MATHEMATICS OF COMPUTATION
VOLUME 36, NUMBER 153
JANUARY 1981

On Fermat's Quotient, Base Two

By D. H. Lehmer

Abstract. This paper extends the search for solutions of the congruence

$$2^{p-1} - 1 \equiv 0 \pmod{p^2}$$

to the limit $p < 6 \cdot 10^9$. No solution, except the well-known $p = 1093$ and $p = 3511$, was found.

In 1969 Brillhart, Tonascia, and Weinberger [1] reported on the search for solutions of the congruence

$$a^{p-1} \equiv 1 \pmod{p^2}, \qquad a = 2(1)199.$$

For $a = 2$, a special effort was made to consider all $p < 3 \cdot 10^9$. Only the two known solutions $p = 1093$ and $p = 3511$ were found. Having the occasional opportunity to use the Illiac IV, one of the projects decided upon was the recalculation and extension of the above result for $a = 2$ by a somewhat different method. The calculation was pushed to twice the above limit, that is to $p < 6 \cdot 10^9$, without finding any further solutions.

The parallel construction of the Illiac IV makes it possible to look for 64 different values of p at the same time. The speed of Illiac IV is such that a range of 100000 numbers can be searched in one second. Thus, the range for $p < 6 \cdot 10^9$ was broken up into 60 runs of 1000 seconds each. The program was run as one of a few backlog problems over the past two years.

Let n belong to one of the 64 residue classes that are prime to 240 and let

$$2^m \equiv A_m + nB_m \pmod{n^2},$$

where $0 < A_m < n$, $0 \leqslant B_m < n$.

For numbers n as large as 10^9, the number n^2 is a doubly precise integer. Nevertheless, the calculation of A_m and B_m can be accomplished by single precision arithmetic in only $O(\log m)$ operations. In fact, one uses one or the other of the following two recurrences:

If $m = 2h + 1$, then $A_m \equiv 2A_{2h}$ and $B_m \equiv 2B_{2h} \pmod{n}$.

If $m = 2h$, and if $A_h^2 = R_m + nQ_m$ $(0 < R_m < n)$
and if $2A_hB_h \equiv D_m \pmod{n}$,

then

$$A_m = R_m \quad \text{and} \quad B_m = Q_m + D_m.$$

Received March 30, 1980.
1980 *Mathematics Subject Classification*. Primary 10–04.

The arithmetic units of the Illiac IV are particularly well suited to carry out these recurrences.

In order to get some output it was decided to put out all values of n and A_{n-1} for which $B_{n-1} = 0$. For $n < 6 \cdot 10^9$ there are only nine such values of n. These are tabulated as follows:

n	factors of n	A_{n-1}
779	$19 \cdot 41$	605
1093	prime	1
3511	prime	1
7651	$7 \cdot 1093$	64
14207	$13 \cdot 1093$	4096
24577	$7 \cdot 3511$	64
38621	$11 \cdot 3511$	1024
226 55923	$19 \cdot 1192417$	9801480
14989 49323	$2341 \cdot 640303$	830355587

As a consequence of this project, the first case of Fermat's Last Theorem is now established for $p < 6 \cdot 10^9$ by Wieferich's Criterion [2].

The author acknowledges his indebtedness to the Institute for Advanced Computing (Sunnyvale, California) for allowing him free machine time for this project.

Department of Mathematics
University of California at Berkeley
Berkeley, California 94720

1. J. Brillhart, J. Tonascia & P. Weinberger, "On the Fermat quotient," *Computers in Number Theory*, Academic Press, London and New York, 1971, pp. 213–222.

2. A. Wieferich, "Zum letzen Fermatschen Theorem," *J. für Math.*, v. 136, 1909, pp. 293–302.