References

[1] Z. I. Borevič and I. R. Šafarevič, *Number theory*, New York 1966.
[2] H. Hasse, *Über die Klassenzahl abelscher Zahlkörper*, Berlin 1952.
[3] K. Iwasawa, *A class number formula for cyclotomic fields*, Ann. of Math. 76 (1) (1962), pp. 171–179.
[4] M. Newman, *A table of the first factor for prime cyclotomic fields*, Math. Comp. 24 (109) (1970), pp. 215–219.

Received on 25. 11. 1977 (1004)

ACTA ARITHMETICA
XXXIX (1981)

The primality of certain integers of the form $2Ar^n-1$

by

H. C. Williams (Winnipeg)

1. Introduction. In [6] Lucas presented conditions which are sufficient for integers of the form Br^n-1 $(B<r^n)$ $r=2, 3, 5$, to be prime. Lehmer [4], Riesel [7] and Stechkin [8] have given criteria which are both necessary and sufficient for the primality of $A2^n-1$ $(A<2^n)$ and Williams [10], [12] has given necessary and sufficient conditions for the primality of $2A3^n-1$ $(A<3^n)$ and $A2^n3^m-1$ $(A<2^{n+1}3^m)$. All of these tests make use of Lucas functions or functions similar to the Lucas functions. In this paper we present, using the Lucas functions together with the generalized Lehmer functions of [11], a necessary and sufficient criterion for the primality of certain numbers of the form $N=2Ar^n-1$ $(A<r^n)$ when r and s are odd primes, $r=2s+1$, and $2A-1$ is a primitive root of s.

We define the Lucas functions

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

where α, β are the roots of the auxiliary quadratic

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

and P, Q are coprime integers. (While it is usual to insist that $(P,Q)=1$, it is sufficient in dealing with the functions modulo N to have $(N,Q)=1$.) The usual test for the primality of $N=Br^n-1$ $(B<r^n)$ (see, for example, Brillhart, Lehmer, Selfridge [1]) involves attempting to find P, Q such that $(Q,N)=1$ and

$$N \mid U_{N+1}(P,Q), \tag{1.1}$$

$$\left(N, U_{(N+1)/r}(P,Q)\right)=1. \tag{1.2}$$

If such a pair P, Q can be found, N is a prime. The determination of this pair is done by trial, subject to the constraint that the Jacobi symbol $(P^2-4Q|N)=-1$. Under this constraint, if (1.1) is not satisfied, N is composite.

Now if N is a prime and $(P^2-4Q|N) = -1$, (1.1) must be true but it is not necessary that (1.2) be true as well. We give here for certain of the values of N mentioned above an explicit formula for P and for Q such that if N is a prime both (1.1) and (1.2) must be true. This gives a necessary and sufficient criterion for the primality of N, which is similar to those given by Lehmer in [4] for the primality of $A2^n-1$.

2. Preliminary results. Define the Chebyshev polynomial $G_m(x)$ by putting $G_0(x) = 1$, $G_1(x) = x+1$ and

$$G_{k+1}(x) = x\,G_k(x)-G_{k-1}(x) \qquad (k = 1, 2, 3, \ldots).$$

We have

$$\frac{x^s-1}{x-1} = x^s G_s(x+x^{-1}) \tag{2.1}$$

rom which it follows on putting $x = (\alpha/\beta)^k$ that

$$U_{kr}(P, Q) = Q^{ks} G_s\big(V_{2k}(P, Q)/Q^k\big)\,U_k(P, Q).$$

As it is well known ([2], p. 51) that

$$\big(U_{kr}(P, Q)/U_k(P, Q),\ U_k(P, Q)\big) = 1, r,$$

we see that conditions (1.1) and (1.2) can be replaced by the single condition

$$Q^{ms} G_s\big(V_{2m}(P, Q)/Q^m\big) \equiv 0 \pmod N,$$

where $m = (N+1)/r$. Now if we define P' by

$$QP' \equiv P^2-2Q \pmod N,$$

we have

$$V_{2m}(P, Q)/Q^m \equiv V_m(P', 1) \pmod N.$$

Thus we can replace (1.1) and (1.2) by the single condition

$$G_s\big(V_m(P', 1)\big) \equiv 0 \pmod N. \tag{2.2}$$

Let q be any prime such that $q \equiv 1 \pmod r$. In [9] it is shown how certain coefficients, denoted by $C(i, r, q)$ $(i = 0, 1, 2, \ldots, s-1)$, can be calculated. The values of these coefficients depend only on those of r and q and are independent of N. Also, several tables(1) of these numbers are given in [9]. With this information we can now give the main result of [9] as

