MATHEMATICS OF COMPUTATION, VOLUME 26, NUMBER 118, APRIL 1972

Some Results for $k! \pm 1$ and $2 \cdot 3 \cdot 5 \cdots p \pm 1$

By Alan Borning

Abstract. The numbers $k! \pm 1$ for $k = 2(1)100$, and $2 \cdot 3 \cdot 5 \cdots p \pm 1$ for p prime, $2 \leqq p \leqq 307$, were tested for primality. For $k = 2(1)30$, factorizations of $k! \pm 1$ are given.

In this note, we present the results of an investigation of $k! \pm 1$ and $2 \cdot 3 \cdot 5 \cdots p \pm 1$. An IBM 1130 computer was used for all computations.

A number N of one of these forms was first checked for primality by computing $b^{N-1} \pmod N$ for $b = 2$ or $b = 3$. If $b^{N-1} \not\equiv 1 \pmod N$, Fermat's Theorem implies that N is composite. On the other hand, if it was found that $b^{N-1} \equiv 1 \pmod N$, then the primality of N was established using one of the following two theorems, both due to Lehmer [1]. No composite numbers N of these forms were found which passed the above test.

THEOREM 1. *If, for some integer b, $b^{N-1} \equiv 1 \pmod N$, and $b^{(N-1)/q} \not\equiv 1 \pmod N$ holds for all prime factors q of $N - 1$, then N is prime.*

For primes of the forms $k! + 1$ and $2 \cdot 3 \cdot 5 \cdots p + 1$, a value for b satisfying the hypothesis of this theorem is given to aid anyone wishing to check these results.

THEOREM 2. *Given an odd integer N, suppose there is some Q such that the Jacobi symbols (Q/N) and $((1 - 4Q)/N)$ are both negative. Let α and β be the roots of $x^2 - x + Q = 0$, and let $V_n = \alpha^n + \beta^n$. If $V_{(N+1)/2} \equiv 0 \pmod N$, and $V_{2(N+1)/q} \not\equiv 2Q^{(N+1)/q}$ holds for all odd prime factors q of $N + 1$, then N is prime.*

For primes of the forms $k! - 1$ and $2 \cdot 3 \cdot 5 \cdots p - 1$, an appropriate value for Q is given.

Values of k such that $k! + 1$ is prime, $2 \leqq k \leqq 100$

k	b
2	2
3	3
11	26
27	37
37	67
41	43
73	149
77	89

Received June 8, 1971.
AMS 1969 *subject classifications.* Primary 1003; Secondary 1060.
Key words and phrases. Prime, factorial, product of primes, factorizations.

Values of k such that $k! - 1$ *is prime*, $2 \leqq k \leqq 100$

k	Q
3	2
4	7
6	19
7	26
12	19
14	62
30	122
32	37
33	53
38	61
94	199

Values of p such that $2 \cdot 3 \cdot 5 \cdots p + 1$ is *prime*, $2 \leqq p \leqq 307$

p	b
2	2
3	3
5	3
7	2
11	3
31	34

Values of p such that $2 \cdot 3 \cdot 5 \cdots p - 1$ *is prime*, $2 \leqq p \leqq 307$

p	Q
3	2
5	3
11	8
13	3
41	28
89	3

Previous results for primality as given by Sierpiński [2] include all $k \leqq 26$ in the case $k! + 1$, and $k \leqq 22$ and $k = 25$ in the case $k! - 1$. Kraitchik [3] gives factorizations of $k! + 1$ for $k \leqq 22$ and $k! - 1$ for $k \leqq 21$, as well as factorizations of $2 \cdot 3 \cdot 5 \cdots p + 1$ for $p \leqq 53$ and of $2 \cdot 3 \cdot 5 \cdots p - 1$ for $p \leqq 47$. The tables of Sierpiński and Kraitchik are in agreement with those given by the author, with the following exceptions:

(1) In Sierpiński $3! + 1$ is omitted from the list of primes;
(2) Both Sierpiński and Kraitchik erroneously list $20! - 1$ as a prime;
(3) Kraitchik fails to give the factor 5171 of $21! - 1$.

For $N = k! \pm 1, 2 \leqq k \leqq 30$, N composite, a variety of methods were used to find the prime factors of N. Trial division to 10^8 or so was tried first, and the prime factors discovered by this method were eliminated. The number remaining, say L, was then checked by computing b^{L-1} (mod L), as previously described. If $b^{L-1} \not\equiv 1$ (mod L), then L was factored by expressing it as the difference of two squares [4], or by employing the continued fraction expansion of $\sqrt{L}$ [5]. On the other hand, if $b^{L-1} \equiv 1$ (mod L), then the primality of L was established by completely factoring $L - 1$ and applying Theorem 1. If it proved too difficult to completely factor $L - 1$, $L + 1$ was factored instead and Theorem 2 applied. (For large L, the primality of the largest factor of $L - 1$ had to be established in a similar fashion, and so on for a chain of four or five factorizations.)

