Canad. Math. Bull. Vol. **15** (4), 1972.

THE PRIMALITY OF $N=2A3^n-1$

BY
H. C. WILLIAMS

1. **Introduction.** Lehmer [3] and Reisel [7] have devised tests for determining the primality of integers of the form $A2^n-1$. Tables of primes of these forms may be found in [7] and Williams and Zarnke [10]. Little work, however, seems to have been done on integers of the form $N=2A3^n-1$. Lucas [6] gave conditions that were only sufficient for the primality of N. Recently Lehmer [4] has given a method for determining the primality of an integer N if the factorization of $N+1$ is known. If $N+1=q^n m$ (q a prime, $q^n>m$), this test can be simplified somewhat, but the test is still only a sufficient criterion for N to be prime. It is, therefore, quite probable that an application of this test will not resolve the question of the primality of N. In this paper we give a criterion which is both necessary and sufficient for the primality of $N=2A3^n-1$, when $3^n>2A$. This test, like Lehmer's, can be easily implemented on a high speed computing device and also requires just about the same number of operations as Lehmer's test.

2. **Preliminary results.** We need some previously known results which we shall simply state here.

THEOREM 1. (Kummer [9], Lehmer [5]). *Let p be any prime, let q be a prime congruent to* 1 *modulo* 3, *and let* $4q=r^2+27s^2$, *where r is congruent to* 1 *modulo* 3. *If p does not divide qs, the congruence*

$$x^3-3qx-qr \equiv 0 \pmod p$$

has an integer root if and only if

$$p^{(q-1)/3} \equiv 1 \pmod q$$

THEOREM 2. (Cailler [1]). *Let p be any prime congruent to* -1 *modulo* 3, $\Delta=27h^2+4g^3$, *and* $(3\Delta|p)=-1$. *If p does not divide g,*

$$x^3+gx+h \equiv 0 \pmod p$$

has an integer root if and only if

$$U_{(p+1)/3} \equiv 0 \pmod p,$$

Received by the editors November 24, 1970 and, in revised form, January 22, 1971.

where

$$U_m = \frac{\alpha^m - \beta^m}{\alpha - \beta},$$

α and β are the roots of

$$z^2 + tz + u = 0,$$

and t, u are coprime integers such that

$$gt \equiv 3h, \qquad 3u \equiv -g \pmod{p}.$$

THEOREM 3. (Lehmer [3]). *If $U_{m\pm 1} \equiv 0 \pmod{m}$ and $(U_{(m\pm 1)/a}, m) = 1$, where a is a prime, then the prime factors of m are of the forms $ka^v \pm 1$, where v is the highest power to which a occurs as a factor of $m \pm 1$.*

We shall also require two lemmas. The first of these is based upon an idea of Robinson [8].

LEMMA 1. *If all the prime factors of $N = 2A3^n - 1$, where A is not divisible by 3, and $1 \le A < 4.3^n - 1$, are of the forms $k3^n \pm 1$, N is a prime.*

Proof. The smallest possible factor of N is $2.3^n - 1$. If this is a divisor of N,

$$2A3^n \equiv 1 \pmod{2.3^n - 1}$$

or

$$A - 1 \equiv A - 2A3^n \equiv 0 \pmod{2.3^n - 1};$$

hence,

$$A - 1 = m(2.3^n - 1).$$

Since 3 does not divide A, m cannot equal 1; therefore, $A \ge 2(2.3^n - 1) + 1 = 4.3^n - 1$, which is impossible. It may be shown in a similar manner that $2.3^n + 1$ is not a prime divisor of N.

Since $N < (4.3^n - 1)^3$, if N is composite it must be a product of two prime factors $t_1 3^n - 1$ and $t_2 3^n + 1$, where t_1, $t_2 \ge 4$, i.e.

$$\begin{aligned} 2A = t_1 t_2 3^n + t_1 - t_2 &> t_2[t_1 3^n - 1] \\ &> 8.3^n - 2; \end{aligned}$$

thus, N is prime.

