MATHEMATICS OF COMPUTATION, VOLUME 33, NUMBER 148
OCTOBER 1979, PAGES 1337–1342

Some Primes of the Form $(a^n - 1)/(a - 1)$

By H. C. Williams and E. Seah

Abstract. A table of primes of the form $(a^n - 1)/(a - 1)$ for values of a and n such that $3 \leqslant a \leqslant 12$, $2 \leqslant n \leqslant 1000$ is presented. A description is given of the techniques used to obtain this table, and some numbers such as $(10^{1031} - 1)/9$ which are pseudoprime but whose primality is not yet rigorously established are also discussed.

1. Introduction. For many years there has been considerable interest in the factorization of integers of the form $a^n - 1$. Much work has been done on primes of the form $2^n - 1$ including an empirical analysis of the distribution of such primes* (Gillies [3], Tuckerman [6]) and on the primes of the form $(10^n - 1)/9$, the so-called repunit numbers. However, there has been little recent work on primes of the form $(a^n - 1)/(a - 1)$ for values of a other than 2 and 10.

Some tables of primes of this form for small values of a can be found in Kraitchik [4] but the methods available at the time [4] was written did not permit investigation of such numbers for large values of n. Modern methods of primality testing (see Williams [9]) often allow for the determination of quite large primes. The purpose of this paper is to illustrate the power and limitations of these techniques by utilizing them to attempt to tabulate all primes of the form $(a^n - 1)/(a - 1)$ for $3 \leqslant a \leqslant 12$ and $1 \leqslant n \leqslant 1000$.

2. Available Techniques. In order to test N (odd) for primality it is usually necessary to have a number of factors of $N - 1$. Suppose

$$N - 1 = F_1 S_1 S_2 S_3 \cdots S_k,$$

where $(S_i, F_1) = 1$ $(i = 1, 2, 3, \ldots, k)$,

$$F_1 = \prod_{i=1}^{n} q_i^{\alpha_i}$$

is completely factored, and any prime factor of S_i $(i = 1, 2, 3, \ldots, k)$ must exceed a factor bound B (>2). We have the following results of Brillhart, Lehmer, and Selfridge [1] which can be used as tests for primality.

THEOREM 1. *If for each $q_i \mid F_1$, there exists an integer a_i such that*

$$(a_i^{(N-1)/q_i} - 1, N) = 1$$

Received November 20, 1978.
AMS (MOS) subject classifications (1970). Primary 10–04, 10A25.
*Recently C. Noll and L. Nickel have identified $2^{21701} - 1$ as a prime.

0025-5718/79/0000-0169/$02.50

and

$$a_i^{N-1} \equiv 1 \pmod{N},$$

then any prime divisor of N must have the form $mF_1 + 1$.

THEOREM 2. *If for each* S_i *above, there exists an integer* b_i *such that*

$$(b_i^{(N-1)/S_i} - 1, N) = 1$$

and

$$b_i^{N-1} \equiv 1 \pmod{N},$$

then any prime divisor of N must have the form $ms_1s_2s_3 \cdots s_k + 1$, *where* s_i *is some prime divisor of* S_i.

Clearly, if the conditions of both Theorem 1 and Theorem 2 hold, then any prime factor of N must have the form $s_1s_2s_3 \cdots s_kF_1m + 1 > B^kF_1$. If $(B^kF_1)^2 > N$, N must be a prime.

Now if $N_n(a) = (a^n - 1)/(a - 1)$, then

$$N_n(a) - 1 = aN_{n-1}(a);$$

also, if $N_n(a)$ is a prime, then n is a prime. As we are interested only in possible prime values of $N_n(a)$, we see that $n - 1$ is not a prime and, as a consequence, $N_n(a) - 1$ can first be factored algebraically. We then try to find factors of the algebraic divisors. The process of finding these factors is frequently time consuming and often very difficult; thus, we attempt to minimize the number of factors of $N_n(a) - 1$ which we will need. To this end we make use of the following theorem, which is an extension of some results in [1].

