Lucasian Criteria for the Primality of $N = h \cdot 2^n - 1$

By Hans Riesel

Abstract. Let $v_i = v_{i-1}^2 - 2$ with v_0 given. If $v_{n-2} \equiv 0 \pmod N$ is a necessary and sufficient criterion that $N = h \cdot 2^n - 1$ be prime, this is called a Lucasian criterion for the primality of N. Many such criteria are known, but the case $h = 3A$ has not been treated in full generality earlier. A theorem is proved that (by aid of computer) enables the effective determination of suitable numbers v_0 for any given N, if $h < 2^n$. The method is used on all N in the domain $h = 3(6)105$, $n \leqq 1000$. The Lucasian criteria thus constructed are applied, and all primes $N = h \cdot 2^n - 1$ in the domain are tabulated.

Introduction. Let $u_0 \geqq 3$ be a given integer, and define $u_\nu = u_{\nu-1}^2 - 2$ for $\nu = 1, 2, 3, \cdots$. The numbers u_ν are said to form a Lucasian sequence with its first element $= u_0$. If h is odd and if $2^n > h$, then necessary and sufficient criteria for the primality of $N = h \cdot 2^n - 1$ exist, and are known for many values of h and n. These criteria are of the following type: For a suitable value of u_0, the number N is prime, if and only if $u_{n-2} \equiv 0 \pmod N$. If $h = 1$, the value $u_0 = 4$ will fit for all odd values of n (Lehmer [2]), and $u_0 = 3$ will fit for all $n \equiv 3 \pmod 4$, (Lucas [3]). If $h = 3$, the value $u_0 = 5778$ will fit for $n \equiv 0, 3 \pmod 4$ (Lehmer [2]). If $h = 6a \pm 1$ and $3 \nmid N$, the value $u_0 = (2 + \sqrt{3})^h + (2 - \sqrt{3})^h$ will fit for all n (Riesel [4]).

The mentioned necessary and sufficient criteria for the primality of the numbers $N = h \cdot 2^n - 1$ are said to be of Lucas' type. The importance of these criteria lies in the fact that they are the most efficient primality criteria hitherto deduced.

Apart from the results, mentioned above, and some other similar results, likewise of limited generality, nobody seems to have undertaken a systematic study of the problem of finding a Lucasian criterion for a given combination of h and n. This is, no doubt, due to the large volume of computation needed in trying out different possibilities for u_0. By use of electronic computers, however, this is a feasible task, and the objective of this paper is to show how it can be done. Finally, we have used the technique to find all primes $N = 3A \cdot 2^n - 1$ for all odd $A \leqq 35$ and all $n \leqq 1000$.

Known Results, Needed in our Proofs. We take the following well-known Theorems 1—2 from the arithmetical theory of quadratic fields $K(\sqrt{D})$ (see, e.g., Hardy and Wright: *Theory of Numbers*) for granted:

Theorem 1 (Fermat's Theorem in $K(\sqrt{D})$). *If α is an integer in the quadratic field $K(\sqrt{D})$, if p is an odd rational prime, and if $(\alpha, p) = 1$ in $K(\sqrt{D})$, then*

$$\alpha^{p-1} \equiv 1 \pmod p\,, \quad \text{if } (D/P) = 1\,,$$
$$\alpha^{p+1} \equiv \alpha\bar{\alpha} \pmod p\,, \quad \text{if } (D/P) = -1\,.$$

(D/P) means Legendre's symbol, and D is a square free integer.

Theorem 2. *If a natural number K exists, such that*

$$\alpha^K \equiv -1 \pmod p\,,$$

then a smallest natural number k exists, such that

Received October 4, 1968.

$$\alpha^k \equiv -1 \pmod p ,$$

and

$$K = k \cdot (\textit{an odd number}) .$$

The smallest natural number e, such that

$$\alpha^e \equiv +1 \pmod p ,$$

is $e = 2k$.