Factorizations of $k! + 1$, $k = 2(1)30$

$2! + 1 = 3$ (prime)
$3! + 1 = 7$ (prime)
$4! + 1 = 5^2$
$5! + 1 = 11^2$
$6! + 1 = 7\cdot 103$
$7! + 1 = 71^2$
$8! + 1 = 61\cdot 661$
$9! + 1 = 19\cdot 71\cdot 269$
$10! + 1 = 11\cdot 3\ 29891$
$11! + 1 = 399\ 16801$ (prime)
$12! + 1 = 13^2\cdot 28\ 34329$
$13! + 1 = 83\cdot 750\ 24347$
$14! + 1 = 23\cdot 37903\ 60487$
$15! + 1 = 59\cdot 479\cdot 462\ 71341$
$16! + 1 = 17\cdot 61\cdot 137\cdot 139\cdot 10\ 59511$

$17! + 1 = 661\cdot 5\ 37913\cdot 10\ 00357$
$18! + 1 = 19\cdot 23\cdot 29\cdot 61\cdot 67\cdot 1236\ 10951$
$19! + 1 = 71\cdot 1\ 71331\ 12733\ 63831$
$20! + 1 = 206\ 39383\cdot 11\ 78766\ 83047$
$21! + 1 = 43\cdot 4\ 39429\cdot 270\ 38758\ 15783$
$22! + 1 = 23\cdot 521\cdot 93\ 79961\ 00957\ 69647$
$23! + 1 = 47^2\cdot 79\cdot 148\ 13975\ 47368\ 64591$
$24! + 1 = 811\cdot 7\ 65041\ 18586\ 09610\ 84291$
$25! + 1 = 401\cdot 386\ 81321\ 80381\ 79201\ 59601$
$26! + 1 = 1697\cdot 2376\ 49652\ 99151\ 77581\ 52033$
$27! + 1 = 1088\ 88694\ 50418\ 35216\ 07680\ 00001$ (prime)
$28! + 1 = 29\cdot 1051\ 33911\ 93507\ 37450\ 00518\ 62069$
$29! + 1 = 14557\cdot 2185\ 68437\cdot 2778\ 94205\ 75550\ 23489$
$30! + 1 = 31\cdot 12421\cdot 82561\cdot 10\ 80941\cdot 7\ 71906\ 83199\ 27551$

Factorizations of $k! - 1$, $k = 2(1)30$

$2! - 1 = 1$
$3! - 1 = 5$ (prime)
$4! - 1 = 23$ (prime)
$5! - 1 = 7 \cdot 17$
$6! - 1 = 719$ (prime)
$7! - 1 = 5039$ (prime)
$8! - 1 = 23 \cdot 1753$
$9! - 1 = 11^2 \cdot 2999$
$10! - 1 = 29 \cdot 1\ 25131$
$11! - 1 = 13 \cdot 17 \cdot 23 \cdot 7853$
$12! - 1 = 4790\ 01599$ (prime)
$13! - 1 = 1733 \cdot 35\ 93203$
$14! - 1 = 8\ 71782\ 91199$ (prime)
$15! - 1 = 17 \cdot 31^2 \cdot 53 \cdot 15\ 10259$
$16! - 1 = 3041 \cdot 68802\ 33439$
$17! - 1 = 19 \cdot 73 \cdot 25\ 64437\ 11677$
$18! - 1 = 59 \cdot 2\ 26663 \cdot 4787\ 49547$
$19! - 1 = 653 \cdot 23\ 83907 \cdot 781\ 43369$
$20! - 1 = 1\ 24769 \cdot 1949\ 92506\ 80671$
$21! - 1 = 23 \cdot 89 \cdot 5171 \cdot 482\ 67136\ 12027$
$22! - 1 = 109 \cdot 606\ 56047 \cdot 17\ 00066\ 81813$
$23! - 1 = 51871 \cdot 498\ 39056\ 00216\ 87969$
$24! - 1 = 62\ 57931\ 87653 \cdot 99\ 14591\ 81683$
$25! - 1 = 149 \cdot 907 \cdot 1\ 14776\ 27434\ 14826\ 21993$
$26! - 1 = 20431 \cdot 197\ 39193\ 43774\ 68374\ 32529$
$27! - 1 = 29 \cdot 37\ 54782\ 56910\ 97766\ 07161\ 37931$
$28! - 1 = 239 \cdot 1\ 56967 \cdot 77980\ 78091 \cdot 104\ 21901\ 96053$
$29! - 1 = 31 \cdot 59 \cdot 311 \cdot 261\ 56201 \cdot 594\ 27855\ 62716\ 09021$
$30! - 1 = 265\ 25285\ 98121\ 91058\ 63630\ 84799\ 99999$ (prime)

Acknowledgement. The author gratefully acknowledges the help of Dr. Joseph Roberts and Michael Penk in this study, which was done at Reed College, Portland, Oregon, in connection with an undergraduate thesis.

Computer Services
University of Idaho
Moscow, Idaho 83843

1. D. H. Lehmer, "Computer technology applied to the theory of numbers," in *Studies in Number Theory* (W. J. LeVeque, Editor), Prentice-Hall, Englewood Cliffs, N. J., 1969, pp. 128-132. MR **40** #84.

2. W. Sierpinski, *Elementary Theory of Numbers*. Parts I, II, Monografie Mat., Tom 19, 38, PWN, Warsaw, 1950, 1959; English transl., Monografie Mat., Tom 42, PWN, Warsaw, 1964, p. 202. MR **13**, 821; MR **22** #2572; MR **31** #116.

3. Maurice Kraitchik, *Introduction à la Théorie des Nombres*, Gauthier-Villars, Paris, 1952, pp. 2, 8.

4. John Brillhart & J. L. Selfridge, "Some factorizations of $2^n + 1$ and related results," *Math. Comp.*, v. 21, 1967, pp. 87–96; Corrigendum, ibid., v. 21, 1967, p. 751. MR **37** #131.

5. Donald Knuth, "Seminumerical algorithms," in *The Art of Computer Programming*. Vol. 2, Addison-Wesley, Reading, Mass., 1969, pp. 351–354.