THEOREM 3. *Suppose that the conditions of Theorems* 1 *and* 2 *hold for some N and let*

$$D(t) = (2tF_1^2 + AF_1 + 2)^2 - 4N,$$

where

$$A \equiv (N - 1)/F_1 \pmod{2F_1}$$

and $0 < A < 2F_1$. *If* $D(t)$ *is not a perfect square for any* t *such that* $0 \leqslant t \leqslant T$ *and* $B^k(A + 2TF_1 - B^k)F_1^2 > N$, *then N is a prime.*

Proof. If p is any prime divisor of N, then $p = 1 + m_1F_1$ and $N/p = 1 + m_2F_1$, where $m_1, m_2 > s_1 \cdot s_2 \cdot s_3 \cdot \ldots \cdot s_k > B^k$. Thus,

$$(N - 1)/F_1 = m_1m_2F_1 + m_1 + m_2.$$

Since $(N - 1)/F_1$ is odd and F_1 is even, we must have $m_1 + m_2$ odd and consequently m_1m_2 is even; thus

$$m_1 + m_2 = A + 2tF_1 \quad (t \geqslant 0)$$

and

$$N = (A + 2tF_1 - m_2)m_2F_1^2 + (A + 2tF_1)F_1 + 1.$$

If we put $X = m_2F_1$, we get

$$X^2 - X(AF_1 + 2tF_1^2) - AF_1 - 2tF_1^2 + N - 1 = 0.$$

Since X must be an integer and the discriminant of this quadratic in X is $D(t)$, we must have $t > T$. Now both $m_1, m_2 > B^k$ and $m_1 + m_2 \geqslant A + 2TF_1$; hence,

$$N > m_1m_2F_1^2 \geqslant B^k(A + 2TF_1 - B^k)F_1^2 > N, \quad \text{a contradiction.}$$

Note that if $D(t)$ is a perfect square, say K^2, for some t, then K must be even and

$$N = (tF_1^2 + AF_1/2 + 1)^2 - (K/2)^2.$$

If $N \neq 2tF_1^2 + AF_1 + 1$, we have a nontrivial factorization of N.

The utilization of this theorem presents little difficulty for values of $T < 10^8$. As there is rarely a chance that N will have a nontrivial factorization, we simply show that for each $t \leqslant T$ the Legendre symbol $(D(t) \mid \pi_i) = -1$ for some π_i in a set Π of about 30 small primes. This is most easily and rapidly accomplished by sieving out all values of $t \leqslant T$ such that $(D(t') \mid \pi_i) = -1$ when $t \equiv t' \pmod{\pi_i}$.

In spite of the existence of the devices mentioned above for minimizing the amount of factoring to be done, we must still do some factoring and, in some cases, a great deal of it. The usual method is to trial divide $N - 1$ up to a factor bound B by using a 'wheel' method such as that described by Wunderlich and Selfridge [10]. D. H. Lehmer has implemented a version of this technique on the ILLIAC IV and any factor bound B recorded below which exceeds 10^8 is due to him.

After trial division, the $P - 1$ method discovered by Pollard [5] can be used. This technique, known to D. N. and D. H. Lehmer but never published by them, consists of calculating $f = (b^P - 1, M)$ for some b, where $P = \Pi_{i=1}^{h} p_i^{\beta_i}$. Here p_i is the ith prime and $p_i^{\beta_i}$ is the largest power of p_i less than a fixed bound BP. Very often f is not 1 or M and a factor of M results.

Finally, we make mention of an already existing (although not yet published) table [2] of factors of numbers of the form $a^n - 1$. Several times the demonstration of the primality of $N_n(a)$ was easily facilitated through the existence of factors of $N_{n-1}(a)$ in this table.

3. Results. The algorithms mentioned above were implemented on an IBM 370-168 computer and run for all possible primes of the form $N_n(a)$ for $3 \leqslant a \leqslant 12$ and $n \leqslant 1000$. In the case of $a = 10$, the work of Williams [8] was continued from $n = 1000$ to 2000. The candidates for primality were, of course, those values of $N_n(a)$ such that n is a prime, $N_n(a)$ does not have a small prime factor and

$$13^{N_n(a)-1} \equiv 1 \pmod{N_n(a)}.$$

In Table 1 below we present the results of these computer runs together with results found previously by others.

a	n
3	3, 7, 13, 71†, 103†, 541
5	3, 7, 11, 13, 47†, 127†, 149††, 181††, 619, 929*
6	2, 3, 7, 29†, 71†, 127††, 271, 509
7	5, 13, 131††, 149††
10	2, 19, 23, 317, 1031*
11	17, 19, 73†, 139**, 907*
12	2, 3, 5, 19, 97††, 109††, 317, 353

TABLE 1

Table of all values of n such that $(a^n - 1)/(a - 1)$ is a prime for $3 \leqslant a \leqslant 12$, $2 \leqslant n \leqslant 1000$. (For $a = 10$, the table records all primes for $2 \leqslant n \leqslant 2000$.)

