The Compositeness Of The Thirteenth Fermat Number

By G. A. Paxson

Fermat numbers are numbers of the form \( F_n = 2^{2^n} + 1 \). As is well known, these numbers are prime for \( n = 0, 1, 2, 3, \) and 4. In fact, Fermat conjectured that they all were prime. Since then, however, factors of many \( F_n \) for \( n > 4 \) have been discovered [4]. In particular, factors are known for \( n = 5, 6, 9, 10, 11, 12, 15, 16, 18, 23, 36, 38, 39, 55, 58, 63, 73, 77, 81, 117, 125, 144, 150, 207, 226, 228, 250, 267, 268, 284, 316, 452, \) and 1945. On the other hand, Morehead and Western [1], [2] showed over fifty years ago that \( F_7 \) and \( F_8 \) are composite. Thus, \( F_{13} \) was the first number whose character was unknown, although [4] it has no factors less than \( 2^{36} \).

Since \( F_n \) is prime if and only if 
\[
3^{(F_n-1)/2} \equiv -1 \pmod{F_n},
\]
a program was written for the IBM 7090 to check this criterion and determine the character of \( F_{13} \). At the beginning of December 1960, the computation was made and the result shows that \( F_{13} \) is composite.

The computation required 6 hours 17 minutes of machine time, including time to punch a number of intermediate residues. The result was checked by a rerun on a different day and all residues were identical. Moreover, as a check on the program, Morehead’s result [1] for \( F_7 \), Morehead and Western’s result [2] for \( F_8 \), and Robinson’s result [3] for \( F_{10} \) were obtained.

The calculation to determine the character of \( F_{14} \) requires about \( 49\frac{1}{2} \) hours. This and the recalculation to check the result are each about half finished. However, lack of available machine time has temporarily suspended the computation.

When machine time does become available, in addition to finishing the computation for \( F_{14} \), a search will be made to insure that Robinson’s list [4] of factors \( p \) of Fermat numbers contains all \( p < 2^{36} \). At present it contains all \( p < 2^{32} \) and all \( p < 2^{36} \) for which \( p \equiv 1 \pmod{2^{16}} \). It should be noted that this last search could yield new factors only for \( 7 \leq n \leq 12 \) since all factors of \( F_n \) are of the form \( k \cdot 2^{n+2} + 1 \).

California Research Corporation
Richmond, California

4. R. M. Robinson, "A report on primes of the form \( k \cdot 2^n + 1 \) and on factors of Fermat numbers," ibid., v. 9, 1958, p. 673-681.

Received January 18, 1961; revised April 25, 1961.