Two Theorems, Basic for Lucasian Criteria. We now proceed to prove the following two theorems:

THEOREM 3. *If* N *is a prime,* $(D/N) = -1$,

$$\alpha = \frac{(a + b\sqrt{D})^2}{r}, \quad \textit{and} \quad (r/N) \cdot \frac{a^2 - b^2 D}{r} = -1 ,$$

then

$$\alpha^{(N+1)/2} \equiv -1 \pmod N .$$

a, b and r are rational integers. If $D \equiv 1 \pmod 4$, *however, a and b may both be odd integers times* $1/2$. *It is no loss to omit this possibility, since a multiplication of a, b, and* $r^{1/2} = (a^2 - b^2 D)^{1/2}$ *by the same constant does not change the theorem.*

Proof.

$$\begin{aligned} \alpha^{(N+1)/2} &= (a + b\sqrt{D})^{N+1}/r^{(N+1)/2} \\ &\equiv (a + b\sqrt{D})(a - b\sqrt{D})/(r^{(N-1)/2} \cdot r) = \frac{a^2 - b^2 D}{r} (r/N) \\ &\equiv -1 \pmod N , \end{aligned}$$

according to Theorem 1.

THEOREM 4. *If* $N = h \cdot 2^n - 1$, $h < 2^n$, $n \geqq 2$, *h is odd, α is an integer of* $K(\sqrt{D})$ *of the form* $\alpha = (a + b\sqrt{D})^2/|a^2 - b^2 D|$, $(\alpha, N) = 1$ *in* $K(\sqrt{D})$, *and*

$$\alpha^{(N+1)/2} \equiv -1 \pmod N ,$$

then N is a prime.

Proof. Let p be an arbitrary prime factor of N. Then obviously,

$$\alpha^{(N+1)/2} \equiv -1 \pmod p .$$

According to Theorem 2, then $(N + 1)/2 = h \cdot 2^{n-1} = k \cdot u$, where k is the smallest exponent > 0 with $\alpha^k \equiv -1 \pmod p$, and u is an odd integer. Thus $k = 2^{n-1}\,\delta$, where δ divides h. The smallest $e > 0$ with $\alpha^e \equiv 1 \pmod p$ will then be $e = 2k = 2^n \cdot \delta \geqq 2^n$.

Now, Theorem 1 gives

$$\begin{aligned} \alpha^{(p-1)/2} &= (a + b\sqrt{D})^{p-1}/|a^2 - b^2 D|^{(p-1)/2} \\ &\equiv \left(\frac{|a^2 - b^2 D|}{p}\right) \pmod p , \quad \text{if } (D/p) = +1 \end{aligned}$$

and

$$\alpha^{(p+1)/2} = \frac{a^2 - b^2D}{|a^2 - b^2D|}\left(\frac{|a^2 - b^2D|}{p}\right) \pmod p\,, \quad \text{if } (D/p) = -1\,.$$

By squaring, we get

$$\alpha^{p\pm 1} \equiv 1 \pmod p\,.$$

Now, since $e \geqq 2^n$, we find that $p \pm 1 \geqq 2^n$ for any prime factor p of N. The smallest possible p would then be $p = 2^n - 1$. Since N is no square ($N \equiv 3 \pmod 4$, since $n \geqq 2$), a factorization of N would yield

$$N = p\cdot q \geqq p(p+2) \geqq (2^n - 1)(2^n + 1) = 2^n\cdot 2^n - 1 > h\cdot 2^n - 1 = N\,,$$

a contradiction. Thus N is prime.

Lucasian Criteria for Primality. The Theorems 3 and 4 together form the basis for the both necessary and sufficient Lucasian prime-criteria for numbers of the form $h\cdot 2^n - 1$, if h is odd and $< 2^n$, and $n \geqq 2$. Suppose that we have found numbers D, a, b, and $r = |a^2 - b^2D|$, such that all the conditions in Theorem 3 are fulfilled. Then, since

$$(\alpha^{h\cdot 2^s} + \alpha^{-h\cdot 2^s})^2 = \alpha^{h\cdot 2^{s+1}} + \alpha^{-h\cdot 2^{s+1}} + 2$$