Remarks. (1) Numbers identified by an (*) have not yet been proved prime. they are pseudoprime to several bases and are most likely to be prime, but not enough factors of $N_n(a) - 1$ are known yet for primality testing. See the next section.

(2) Most of the prime values of $N_n(a)$ for $n \leqslant 23$ can be found in [4].

(3) Values of $N_n(a)$ with n marked by (†) were identified as prime in [2] and values of $N_n(a)$ with n marked by (††) were identified as pseudoprime in [2].

(4) The number $N_{139}(11)$ was identified as a pseudoprime at a time when the authors of [2] thought that the base 11 table of [2] would extend to 150 instead of the present limit of 135.

Some of the numbers proved prime above merit some extended discussion. For example, $(12^{317} - 1)/11$ and $(12^{353} - 1)/11$ could only be proved prime after the prime factor 77554200461 of $12^{158} + 1$ and the prime factor 1200913648289 of $12^{176} + 1$ were found by the $P - 1$ method with $BP = 130000$. Also, it was necessary to prove that

$$(12^{79} - 1)/11 \cdot 162109 \cdot 130479719$$

is a prime.

For $N_{509}(6) = (6^{509} - 1)/5$ and $B = 2702845200$, the only prime factors of $N_{509}(6) - 1$ are 2, 3, 7, 37, 509, 2287. Fortunately, the $P - 1$ method with $BP = 130000$ was able to isolate the prime factors 140348646913 and 25974264373441 of $6^{254} + 1$. This together with the fact that $(6^{127} - 1)/5$ is a prime was sufficient to prove $N_{509}(6)$ a prime.

Of the numbers proved prime here $(5^{619} - 1)/4$ was the most difficult. We first showed that $(5^{103} + 1)/6$ is a prime. With a factor bound of $B = 2575300800$ we have

$$5^{103} - 1 = 2^2 \cdot 3709 \cdot 28429 \cdot C_1,$$

$$5^{206} - 5^{103} + 1 = 3 \cdot 7 \cdot 1487527 \cdot 4527469 \cdot 642310267 \cdot C_2,$$

$$5^{206} + 5^{103} + 1 = 31 \cdot 619 \cdot C_3,$$

where C_1, C_2, C_3 are composite. Again the $P - 1$ technique with $BP = 130000$ provided the prime factors 330545029709161 of C_2 and 8934148519 of C_3. This, and Theorem 3 with $T = 2000000$ was sufficient to establish the primality of $(5^{619} - 1)/4$.

4. Limitations. As indicated in the previous section, the status of $(5^{929} - 1)/4$, $(11^{907} - 1)/10$ and $(10^{1031} - 1)/9$ is still unproved. We give below what is currently known about the factors of $N_n(a) - 1$ for these numbers.

For $(5^{929} - 1)/4$ we have complete factorizations of $5^{29} - 1$, $5^{29} + 1$, $5^{58} + 1$. Also

$$5^{116} + 1 = 2 \cdot 313 \cdot 233 \cdot 929 \cdot 33409 \cdot C_1,$$

$$5^{232} + 1 = 2 \cdot 17 \cdot 11489 \cdot C_2,$$

$$5^{464} + 1 = 2 \cdot 2593 \cdot 974401 \cdot 7099201 \cdot 29423041 \cdot C_3,$$

with a factor bound on C_1, C_2, C_3 of 5×10^7. No factors of the composite numbers C_1, C_2, C_3 were found by the $P - 1$ method with $BP = 130000$.

For $(11^{907} - 1)/10$, we have

$$11^{151} + 1 = 2^2 \cdot 3 \cdot 907 \cdot 3323 \cdot 255421785001 \cdot C_1,$$

$$11^{151} - 1 = 2 \cdot 5 \cdot 16944919 \cdot 13665285883 \cdot C_2,$$

$$11^{302} + 11^{151} + 1 = 7 \cdot 19 \cdot 2719 \cdot C_3,$$

$$11^{302} - 11^{151} + 1 = 3 \cdot 37 \cdot 799093 \cdot C_4.$$

Here the factor bound is 6×10^7 and the larger factors were found by using the $P - 1$ method with $BP = 130000$. C_1, C_2, C_3, C_4 are all composite.