(1) On page 553 of [9] the entry for $C(1, 5, 101)$ should read -1025 not 1025. This means that P (1, 101, 5) and P (2, 101, 5) in table 1 of [11], p. 336, should now be changed to 271 and -1294921 respectively.

THEOREM 1. *Let $N = 2Ar^n-1$, where $r = 2s+1$ is a prime, $(A, r) = 1$, $A < r^n$. Let R be an integer such that*

$$G_s(R) \equiv 0 \pmod N$$

and let q $(\equiv 1 \pmod r)$ be a prime such that

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

If

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

then N is a prime if and only if

$$N \mid G_s\big(V_{(N+1)/r}(P', 1)\big).$$

The main difficulty in using this result is that we do not have an explicit formula for R. As it is sufficient to determine a value for R under the assumption that N is a prime, this is what we will do in the next two sections.

3. Some results from cyclotomy. Let r, s be odd primes such that $r = 2s+1$ and let p be a prime such that $p \equiv -1 \pmod r$. We assume that p belongs to exponent ν $(= 2\mu)$ modulo s and that

$$\big(s, (p^\mu+1)/s\big) = 1.$$

Let $K = \mathrm{GF}[p^r]$ and let θ be a primitive element of K. Put

$$\xi = \alpha^{k(p^r-1)/s}, \qquad \omega = \theta^{l(p^r-1)/r},$$

where $(s, k) = (l, r) = 1$. We have $\xi \neq 1$, $\omega \neq 1$, and $\xi^s = \omega^r = 1$. We also let g be any primitive root of r, γ be any primitive root of s, and put the Lagrange resolvent

$$(\xi^i, \omega) = \sum_{j=0}^{r-2} \xi^{ij} \omega^{g^j}.$$

Finally, define for each λ such that $0 \leqslant \lambda \leqslant s-1$

$$T_\lambda = \sum_{i=0}^{s-1} \xi^{\lambda i} (\xi^i, \omega).$$

LEMMA 1. *In K, $G_s(T_\lambda/s) = 0$ for $\lambda = 0, 1, 2, \ldots, s-1$.*

Proof. For any λ

$$T_\lambda = \sum_{i=0}^{s-1} \xi^{\lambda i} \sum_{j=0}^{r-2} \xi^{ij} \omega^{g^j} = \sum_{j=0}^{r-2} \omega^{g^j} \sum_{i=0}^{s-1} \xi^{i(j+\lambda)}.$$

Now

$$\sum_{i=0}^{s-1} \xi^{(\lambda+j)i} = \begin{cases} s & \text{when} \quad s|\lambda+j, \\ 0 & \text{when} \quad s\nmid\lambda+j. \end{cases}$$

Thus, the above sum zero is not zero only for $j = s-\lambda$, $j = 2s-\lambda$ and

$$T_\lambda = s.(\omega^{g^{s-\lambda}} + \omega^{g^{2s-\lambda}}).$$

If $g^{-\lambda} \equiv a \pmod r$, we get

$$T_\lambda/s = \omega^a + \omega^{-a}.$$

Since $(a, r) = 1$, we see from (2.1) that

$$G_s(T_\lambda/s) = 0.$$

LEMMA 2. *If τ is the index to base γ of p modulo s, then*

$$T_\lambda = -1 + \sum_{i=0}^{\tau-1} \sum_{j=0}^{\nu-1} \xi^{\lambda\gamma^j\tau+i}(\xi^{\gamma^j\tau+i}, \omega).$$

Proof. This result follows easily from the facts that $(1, \omega) = -1$ and $s-1 = \nu\tau$.

