MATHEMATICS OF COMPUTATION, VOLUME 25, NUMBER 115, JULY, 1971

On the Feit-Thompson Conjecture

By N. M. Stephens

Abstract. A counterexample is found to the conjecture that $(p^q - 1)/(p - 1)$ and $(q^p - 1)/(q - 1)$ are coprime where p, q are primes.

In [1], referring to their work on the solvability of groups of odd order, Feit and Thompson state "The validity of the conjecture that $(p^q - 1)/(p - 1)$ never divides $(q^p - 1)/(q - 1)$ if p, q are distinct primes would also simplify the proof, rendering unnecessary the detailed use of generators and relations." The truth of this conjecture is implied by the truth of the stronger conjecture that the two expressions are coprime. Though the latter conjecture is widely known, the author can find no explicit reference apart from [2] where the author considers the case $p = 3$. In this paper a counterexample is exhibited.

Let $A = (p^q - 1)/(p - 1)$ and $B = (q^p - 1)/(q - 1)$ where p and q are distinct primes, and suppose r is a prime dividing both A and B. If $p = 2$, it follows that $2^q - 1 \equiv q + 1 \equiv 0 \pmod{r}$, and hence that $q|(r - 1)$ and $r|(q + 1)$, which is impossible. Thus p and q must be odd.

If $r|(p - 1)$, then $A = 1 + p + \cdots + p^{q-1} \equiv q \pmod{r}$, and so $r = q$. But q does not divide B; thus $r \nmid (p - 1)$ and, similarly, $r \nmid (q - 1)$. Hence $p^q \equiv 1 \pmod{r}$, whence $q|(r - 1)$. It follows, therefore, that, for some integer λ,

$$r = 2\lambda pq + 1. \tag{1}$$

A program was written in Fortran and run on Atlas to test the residues of p^q and q^p modulo r for all odd primes p and q, $p \leqq 443$, $pq < 200000$, and for all r of the form given by (1) with $r < 400000$. The program took less than two minutes.

The results showed that, within these ranges, there is just one instance where $p^q \equiv q^p \equiv 1 \pmod{r}$, namely, for $p = 17$, $q = 3313$ and $r = 112643 = 2pq + 1$. Using his multilength package, Dr. F. Lunnon computed A and B for these values of p and q, and showed that r was indeed their highest common factor. The original conjecture remains, therefore, unresolved.

Atlas Computer Laboratory
Chilton, Berkshire, England

1. W. Feit & J. C. Thompson, "A solvability criterion for finite groups and some consequences," *Proc. Nat. Acad. Sci. U.S.A.*, v. 48, 1962, pp. 968–970. MR **26** #1352.
2. K. E. Kloss, "Some number-theoretic calculations," *J. Res. Nat. Bur. Standards Sect. B*, v. 69B, 1965, pp. 335–336. MR **32** #7473.

Received October 12, 1970.
AMS 1970 *subject classifications.* Primary 10A05, 10-04; Secondary 20D10.
Key words and phrases. Primes, counterexample.