MATHEMATICS OF COMPUTATION, VOLUME 34, NUMBER 149
JANUARY 1980, PAGES 303–304

On the Primality of $k! + 1$ and $2 * 3 * 5 * \cdots * p + 1$

By Mark Templer

Abstract. In this paper the results of an investigation of $k! + 1$ and $2*3*5* \cdots *p + 1$ are reported. Values of $k = 1(1)230$ and $2 \leqslant p \leqslant 1031$ were investigated. Five new primes were discovered.

In this paper the results of an investigation of $k! + 1$ and $2*3*5* \cdots *p + 1$ are reported. A PDP-11/70 computer was used for all computations.

Numbers N of the above forms were first checked for small factors by trial division. Then they were tested for pseudoprimality by computing $a_1^{(N-1)/2} \pmod N$ for a base a_1 such that the Jacobi symbol $(a_1|N) = -1$. If $a_1^{(N-1)/2} \not\equiv -1 \pmod N$, then N is composite by Euler's criterion. If $a_1^{(N-1)/2} \equiv -1 \pmod N$, then it was proved prime by the following theorem developed by Brillhart, Lehmer, and Selfridge [1, p. 623].

THEOREM 1. *Let $N - 1 = \Pi\, p_i^{a_i} = F_1R_1$, where F_1 is the even factored portion of $N - 1$, $F_1 > R_1 \geqslant 1$, and $(F_1, R_1) = 1$. If for each p_i dividing F_1 there exists an a_i such that $a_i^{N-1} \equiv 1 \pmod N$, but $(a_i^{(N-1)/p_i} - 1, N) = 1$, then N is prime.*

The calculations were performed by calculating

$$(1) \quad a_i^{(N-1)/p_i} \equiv b_i \not\equiv 1 \pmod N,\ (N, b_i - 1) = 1, \quad \text{and then } b_i^{p_i} \equiv 1 \pmod N.$$

The base a_1 was used as long as (1) was satisfied, otherwise a new a_i was chosen until (1) was satisfied, at which point the original base a_1 was used for the next p_i (avoiding the computation of $b_i^{p_i} \pmod N$).

Theorem 1 was used in the program in favor of other theorems in [1] with slightly faster running speeds. This was due to the fact that Theorem 1 requires relatively little memory space. The processor time to compute (1) for $p_i = 2$ was roughly $(x^3/(\ln x)^2)*C$, where x is the number of bits in $(N - 1)/2$ and C is a constant. The time required to prove N prime was $(x^3/(\ln x)^2)*C*D/2$, where D is the number of distinct prime factors of $(N - 1)/2$.

This investigation confirmed all of Borning's [2] results for $k! + 1$ and $2*3*5* \cdots *p + 1$. It extended the upper limit on k from 100 to 230, and on p from 307 to 1031. The primes $k = 116$ and 154, and $p = 379$, 1019, and 1021 were discovered, with 191, 272, 154, 425, and 428 digits, respectively.

Received March 6, 1979.
AMS (MOS) subject classifications (1970). Primary 10A25; Secondary 10A10.
Key words and phrases. Pseudoprimality (psp), Euler's criterion.

Acknowledgements. The author is grateful to John Brillhart of the University of Arizona for his helpful suggestions. Also, he must express his gratitude for the immeasurable assistance given by Lloyd Mish of Arizona State University. Finally, the author thanks Sheldon Wion of the Tempe High School Mathematics Department for making computer time available for this investigation.

Values of k such that $k! + 1$ *is prime* $1 \leqslant k \leqslant 230$	*Values of p such that* $2*3*5* \cdots *p + 1$ *is prime* $2 \leqslant p \leqslant 1031$
k	p
1	2
2	3
3	5
11	7
27	11
37	31
41	379
73	1019
77	1021
116	
154	

345 Encanto Drive
Tempe, Arizona 85281

1. JOHN 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. ALAN BORNING, "Some results for $k! + 1$ and $2 \cdot 3 \cdot 5 \cdots p \pm 1$," *Math. Comp.*, v. 26, 1972, pp. 567–570.