In Section 4 we will also require some other results from the theory of cyclotomy. By using the methods in Landau [3] (p. 279 and p. 301) we see that in the finite field K we must have

$$(\xi, \omega)(\xi^{-1}, \omega) = r, \tag{3.1}$$

and

$$(\xi, \omega)^{p^\varkappa} = \xi^{-k\,\mathrm{ind}_g p}(\xi^{p^\varkappa}, \omega). \tag{3.2}$$

4. The main result. In this section we give an explicit formulation for T_λ when $\nu = s-1$, i.e. when p is a primitive root of s. We first require

LEMMA 3. *Let $t = (s-1)/2$ and let c, m be integers such that*

$$c(p^\mu+1)/s+1 = sm.$$

If in K we put

$$\varphi = r^{-(t+c)}(r^{st}(\xi, \omega)^s)^m,$$

then

$$\varphi = \xi^\lambda(\xi, \omega)$$

for some integer λ.

Proof. We first note that since $p \equiv -1 \pmod r$, have $s|\mathrm{ind}_g p$. Thus, in K we get (using (3.2))

$$(\xi, \omega)^{p^\mu} = \xi^{-\mu\,\mathrm{ind}_g p}(\xi^{p^\mu}, \omega) = (\xi^{-1}, \omega)$$

and it follows from (3.1) that

$$(\xi, \omega)^{p^\mu+1} = r.$$

We also have

$$q^{p^\mu+1} \equiv q^2 \pmod p;$$

hence,

$$\varphi^s = q^{-(st+cs)+ct(p^\mu+1)+st}(\xi, \omega)^{c(p^\mu+1)+s} = q^{2tc+c-sc}(\xi, \omega)^s = (\xi, \omega)^s.$$

It follows that, for some λ, $\varphi = \xi^\lambda(\xi, \omega)$.

Now if $\nu = s-1$, then $\tau = 1$ and

$$\begin{aligned} T_\lambda &= -1 + \sum_{j=0}^{\nu-1} \xi^{\lambda p^j}(\xi^{p^j}, \omega) = -1 + \sum_{j=0}^{\nu-1} [\xi^\lambda(\xi, \omega)]^{p^j} \\ &= -1 + r^{-(t+c)} \sum_{j=0}^{\nu-1} [r^{st}(\xi, \omega)^s]^{mp^j} = -1 + r^{-(t+c)} \sum_{j=0}^{\nu-1} [r^{st}(\xi^{p^j}, \omega)^s]^m \\ &= -1 + r^{-(t+c)} \sum_{i=1}^{\nu} [r^{st}(\xi^i, \omega)^s]^m. \end{aligned}$$

If we put

$$\varrho_i = r^{st}[(\xi^i, \omega)^s + (\xi^{-1}, \omega)^s] \qquad (i = 1, 2, \ldots, t),$$

the monic polynomial whose roots are $\varrho_1, \varrho_2, \varrho_3, \ldots, \varrho_t$ in K has coefficients in GF[p]. In fact, if we denote this polynomial by

$$f(x) = \sum_{i=0}^{t} (-1)^{t-i} P_{t-i} x^i, \tag{4.1}$$

then

$$P_i = r^{i(st+1)} P(i, r, s),$$

where the integer coefficients $P(i, r, s)$ depend for their values only on the values of i, r, and s (see Williams [11], p. 336). We also have

$$T_\lambda = -1 + r^{-(t+c)} \sum_{i=1}^{t} (\alpha_i^m + \beta_i^m),$$

where $\alpha_i\beta_i = r^{s^2}$ and $\alpha_i + \beta_i = \varrho_i$. By employing the generalized Lehmer functions of [11], pp. 316–317 and p. 320, we can rewrite this as

$$\begin{aligned} T_\lambda &= -1 + r^{-(t+c)} \sum_{i=1}^{t} \sum_{j=0}^{t-1} V_{j,m}(P_1, P_2, \ldots, P_t, r^{s^2}) \varrho_i^j \\ &= -1 + r^{-(t+c)} \sum_{j=0}^{t-1} V_{j,m}(P_1, P_2, \ldots, P_t, r^{s^2}) S_j, \end{aligned}$$

where

$$S_j = \sum_{i=1}^{t} \varrho_i^j$$

and

$$V_{j,m}(P_1, P_2, \ldots, P_t, r^{s^2}) \quad (j = 0, 1, 2, \ldots, t-1)$$

are the generalized Lehmer functions defined for $f(x)$ given by (4.1) and $Q = r^{s^2}$.