we find the recursion formula

$$u_{s+1} = u_s^2 - 2$$

if we choose

$$u_s = \alpha^{h\cdot 2^s} + \alpha^{-h\cdot 2^s}\,.$$

Furthermore,

$$\begin{aligned} u_{n-2} &= \alpha^{h\cdot 2^{n-2}} + \alpha^{-h\cdot 2^{n-2}} \\ &= \alpha^{-h\cdot 2^{n-2}}(\alpha^{h\cdot 2^{n-1}} + 1) \equiv 0 \pmod N) \end{aligned}$$

will be a necessary and sufficient condition for the primality of N, since $\alpha^{-h\cdot 2^{n-2}}$ is a unit of $K(\sqrt{D})$. ($N(\alpha) = \alpha\bar{\alpha} = (a^2 - b^2D)^2/|a^2 - b^2D|^2 = 1$), and so α and $\alpha^{-h\cdot 2^{n-2}}$ are units of $K(\sqrt{D})$. So, since $u_0 = \alpha^h + \alpha^{-h}$, we get the following:

THEOREM 5 (LUCAS' CRITERIA FOR $h\cdot 2^n - 1$). *Suppose that $n \geqq 2$, h is odd $< 2^n$, $N = h\cdot 2^n - 1$, $r = |a^2 - b^2D|$ with square free D, $\alpha = (a + b\sqrt{D})^2/r$, $(D/N) = -1$, and $(r/N)\ (a^2 - b^2D)/r = -1$. Then a necessary and sufficient condition that N shall be prime is that*

$$u_{n-2} \equiv 0 \pmod N\,,$$

if $u_\nu = u_{\nu-1}^2 - 2$ with $u_0 = \alpha^h + \alpha^{-h}$.

Remark. It would be possible to give a weaker condition than $h < 2^n$ in the same way as is shown in [4].

Since α is a unit of $K(\sqrt{D})$, $\alpha = \epsilon^s$, where $s = 1, 2, 3, \cdots$, and ϵ is a fundamental unit of $K(\sqrt{D})$. If ϵ has a representation of the form $\epsilon = (a + b\sqrt{D})^2/r$, s must be odd, since an even number s in this case would give already $\alpha^{(N+1)/4} \equiv -1 \pmod N$ in Theorem 3, and thus $u_{n-3} \equiv 0 \pmod N$. The simplest choice of α is thus $\alpha = \epsilon$, if $\epsilon = (a + V\overline{D})^2/r$, and $\alpha = \epsilon^2$, if ϵ lacks such a representation.

TABLE 1.

Values of D and representations of the fundamental units $\epsilon = (a + b\sqrt{D})^2/r$ in $K(\sqrt{D})$ for $v_1 = \epsilon + \epsilon^{-1} \leqq 100$. In some cases ϵ^2 is used instead of ϵ.