The most interesting of these three numbers is $(10^{1031} - 1)/9$. We have

$$10^{103} - 1 = 3^2 \cdot 1031 \cdot 7034077 \cdot P_1,$$

$$10^{103} + 1 = 11 \cdot 1237 \cdot 44092859 \cdot 102860539 \cdot 984385009 \cdot C_1 \text{ [2]},$$

$$(10^{515} + 1)/(10^{103} + 1) = 7211 \cdot 9091 \cdot 497491 \cdot 569836171 \cdot 2013681931 \cdot C_2,$$

$$(10^{515} - 1)/(10^{103} - 1) = 41 \cdot 271 \cdot 5905014721 \cdot C_3,$$

where C_1, C_2, C_3 are composite, the factor bound on C_2 and C_3 is 10^8 and the factor bound on C_1 is 2^{35} [2]. The larger factors of the last two numbers were found by the $P - 1$ method with $BP = 70000$.

The number P_1 is a rather interesting prime and worthy of some further mention. It was necessary to use the methods of Williams and Judd [7] to prove the primality of this number. With a factor bound of 31250044839 we get

$$P_1 - 1 = 2^2 \cdot 103 \cdot C_1,$$

$$P_1 + 1 = 2 \cdot 3^2 \cdot 15358247\ C_2,$$

$$P_1^2 + P_1 + 1 = 7 \cdot C_3,$$

$$P_1^2 + 1 = 2 \cdot 5 \cdot 13 \cdot 941 \cdot 4049 \cdot 244200149 \cdot C_4,$$
$$P_1^2 - P_1 + 1 = 3 \cdot 19 \cdot 124783 \cdot C_5,$$

where C_1, C_2, C_3, C_4, C_5 are all composite. This is not enough to establish primality, but by using the $P - 1$ method on C_1, C_2, C_3, C_4, C_5 with $BP = 130000$, we get the prime factors 906732292429 of C_3 and 162391349686704225169920001 of C_5. This additional information was enough to prove P_1 a prime.

While it is not now possible with the information we have here to prove primality for the large numbers above, it should be mentioned that a decade ago no one would have thought it possible to prove a number like $(5^{619} - 1)/4$ a prime. Yet in the last ten years much progress has been made both in technology and in the theory of factorization and primality testing. Perhaps future results will permit a rigorous demonstration of the primality of these numbers.

5. Acknowledgements. The authors gratefully acknowledge the results obtained for them by D. H. Lehmer on the ILLIAC IV. Without these results this present work could not have been completed. They also wish to thank J. Brillhart and J. Selfridge for making a copy of [2] available and S. Yates for providing a table of factors of $10^n - 1$.

Department of Computer Science
University of Manitoba
Winnipeg, Manitoba, Canada R3T 2N2

1. J. BRILLHART, D. H. LEHMER & J. L. SELFRIDGE, "New primality criteria and factorizations of $2^m \pm 1$," *Math. Comp.*, v. 29, 1975, pp. 620–647.

2. J. BRILLHART, D. H. LEHMER, EMMA LEHMER, J. L. SELFRIDGE, BRYANT TUCKERMAN & S. S. WAGSTAFF, JR., "Factorizations of $b^n - 1$ and $b^n + 1$ for $b < 13$." (Unpublished.)

3. DONALD B. GILLIES, "Three new Mersenne primes and a statistical theory," *Math. Comp.*, v. 18, 1964, pp. 93–97.

4. M. KRAITCHIK, *Recherches sur la Théorie des Nombres*, Tome 2, Gauthier-Villars, Paris, 1929.

5. J. M. POLLARD, "Theorems on factorization and primality testing," *Proc. Cambridge Philos. Soc.*, v. 76, 1974, pp. 521–528.

6. BRYANT TUCKERMAN, "The 24th Mersenne prime," *Proc. Nat. Acad. Sci. U.S.A.*, v. 68, 1971, pp. 2319–2320.

7. H. C. WILLIAMS & J. S. JUDD, "Some algorithms for prime testing using generalized Lehmer functions," *Math. Comp.*, v. 30, 1976, pp. 867–886.

8. H. C. WILLIAMS, "Some primes with interesting digit patterns," *Math. Comp.*, v. 32, 1978, pp. 1306–1310.

9. H. C. WILLIAMS, "Primality testing on a computer," *Ars Combinatoria*, v. 5, 1978, pp. 127–185.

10. M. C. WUNDERLICH & J. L. SELFRIDGE, "A design for a number theory package with an optimized trial division routine," *Comm. ACM*, v. 17, 1974, pp. 272–276.