We are now able to state our main theorem.

THEOREM 2. *Let* $N = 2Ar^n - 1$, *where* $A < r^n$, $r = 2s+1$, r, s *are primes*, $s = 2+1$, $2A-1$ *is a primitive root of* s *and*

$$-2nA \not\equiv E \pmod{s}, \quad \text{where} \quad E \equiv (2A-1)\left((2A-1)^t+1\right)/s \pmod{s}.$$

If c *is an integer such that*

$$c(E+2nA) \equiv 1-2A \pmod{s},$$

and if q *is a prime such that* $q \equiv 1 \pmod{r}$ *and*

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

then N *is a prime if and only if*

$$N \mid G_s\left(V_{(N+1)/r}(P', 1)\right), \tag{4.2}$$

where

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

$$sr^{t+c}R \equiv -r^{t+c} + \sum_{j=0}^{t-1} V_{j,m}(P_1, P_2, \ldots, P_t, r^{s^2})S_j \pmod{N},$$

and

$$m = \left(1+c(N^t+1)/s\right)/s.$$

Proof. We first note that since $2A-1$ is a primitive root of s, so is N; hence, N belongs to exponent $2t$ modulo s.

Since $r = 2s+1$ and $s = 2t+1$, we have

$$N = 2Ar^n - 1 = 2A - 1 + 4Ans \pmod{s^2}$$

and

$$N^t \equiv (2A-1)^t + 4(2A-1)^{t-1}Anst \pmod{s^2};$$

thus,

$$(2A-1)(N^t+1)/s \equiv E + 2nA \pmod{s}.$$

Since $(s, E+2nA) = 1$, we can find an integer c such that

$$c(E+2nA) \equiv 1-2A \pmod{s};$$

also, we see that

$$m = \left(1+c(N^t+1)/s\right)/s$$

is an integer.

If (4.2) holds, we know that N must be a prime; on the other hand, if N is a prime, we see by Lemma 1 and the result above that R must be an integer such that

$$G_s(R) \equiv 0 \pmod{N}.$$

The theorem now follows from Theorem 1.

5. Some examples. If we consider integers of the form $6C7^n - 1$ $(3 \nmid C,\ 3C < 7^n)$, we have $r = 7$, $s = 3$; also, we see that $6C-1$ is a primitive root of 3, and

$$-2n(3C) \not\equiv \left((6C-1)+1\right)/3 \pmod{3}.$$

Since $t = 1$ in this case, we have $c \equiv C \pmod{3}$, i.e. $c = 1$ when $C \equiv 1 \pmod{3}$ and $c = 2$ when $C \equiv 2 \pmod{3}$. Also, $P(1, 7, 3) = 1$ and the function $V_{0,m}(P_1, 7^9)$ is the usual Lucas function $V_m(7^4, 7^9)$; therefore,

$$3 \cdot 7^{1+c}R \equiv -7^{1+c} + V_m(7^4, 7^9) \pmod{N},$$

where $m = \left(c(N+1)/3+1\right)/3$. If q is a prime such that $q \equiv 1 \pmod{7}$, $N^{(q-1)/7} \not\equiv 0, 1 \pmod{q}$, and

$$q^5P' \equiv P^2 - 2q^5 \pmod{N},$$

where

$$P \equiv C(0, 7, q) + C(1, 7, q)R + C(2, 7, q)R^2 \pmod{N},$$

then N is a prime if and only if

$$N \mid X^3 + X^2 - 2X - 1, \quad \text{where} \quad X \equiv V_{(N+1)/7}(P', 1) \pmod{N}.$$

Thus, we have a test for the primality of $N = 6C7^n - 1$ $(3 \nmid C,\ 3C < 7^n)$, which involves Lucas functions only.