v_1	D	a	b	r	$(a^2 - b^2D)/r$	v_1	D	a	b	r	$(a^2 - b^2D)/r$
3	5	1	1	4	$-1, \epsilon^2$	54	182	13	1	13	-1
4	3	1	1	2	-1	55	3021	53	1	212	-1
5	21	3	1	12	-1	56	87	9	1	6	-1
6	2	1	1	1	$-1, \epsilon^2$	57	3245	55	1	220	-1
8	15	3	1	6	-1	58	210	14	1	14	-1
9	77	7	1	28	-1	59	3477	57	1	228	-1
10	6	2	1	2	-1	60	899	29	1	58	-1
11	13	3	1	4	$-1, \epsilon^2$	61	413	21	1	28	$+1$
12	35	5	1	10	-1	63	3965	61	1	244	-1
13	165	11	1	44	-1	64	1023	31	1	62	-1
15	221	13	1	52	-1	65	469	21	1	28	-1
16	7	3	1	2	$+1$	66	17	4	1	1	$-1, \epsilon^2$
17	285	15	1	60	-1	67	4485	65	1	260	-1
19	357	17	1	68	-1	68	1155	33	1	66	-1
20	11	3	1	2	-1	69	4757	67	1	268	-1
21	437	19	1	76	-1	70	34	6	1	2	$+1$
22	30	5	1	5	-1	71	5037	69	1	276	-1
24	143	11	1	22	-1	72	1295	35	1	70	-1
25	69	9	1	12	$+1$	73	213	15	1	12	$+1$
26	42	6	1	6	-1	74	38	6	1	2	-1
27	29	5	1	4	$-1, \epsilon^2$	75	5621	73	1	292	-1
28	195	13	1	26	-1	76	1443	37	1	74	-1
29	93	9	1	12	-1	77	237	15	1	12	-1
30	14	4	1	2	$+1$	78	95	10	1	5	$+1$
31	957	29	1	116	-1	80	1599	39	1	78	-1
32	255	15	1	30	-1	81	6557	79	1	316	-1
33	1085	31	1	124	-1	82	105	10	1	5	-1
35	1221	33	1	132	-1	83	85	9	1	4	$-1, \epsilon^2$
36	323	17	1	34	-1	84	1763	41	1	82	-1
37	1365	35	1	140	-1	85	7221	83	1	332	-1
38	10	3	1	1	$-1, \epsilon^2$	86	462	21	1	21	-1
39	1517	37	1	148	-1	87	7565	85	1	340	-1
40	399	19	1	38	-1	88	215	15	1	10	$+1$
41	1677	39	1	156	-1	89	7917	87	1	348	-1
42	110	10	1	10	-1	90	506	22	1	22	-1
43	205	15	1	20	$+1$	91	8277	89	1	356	-1
44	483	21	1	42	-1	92	235	15	1	10	-1
45	2021	43	1	172	-1	93	8645	91	1	364	-1
46	33	6	1	3	$+1$	94	138	12	1	6	$+1$
48	23	5	1	2	$+1$	95	9021	93	1	372	-1
49	2397	47	1	188	-1	96	47	7	1	2	$+1$
50	39	6	1	3	-1	97	1045	33	1	44	$+1$
51	53	7	1	4	$-1, \epsilon^2$	99	9797	97	1	388	-1
53	2805	51	1	204	-1	100	51	7	1	2	-1

We thus find that, given h and n, the "only" thing to do is to try different values of D and check if the fundamental unit ϵ (or sometimes ϵ^2) of $K(\sqrt{D})$ fits into the conditions of Theorem 5. Having found D and α, we can calculate u_0 (or, if N is large, preferably $u_0 \pmod N$) by using the well-known recursion for $v_\nu = \alpha^\nu + \alpha^{-\nu}$:

$$v_0 = 2 , \quad v_1 = \alpha + \alpha^{-1} , \quad v_\nu = (\alpha + \alpha^{-1})v_{\nu-1} - v_{\nu-2} .$$

The Choice of D and v_1. As usual in problems with conditions on (D/N), it turns out that a certain value of D will fit for values of n in certain arithmetic series, provided h is fixed. It is possible to state all the results in this form, but it is a rather complicated and impractical way of describing the situation. Instead one can try to find a D for each combination of h and n in a certain region.

In which order are the different D's to be tested? Since nothing in particular is known about the D's in the general case, the author chose to try the values of D in increasing order of magnitude for the numbers $v_1 = \alpha + \alpha^{-1}$. This gives the smallest possible values of u_0. However, it was then first necessary to find a connection between D and v_1. This is simple. Since $v_1 = \alpha + \alpha^{-1}$, we find $\alpha^2 - v_1\alpha + 1 = 0$, and $D =$ the square free part of $(v_1^2 - 4)$. For the different values of D we then find the representations of $\epsilon = (a + b\sqrt{D})^2/r$, if any, in [1]. The result is given in Table 1 for all $v_1 \leqq 100$. The values of $v_1 = x^2 - 2$ (resembling $\alpha^2 + \alpha^{-2}$) and $v_1 = x^3 - 3x$ (resembling $\alpha^3 + \alpha^{-3}$) and so on, are omitted from Table 1.