LEMMA 2. *Let $N = 2A3^n - 1$, $4q = r^2 + 27s^2$, $(q, N) = 1$, and $qK \equiv 1 \pmod{N}$. If*

$$P_1 \equiv K^A V_{2A} \pmod{N},$$

and

$$P_{k+1} \equiv P_k(P_k^2 - 3) \pmod{N},$$

then

$$P_n \equiv K^{(N+1)/6} V_{(N+1)/3} \pmod{N},$$

where

$$V_m = \alpha^m + \beta^m$$

and α, β are the roots of

$$z^2 + rz + q = 0.$$

https://doi.org/10.4153/CMB-1972-101-7 Published online by Cambridge University Press

Proof. Put

$$P_k \equiv K^{A3^{k-1}} V_{2A3^{k-1}} \pmod N.$$

Since

$$V_{3m} = V_m[V_m^2 - 3q^m],$$

we have

$$P_{k+1} \equiv P_k(P_k^2 - 3) \pmod N;$$

hence,

$$P_n \equiv K^{(N+1)/6} V_{(N+1)/3} \pmod N.$$

3. **The main result.**

THEOREM 4. *Let $N=2A3^n-1$, where 3 does not divide A and $1 \le A < 4.3^n-1$; let q be any prime such that q is congruent to 1 modulo 3 and*

$$N^{(q-1)/3} \not\equiv 1 \pmod q;$$

finally, let $4q=r^2+27s^2$, where $r\equiv 1 \pmod 3$. If $(qs, N)=1$, N is a prime if and only if

$$P_n \equiv \pm 1 \pmod N,$$

where P_n is defined in Lemma 2.

Proof. If N is a prime,

$$x^3 - 3qx - qr \equiv 0 \pmod N$$

is not resolvable by Theorem 1; hence, by Theorem 2

$$U_{(N+1)/3} \not\equiv 0 \pmod N,$$

where $U_m = (\alpha^m - \beta^m)/(\alpha-\beta)$ and α, β are defined in Lemma 2. Since (Lehmer [3])

$$U_{N+1} \equiv 0 \pmod N,$$

we have

$$U_{(N+1)/3}[V^2_{(N+1)/3} - q^{(N+1)/3}] \equiv 0 \pmod N$$

or

$$V_{(N+1)/3} \equiv \pm q^{(N+1)/6} \pmod N;$$

hence,

$$P_n \equiv \pm K^{(N+1)/6} q^{(N+1)/6} \equiv \pm 1 \pmod N.$$

If

$$P_n \equiv \pm 1 \pmod N,$$

then

$$V_{(N+1)/3} \equiv \pm q^{(N+1)/6} \pmod N.$$

Since

$$V^2_{(N+1)/3} + 27s^2 U^2_{(N+1)/3} = 4q^{(N+1)/3},$$

we have

$$27s^2 U^2_{(N+1)/3} \equiv 3q^{(N+1)/3} \pmod N;$$

Consequently, $(U_{(N+1)/3}, N)=1$. Also

$$\begin{aligned} U_{N+1} &\equiv U_{(N+1)/3}[V^2_{(N+1)/3} - q^{(N+1)/3}] \\ &\equiv 0 \pmod N. \end{aligned}$$

https://doi.org/10.4153/CMB-1972-101-7 Published online by Cambridge University Press

By Theorem 3 the prime factors of N must be of the form $k3^n \pm 1$; by Lemma 1, N is a prime.

If $A=1$, $q=7$, we obtain the following:

COROLLARY. *If* $n \equiv a \pmod 6$, *where* $a=1, 2, 3, 5$ *and* P_1 *is selected from Table* 1 *below*, $N=2.3^n-1$ *is a prime if and only if*

$$P_n \equiv \pm 1 \pmod N,$$

where

$$P_{k+1} \equiv P_k(P_k^2-3) \pmod N.$$

a	1	2	3	5
P_1	$4(N-5)/7+1$	$2(N-3)/7-1$	$5(N-4)/7+1$	$3(N-2)/7-1$

Table 1.