For the special case $N = 6 \cdot 7^n - 1$, we have $N^4 \not\equiv 0, 1 \pmod{29}$ when $n \not\equiv 1 \pmod{7}$; consequently, if $n \not\equiv 1 \pmod{7}$ N is a prime if and only if

$$N \mid X^3 + X^2 - 2X - 1,$$

where

$$X \equiv V_{(N+1)/7}(P', 1) \pmod{N}, \quad 29^5P' \equiv P^2 - 2 \cdot 29^5 \pmod{N},$$

$$P \equiv 5199 - 2597R - 5831R^2 \pmod{N}$$

and

$$3\cdot 7^2 R \equiv -7^2 + V_{(N+4)/9}(7^4, 7^9) \pmod N.$$

If $N = 4\cdot 11^n - 1$ (n odd, $n \not\equiv 1 \pmod 5$), we have $r = 11$, $s = 5$, $t = 2$. Also, $2A - 1 = 3$ is a primitive root of 5, and $(E + 2nA, 5) = 1$, since $A = 2$, $E = 1$, $n \not\equiv 1 \pmod 5$. We have

$$P(1, 11, 5) = -89, \quad P(2, 11, 5) = 1199,$$

$$c = \begin{cases} 3 & \text{for} \quad n \equiv 2 \pmod 5, \\ 4 & \text{for} \quad n \equiv 3 \pmod 5, \\ 1 & \text{for} \quad n \equiv 4 \pmod 5, \\ 2 & \text{for} \quad n \equiv 0 \pmod 5, \end{cases}$$

$$m = \big(c(N^2+1)/5 + 1\big)/5,$$

$$5\cdot 11^{c+2} R \equiv -11^{c+2} + 2V_{0,m}(-89\cdot 11^{11},\ 1199\cdot 11^{22},\ 11^{25}) - \\ -89\cdot 11^{11} V_{1,m}(-89\cdot 11^{11},\ 1199\cdot 11^{22},\ 11^{25}) \pmod N.$$

Since n is odd, we have $(4\cdot 11^n - 1)^2 \not\equiv 1 \pmod{23}$; thus, N is a prime if and only if

$$N \mid X^5 + X^4 - 4X^3 - 3X^2 + 3X + 1,$$

where

$$X \equiv V_{(N+1)/11}(P', 1) \pmod N, \qquad 23^9 P' \equiv P^2 - 2\cdot 23^9 \pmod N,$$

$$P \equiv 2892063 + 1176725R - 1281027R^2 - 635734R^3 - 79860R^4 \pmod N.$$

6. A special case. Since necessary and sufficient tests for primality of integers of the form $(r-1)r^n - 1$ have been developed for $r = 2, 3, 5$ [9], and 7, it is of some interest to obtain a criterion for the primality of $10\cdot 11^n - 1$. Unfortunately, we do not have 9 as a primitive root of 5; however, we can modify our above technique somewhat to obtain a test for the primality of $N = 10C11^n - 1$ when $(C, 5) = 1$ and $5C < 11^n$.

We make use of the result that

$$(\xi, \omega)^2 = \psi(\xi)(\xi^2, \omega), \tag{6.1}$$

where

$$\psi(\xi) = \sum_{i=1}^{r-2} \xi^{\operatorname{ind}_g i - 2\operatorname{ind}_g (i+1)} \qquad \text{(see [3], pp. 278–280)}.$$

Also, $\psi(\xi)\psi(\xi^{-1}) = r$.

When $s = 5$ and $r = 11$, we have

$$\psi(\xi) = 2\xi - 2\xi^2 - \xi^3.$$

If we let p be a prime such that $p \equiv -1 \pmod{55}$ and return to the result of Lemma 1, we see that

$$T_\lambda = -1 + \xi^\lambda(\xi, \omega) + \xi^{2\lambda}(\xi, \omega)^2/\psi(\xi) + \xi^{-2\lambda}(\xi^{-1}, \omega)^2/\psi(\xi^{-1}) + \xi^{-\lambda}(\xi^{-1}, \omega).$$

We also have $\mu = 1$, $c \equiv 2C^{-1} \pmod 5$. If we put

$$\alpha = 11^{10}(\xi, \omega)^5, \qquad \beta = 11^{10}(\xi^{-1}, \omega)^5,$$

then

$$T_\lambda = -1 + 11^{-(2+c)}(\alpha^m + \beta^m) + 11^{-(4+2c)}\left(\frac{\alpha^{2m}}{\psi(\xi)} + \frac{\beta^{2m}}{\psi(\xi^{-1})}\right), \tag{6.2}$$

where $m = \left(c\,\dfrac{p+1}{5} + 1\right)/5$.