The following values of D are lacking representations of ϵ of the form $\epsilon = (a + b\sqrt{D})^2/r$: $D = 5, 2, 13, 29, 10, 53, 17$, and 85 (if $v_1 \leqq 100$). This fact is, in Table 1, indicated by "ϵ^2" in the column for $(a^2 - b^2D)/r$. These cases are particularly interesting, since r is then 1 or 4, and $(r/N) = +1$ for all values of N. They are also the only cases (in the table) where (r/N) is always $= +1$ (r is a perfect square). Furthermore, $(a^2 - b^2D)/r = -1$ in these cases, and so the condition

$$(r/N)\,\frac{a^2 - b^2D}{r} = -1$$

in Theorem 5 is fulfilled for all N. Thus each of these particular values of D gives a Lucasian criterion for N, if only the one condition, $(D/N) = -1$, is fulfilled. It thus makes it a little less complicated in these cases to write down, in form of different arithmetic series, those combinations of h and n for which the corresponding value of D can be used to construct a Lucasian criterion for N. For $D = 5$, e.g., we find

$$(D/N) = \left(\frac{5}{h\cdot 2^n - 1}\right) = \left(\frac{h\cdot 2^n - 1}{5}\right) = -1$$

if and only if

$$h\cdot 2^n - 1 \equiv \pm 2 \pmod 5$$

or

$$h\cdot 2^n \equiv 3, 4 \pmod 5 .$$

The following combinations of h and n satisfy one of these congruences:

$$h \equiv 1 \pmod 5 \text{ and } n \equiv 2, 3 \pmod 4$$
$$h \equiv 2 \pmod 5 \text{ and } n \equiv 1, 2 \pmod 4$$
$$h \equiv 3 \pmod 5 \text{ and } n \equiv 0, 3 \pmod 4$$
$$h \equiv 4 \pmod 5 \text{ and } n \equiv 0, 1 \pmod 4.$$

To avoid unnecessary testing we may remark that D cannot be any divisor of $2h$, because $(D/N) = +1$ in these cases. A preliminary search for small prime factors of N is worthwhile, since such a discovery obviates the necessity of testing N for primality.

The Computations. According to the preceding scheme, the author has run a program to find a possible D for every $N = h \cdot 2^n - 1$ in the range $h = 3(6)105$ and $n \leqq 1000$. (As has already been pointed out in the Introduction, $v_1 = 4$ will fit for all other odd values of h, unless $3|N$.) We succeeded in finding a D or a small factor for every N in this range. The largest value of v_1 needed was $v_1 = 57$ (for $N = 63 \cdot 2^{354} - 1$).

TABLE 2.
All primes $3A \cdot 2^n - 1$ *for* $n \leqq 1000$.

