = K - L , \tag{5.8}$$

and

$$\begin{aligned} 8K &= 8qx - x^3 + 625(v^2 - u^2)w \\ (16/25)L &= 10w(u^2 + v^2) - 25w^3 - x(xw + 8uv) . \end{aligned} \tag{5.9}$$

It should be noted here that there are precisely four solutions (x, u, v, w), $(x, v, -u, w)$, $(x, -v, u, -w)$, and $(x, -u, -v, w)$ of (5.6). These give us two possible solutions for (c_1, c_2); however, since $R_{3-i} = -R_i - 1$, we see that we have a valid value of P for either of these values of (c_1, c_2). We also note that since Theorem 4 only requires a value of $P^2 \pmod N$, we have four possible values for P:

$$LR_i - c_2,\ -LR_i - c_1,\ -LR_i + c_2,\ LR_i + c_1 .$$

Since the choice of formula here is arbitrary we will specify P as follows. Set $M = \min(|c_1|, |c_2|)$ so that $M = |c_1|$ or $|c_2|$ according as sign $KL < 0$ or $\geqq 0$. Then we may redefine P by setting

$$P = M + \varepsilon L R_i (i = 1, 2) \tag{5.10}$$

where $\varepsilon = \text{sign}(L - K)$ or $\text{sign}(L + K)$ according as $\text{sign}(KL) \geqq 0$ or < 0.

We give some values of M, L, and ε in Table 5.1 below

TABLE 5.1

q	x	u	v	w	K	$L/25$	M	ε
11	1	1	0	-1	89	1	32	$-$
31	11	2	1	-1	409	-5	142	$+$
41	-9	3	0	1	-981	-1	478	$+$
61	1	1	4	-1	1111	-11	418	$+$
71	-19	2	3	1	-101	41	462	$+$

When $r \geqq 5$ we have the additional problem of finding a solution of $G_s(R) \equiv 0 (\text{mod } N)$. For some values of N and r this can be done as in Williams [18], but this rather complicated technique does not allow us to calculate T_0 easily. When $r = 5$, however, we can compute a value of R for certain values of N with very little difficulty.

We note that if

$$N = (c^2 + cd - d^2)k^2 + (c - 2d)k - 1 \text{ , } \quad (c, dk + 1) = 1 \tag{5.11}$$

and

$$cR \equiv (c^2 + cd - d^2)k - d \pmod N \text{ ,} \tag{5.12}$$

then

$$c^2G_2(R) = c^2R^2 + c^2R - c^2 \equiv (c^2 + cd - d^2)N \equiv 0 \pmod N$$

Since $(c, N) = 1$, we have a solution R of $G_2(x) = 0$.

We now construct some primality tests with the aid of Theorem 4, (5.1), (5.2), (5.3), (5.10), (5.11), (5.12) and Lemma 3 in §2. In each case below we have a companion test obtained by replacing k by $-k$, and in (i) no change in the values of n involved is required.

(i) $c = 1, d = 0, k = 5^n$, so that $b = 5, a = 1, A = B = 1, R = k$, and condition (i) of Theorem 4 holds. Take $q = 11$, $n \equiv 1 \pmod 5$ so that $N \equiv 5^2 + 5 - 1 \equiv 7$ and $j \equiv 3 (\text{mod } 11)$. We have $P = 32 - 25k$, $T_0 = P' \equiv P^2((3n + 1)/11)^3 - 2 \pmod N$, $T_{k+1} \equiv F_5(T_k)$ and $J =: J_5(t^2 - 2, u^2 - 2)$, where $(x - y)J_5(x, y) = (x^5 - y^5) - 5(x^3 - y^3) + 5(x - y)$.

For $n = 1$ we have $N = 29$, and the reader may verify that $J \equiv 0 (\text{mod } 29)$ in accordance with Theorem 4, where $t = T_1$, $u = T_0$.

(ii) $c = 1, d = 0, k = -10^n$, so that $b = 10, a = 2, A = B = 1$, $R = k$.

Condition (ii) of Theorem 4 says that $5^n > (2^{2n} + 2^{n+1})/8$ which is true. Take $q = 41$, $n \equiv 3 \pmod 5$ so that $N \equiv 34$ and $j \equiv 6 \pmod{41}$. We have $P = 478 - 25k$, $T_0 \equiv P^2((6N + 1)/41)^3 - 2$, $T_{k+1} = F_{10}(T_k) = F_5^2(T_k) - 2$ (see Lemma 2), and J is the same as in (i). We obtain a companion test on taking $n \equiv 2 \pmod 5$.

Thus, when $N = 10^{2n} - 10^n - 1$, $n \equiv 3 (\mathrm{mod}\, 5)$, $(n > 0)$, put

$$T_0 = (418 + 25\cdot 10^n)^2\left(\frac{6\cdot 10^{2n} - 6\cdot 10^n - 5}{41}\right)^3 - 2$$

$$T_{k+1} \equiv [T_k(T_k^4 - 5T_k^2 + 5)]^2 - 2 \pmod N .$$

N is a prime if and only if

$$\begin{aligned} &T_{2n-1}^8 + T_{2n-1}^6 T_{n-1}^2 + T_{2n-1}^4 T_{n-1}^4 + T_{2n-1}^2 T_{n-1}^6 + T_{n-1}^8 \\ &\quad - 10(T_{2n-1}^6 + T_{2n-1}^4 T_{n-1}^2 + T_{2n-1}^2 T_{n-1}^4 + T_{n-1}^6) \\ &\quad + 35(T_{2n-1}^4 + T_{2n-1}^2 T_{n-1}^2 + T_{n-1}^4) - 50(T_{2n-1}^2 + T_{n-1}^2) + 25 \equiv 0 \\ &\quad \pmod N . \end{aligned}$$