Using the simple identities

$$2\alpha^{2m} = (\alpha^m + \beta^m)^2 + (\alpha^m + \beta^m)(\alpha^m - \beta^m) - 2(\alpha\beta)^m,$$

$$2\beta^{2m} = (\alpha^m + \beta^m)^2 - (\alpha^m + \beta^m)(\alpha^m - \beta^m) - 2(\alpha\beta)^m,$$

we can rewrite (5.2) as

$$\begin{aligned} T_\lambda &= -1 + 11^{-(2+c)}(\alpha^m + \beta^m) + 11^{-(4+2c)}\big[(\alpha^m + \beta^m)^2\big(\psi(\xi) + \psi(\xi^{-1})\big)/22 - \\ &\quad - 11^{25m}\big(\psi(\xi) + \psi(\xi^{-1})\big)/11 + (\alpha^m + \beta^m)(\alpha^m - \beta^m)\big(\psi(\xi^{-1}) - \psi(\xi)\big)/22\big] \\ &= -1 - [\psi(\xi) + \psi(\xi^{-1})] + 11^{-(2+c)}(\alpha^m + \beta^m) + \\ &\quad + 11^{-(4+2c)}\left[\frac{\psi(\xi) + \psi(\xi^{-1})}{22}(\alpha^m + \beta^m)^2 + \right. \\ &\quad \left. + \frac{\psi(\xi^{-1}) - \psi(\xi)}{22}(\alpha - \beta)(\alpha^m + \beta^m)\,\frac{\alpha^m - \beta^m}{\alpha - \beta}\right]. \end{aligned}$$

Now $\alpha + \beta = 11^{11}[(\xi, \omega)^5/11 + (\xi^{-1}, \omega)^5/11]$; also, from (3.1) and (5.1) we get

$$(\xi, \omega)^5/11 = \psi(\xi)^2\psi(\xi^2) = 6\xi + 41\xi^2 + 16\xi^3 + 26\xi^4;$$

thus,

$$\alpha + \beta = 11^{11}(-57 - 25\delta), \qquad \text{where} \qquad \delta = \xi + \xi^{-1}.$$

We also calculate

$$\psi(\xi) + \psi(\xi^{-1}) = 3 + 5\delta, \qquad \alpha - \beta = 5\cdot 11^{11}(\xi - \xi^{-1})(-4 + 5\delta),$$

$$(\alpha - \beta)\big(\psi(\xi^{-1}) - \psi(\xi)\big) = 25\cdot 11^{11}(-4 + 5\delta).$$

Since $\delta \in \mathrm{GF}[p]$, we can use the Lucas functions

$$V_m(K, L) = \alpha^m + \beta^m, \qquad U_m(K, L) = (\alpha^m - \beta^m)/(\alpha - \beta),$$

where

$$K = 11^{11}(-57-25D), \quad L = 11^{25}, \quad D^2+D-1 \equiv 0 \pmod p,$$

and find that

$$10\cdot 11^{5+2c}R \equiv (-8-10D)11^{5+2c}+2\cdot 11^{3+c}V_m(K,L)+$$
$$+(3+5D)\,V_m^2(K,L)+25\cdot 11^{11}(-4+5D)\,V_m(K,L)\,U_m(K,L) \pmod p.$$

When C is odd, $N = 10C11^n-1 \equiv 1 \pmod 4$; thus, the Jacobi symbol $(11\,|\,N) = -1$. If N is a prime, we have

$$\left(\tfrac{1}{2}V_{(n+1)/2}(8,5)\right)^2 \equiv 5 \pmod N \quad \text{(Lehmer [5])}.$$