We now summarize the steps necessary to carry out the test for the primality of $N=2A3^n-1$, $A<4.3^n-1, 3\nmid A$. We give some idea of the time required for these steps by indicating the approximate number of operations needed to complete each of them.

(1) Find a prime $q \equiv 1 \pmod 3$ such that

$$N^{(q-1)/3} \equiv 1 \pmod q.$$

This is not very difficult in practice; in fact, for $n<1000$, $A \leq 50$, we can find such a $q \leq 79$.

(2) Obtain integers r and s such that

$$4q = r^2+27s^2,$$

where $r \equiv 1 \pmod 3$. For small values of q, table 2 below should suffice for this operation. For q beyond the range of this table, the table in Cunningham [2] could be used. On a computer, however, it would be easier to simply obtain these numbers by exclusion, a process requiring approximately $\sqrt{q}$ operations.

(3) Calculate K such that

$$qK \equiv 1 \pmod N.$$

This is best accomplished using the Euclidean algorithm. The average time required for this step varies directly with the logarithm of q.

(4) Find V_{2A}. For small values of A this can be done by using the recurrence relation

$$V_m = -rV_{m-1} - qV_{m-2},$$

where $V_0=2$, $V_1=-r$. For large values of A a duplication formula such as that described in [4] should be used. The number of operations required for this step is of order $\log A$.

(5) We put

$$P_1 \equiv V_{2A}K^A \pmod{N}.$$

This is a process of order $\log A$ (see [4]). Define

$$P_{k+1} \equiv P_k(P_k^2-3) \pmod{N}$$

and calculate $P_n \pmod{N}$. N will be a prime if and only if N divides one of P_n+1 or P_n-1. It is easy to see that the time required to complete the entire algorithm varies directly with $\log N$.

q	r	s	q	r	s	q	r	s	q	r	s
7	1	1	31	4	2	61	1	3	79	−17	1
13	−5	1	37	−11	1	67	−5	3	97	19	1
19	7	1	43	−8	2	73	7	3	103	13	3

Table 2.

4. **Example.** Let $N=13121=2.3^8-1$; then $P_1=2(13118)/7-1=3747$. The successive values of $P_k \pmod{N}$ are then 3747, 879, 5842, 1288, 521, 1060, 6529, 1.

Bibliography

1. C. Cailler, *Sur les congruences du troisième degré*, L'Enseig. Math., **10** (1908), 474–487.
2. A. J. C. Cunningham, *Quadratic Partitions*, London, 1907.
3. D. H. Lehmer, *An extended theory of Lucas' functions*, Ann. of Math. (2), **31** (1930), 419–448.
4. ———, *Computer technology applied to the theory of numbers*, M.A.A. studies in Mathematics, **6** (1969), 117–151.
5. Emma Lehmer, *Criteria for cubic and quartic residuacity*, Mathematika **5** (1958), 20–29.
6. Edouard Lucas, *Théorie des functions numériques simplement périodiques*, Amer. J. Math. **1** (1878), 184–240, 289–321.
7. H. Reisel, *Lucasian criteria for the primality of $N=h\cdot 2^n-1$*, Math. Comp. **23** (1969). 869–875.
8. R. M. Robinson, *The converse of Fermat's theorem*, Amer. Math. Monthly, **64** (1957), 703–710.
9. H. J. S. Smith, *Report on the Theory of Numbers*, Chelsea, New York, (1965), 103–105.
10. H. C. Williams and C. R. Zarnke, *A report on prime numbers of the forms $M=(6a+1)2^{2m-1}-1$ and $M'=(6a-1)2^{2m}-1$*, Math. Comp. **22** (1968), 420–422.

University of Manitoba,
Winnipeg, Manitoba