If $N = 10^{2n} + 10^n - 1$, $n \equiv 2 \pmod 5$, we can use this same test except that

$$T_0 = (478 - 25\cdot 10^n)^2\left(\frac{20 - 19\cdot 10^n - 19\cdot 10^{2n}}{41}\right)^3 - 2 .$$

Primes of the form $10^{2n} \pm 10^n \pm 1$ have rather interesting digit patterns. For $10^{2n} - 10^n + 1$, we have the pattern

$$\underbrace{999\cdots 9}_{n \text{ nines}}\ \underbrace{000\cdots 0}_{n-1 \text{ zeros}}1;$$

for $10^{2n} - 10^n - 1$, we have the pattern

$$\underbrace{999\cdots 9}_{n-1 \text{ nines}}8\underbrace{999\cdots 9}_{n \text{ nines}};$$

and for $10^{2n} + 10^n - 1$, we have the pattern

$$1\ \underbrace{000\cdots 0}_{n \text{ zeros}}\ \underbrace{999\cdots 9}_{n \text{ nines}} .$$

Lehmer [9] tabulated the four primes of the form $10^{2n} - 10^n + 1$ for $n \leq 10$. Since these numbers have the form $N_n = (10^{3n} + 1)/(10^n + 1)$, we see that if N_n is a prime, then $n = 2^\alpha 3^\beta$. In fact, there are no more primes of this type for $n < 1000$. Indeed, one would expect such primes to be just about as scarce as Fermat primes. However, primes of the form $10^{2n} \pm 10^n - 1$, like the Mersenne primes, are somewhat more abundant. In Table 5.2 below, we give all those values of $n \leq m$ such that $N_n = k^2 \pm k \pm 1$ is a prime with $k = 10^n$.

TABLE 5.2

N_n	m	values of n such that N_n is prime
$k^2 - k + 1$	1023	2 4 6 8
$k^2 + k - 1$	500	1 2 3 5 6 7 9 13 26 42 153 188 282
$k^2 - k - 1$	750	1 6 9 154 253

6. Acknowledgement. The author gratefully acknowledges the many suggestions from the referee concerning the presentation of this work. He also wishes to thank him for supplying Propositions 1, 2, and 3, which were not in the original submission.

REFERENCES

1. R. D. Carmichael, *On the numerical factors of the arithmetic forms* $\alpha^n \pm \beta^n$, Ann. of Math., (2) **15** (1913-14), 30-70.
2. P. Chowla, *On a theorem of Kummer*, J. Number Theory, **2** (1970), 56-57.
3. L. E. Dickson, *Cyclotomy and trinomial congruences*, Trans. Amer. Math. Soc., **37** (1935), 363-380.
4. ———, *Cyclotomy, higher congruences, and Waring's problem*, Amer. J. Math., **57** (1935), 391-424.
5. K. Inkeri, *Tests for primality*, Ann. Acad. Sci. Fenn. Ser. AI, No. 279, (1960), 19 pp.
6. K. Ireland and M. Rosen, *Elements of Number Theory*, Bogden and Quiggley, Tarrytown, New York, 1972.
7. E. Kummer, *Papers*, vol. 1, edited by A. Weil, New York, Springer, 1975.
8. E. Landau, *Vorlesungen über Zahlentheorie*, vol. 3, Chelsea, New York, 1947. (Originally published in 1927).
9. D. H. Lehmer, *Tests for primality by the converse of Fermat's theorem*, Bull. Amer. Math. Soc., **33** (1927), 327-340.
10. ———, *An extended theory of Lucas' functions*, Ann. of Math., (2) **31** (1930), 419-448.
11. H. Riesel, *A note on the prime numbers of the form* $N = (6a+1)2^{2n} - 1$ *and* $M = (6a-1)2^{2n} - 1$, Ark. Mat., **3** (1956), 245-253.
12. ———, *Lucasian criteria for the primality of* $N = h\cdot 2^n - 1$, Math. Comp., **23** (1969), 869-875.
13. D. Shanks, *Solved and Unsolved Problems in Number Theory*, 2nd edition, Chelsea, New York, 1978.
14. S. B. Stechkin, *Lucas's criterion for the primality of numbers of the form* $N = h2^n - 1$, Math. Notes, **10** (1971), 578-584. (Translation of Mat. Zametki).
15. H. C. Williams, *An algorithm for determining certain large primes*, Congressus Numerantium III, Proc. of the second Louisiana Conf. on Combinatorics, Graph Theory and Computing, Utilitas Mathematica, Winnipeg, 1971, 533-566.
16. ———, *The primality of* $N = 2A3^n - 1$, Canad. Bull., **15** (1972), 585-589.
17. ———, *Primality testing on a computer*, Ars Combinatoria, **5** (1978), 127-185.
18. ———, *The primality of certain integers of the form* $2Ar^n - 1$, Acta Arith. To appear.

Received March 6, 1979 and in revised form March 6, 1981.

UNIVERSITY OF MANITOBA
WINNIPEG, CANADA R3T 2N2