Also, if $n \not\equiv 17 \pmod{22}$, $N^2 \not\equiv 1 \pmod{23}$; hence, if $N = 10\cdot 11^n-1$, $n \not\equiv 17 \pmod{22}$, then N is a prime if and only if

$$N\,|\,X^5+X^4-4X^3-3X^2+3X+1,$$

where

$$X \equiv V_{(N+1)/11}(P',1) \pmod N, \quad 23^9P' \equiv P^2-2\cdot 23^9 \pmod N,$$

$$P \equiv 2892063+1176725R-1281027R^2-635734R^3-79860R^4 \pmod N,$$

$$5\cdot 11^9R \equiv (-8-10D)11^9+2\cdot 11^5V_m(K,L)+(3+5D)\,V_m^2(K,L)+$$
$$+25\cdot 11^{11}(-4+5D)\,V_m(K,L)\,U_m(K,L) \pmod N,$$

$$m = (2N+7)/25,$$

$$K \equiv 11^{11}(-57-25D), \quad L \equiv 11^{25} \pmod N,$$

$$4D \equiv -2+V_{(N+1)/2}(8,5) \pmod N.$$

This again is a criterion for primality that involves only Lucas functions.

Anyone involved in the actual testing of integers for primality knows that if an integer of the form $N = Br^n-1$ ($r^n > B$) is a prime, finding a pair P, Q such that N satisfies (1.1) and (1.2) never takes very long. Usually the first pair selected suffices. Also, if N is composite, it is almost always the case that for the first pair P, Q selected, (1.1) will be false. In view of this it does not seem to be unreasonable to expect to find much simpler values of P, Q than those given above such that a necessary and sufficient condition that N be prime is that (2.2) should be satisfied. However, the process by which such simpler values of P, Q could be obtained appears to be very difficult to discover.

In conclusion, we present in Table 1 a list of all the primes of the form $(r-1)r^n-1$ for $r = 3, 5, 7, 11$, $1 \leqslant n \leqslant 500$.

Table 1

r	all values of $n \leqslant 500$ such that $(r-1)r^n-1$ is prime
3	1, 2, 3, 7, 8, 12, 20, 23, 27, 35, 56, 62, 68, 131, 222, 384, 387
5	1, 3, 9, 13, 15, 25, 39, 69, 165, 171, 209, 339
7	1, 2, 7, 18, 55, 69, 87, 119, 141, 189, 249, 354
11	1, 3, 37, 119, 255, 355, 371, 497

References

[1] J. Brillhart, D. H. Lehmer, J. L. Selfridge, *New primality criteria and factorizations of* $2^m \pm 1$, Math. Comp. 29 (1975), pp. 620–647.

[2] R. D. Carmichael, *On the numerical factors of the arithmetic forms* $\alpha^n \pm \beta^n$, Ann. of Math. (2), 15 (1913–14), pp. 30–70.

[3] E. Landau, *Vorlesungen über Zahlentheorie*, Vol. III, Chelsea, New York 1947.

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

[5] — *Computer technology applied to the theory of numbers*, MAA Studies in Mathematics 6 (1969), pp. 117–151.

[6] Ed. Lucas, *Theorie des fonctions numeriques simplement periodiques*, Amer. Journ. Math. 1 (1878), pp. 184–240, 289–321.

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

[8] S. B. Stechkin, *Lucas' criterion for the primality of numbers of the form* $N = h\cdot 2^n-1$, Math. Notes 10 (1971), pp. 578–584.

[9] H. C. Williams, *An algorithm for determining certain large primes*, Proc. Second Louisiana Conference on Combinatorics, Graph Theory and Computing, Baton Rouge, 1971, pp. 533–556.

[10] — *The primality of* $2A3^n-1$, Canad. Math. Bull. 15 (1972), pp. 585–589.

[11] — *A generalization of Lehmer's functions*, Acta Arith. 29 (1976), pp. 315–341.

[12] — *Some properties of a special set of recurring sequences*, Pacific Journ. Math., to appear.

DEPARTMENT OF COMPUTER SCIENCE
UNIVERSITY OF MANITOBA
Winnipeg, Manitoba R3T 2N2, Canada

Received on 14. 12. 1977
and in revised form on 26. 6. 1978 (1010)