3A	n
3	1, 2, 3, 4, 6, 7, 11, 18, 34, 38, 43, 55, 64, 76, 94, 103, 143, 206, 216, 306, 324, 391, 458, 470, 827
9	1, 3, 7, 13, 15, 21, 43, 63, 99, 109, 159, 211, 309, 343, 415, 469, 781, 871, 939
15	1, 2, 4, 5, 10, 14, 17, 31, 41, 73, 80, 82, 116, 125, 145, 157, 172, 202, 224, 266, 289, 293, 463
21	1, 2, 3, 7, 10, 13, 18, 27, 37, 51, 74, 157, 271, 458, 530, 891
27	1, 2, 4, 5, 8, 10, 14, 28, 37, 38, 70, 121, 122, 160, 170, 253, 329, 362, 454, 485, 500, 574, 892, 962
33	2, 3, 6, 8, 10, 22, 35, 42, 43, 46, 56, 91, 102, 106, 142, 190, 208, 266, 330, 360, 382, 462, 503, 815
39	3, 24, 105, 153, 188, 605, 795, 813, 839
45	1, 2, 3, 4, 5, 6, 8, 9, 14, 15, 16, 22, 28, 29, 36, 37, 54, 59, 85, 93, 117, 119, 161, 189, 193, 256, 308, 322, 327, 411, 466, 577, 591, 902, 928, 946
51	1, 9, 10, 19, 22, 57, 69, 97, 141, 169, 171, 195, 238, 735, 885
57	1, 2, 4, 5, 8, 10, 20, 22, 25, 26, 32, 44, 62, 77, 158, 317, 500, 713
63	2, 3, 8, 11, 14, 16, 28, 32, 39, 66, 68, 91, 98, 116, 126, 164, 191, 298, 323, 443, 714, 758, 759
69	1, 4, 5, 7, 9, 11, 13, 17, 19, 23, 29, 37, 49, 61, 79, 99, 121, 133, 141, 164, 173, 181, 185, 193, 233, 299, 313, 351, 377, 540, 569, 909
75	1, 3, 5, 6, 18, 19, 20, 22, 28, 29, 39, 43, 49, 75, 85, 92, 111, 126, 136, 159, 162, 237, 349, 381, 767, 969
81	3, 5, 11, 17, 21, 27, 81, 101, 107, 327, 383, 387, 941
87	1, 2, 8, 9, 10, 12, 22, 29, 32, 50, 57, 69, 81, 122, 138, 200, 296, 514, 656, 682, 778, 881
93	3, 4, 7, 10, 15, 18, 19, 24, 27, 39, 60, 84, 111, 171, 192, 222, 639, 954
99	1, 4, 5, 7, 8, 11, 19, 25, 28, 35, 65, 79, 212, 271, 361, 461
105	2, 3, 5, 6, 8, 9, 25, 32, 65, 113, 119, 155, 177, 299, 335, 426, 462, 617, 896

For each N without a small prime factor, the prime character was established by a second program, which checks $u_{n-2} \equiv 0 \pmod{N}$. For $h \not\equiv 3A$, $h \leqq 151$, and $n \leqq 1000$, this work was recently done by Williams and Zarnke [5]. For $h = 3(6)105$, and $n \leqq 1000$, the author did the corresponding work, using the previously found values of v_1. The results are given in Table 2. Comparing our results with those of Robinson [6], we incidentally found some large prime twins,* namely

* Editorial note: The two largest pairs here, $9 \cdot 2^{211} \pm 1$ and $45 \cdot 2^{189} \pm 1$ were both found by Emma Lehmer in 1964. While they have not been previously published, they are known to a number of investigators.

$$9 \cdot 2^{43} \pm 1, \quad 9 \cdot 2^{63} \pm 1, \quad 9 \cdot 2^{211} \pm 1,$$
$$45 \cdot 2^{189} \pm 1, \quad 75 \cdot 2^{43} \pm 1, \quad \text{and} \quad 99 \cdot 2^{65} \pm 1.$$

The computing time was approximately $10^{-8} n^3$ seconds to test $h \cdot 2^n - 1$ on an IBM/360 model 75 computer.

In analogy to the Cullen numbers (primes of the form $n \cdot 2^n + 1$), we may note that $n \cdot 2^n - 1$ is prime for $n = 2, 3, 6, 30, 75$, and 81 for $n \leqq 110$.

Acknowledgements. All programming and supervising of the runs was carefully done by Mr. Torbjörn Kaving, Stockholm, and the computing time put at our disposal by the Royal Institute of Technology, Stockholm.

Royal Institute of Technology
100 44 Stockholm 70
Sweden

1. E. L. INCE, *Cycles of Reduced Ideals in Quadratic Fields*, British Association for the Advancement of Science, London, 1934.

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

E. LUCAS, "Théorie des fonctions numériques simplement périodiques," *Amer. J. Math.*, v. 1, 1878, pp. 184–239, pp. 289–321.

4. 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. MR **17**, 945.

5. H. C. WILLIAMS & 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.*, v. 22, 1968, pp. 420–422. MR **37** #2680.

6. R. M. ROBINSON, "A report on primes of the form $k \cdot 2^n + 1$ and on factors of Fermat numbers," *Proc. Amer. Math. Soc.*, v. 9, 1958, pp. 673–681. MR **20** #3097.