PACIFIC JOURNAL OF MATHEMATICS
Vol. 22, No. 3, 1967

ON THE SQUARE-FREENESS OF FERMAT AND MERSENNE NUMBERS

LE ROY J. WARREN AND HENRY G. BRAY

It has been conjectured that the Fermat and Mersenne numbers are all square-free. In this note it is shown that if some Fermat or Mersenne number fails to be square-free, then for any prime p whose square divides the appropriate number, it must be that $2^{p-1} \equiv 1 \pmod{p^2}$. At present there are only two primes known which satisfy the above congruence. It is shown that neither of these two primes is a factor of any Fermat or Mersenne number.

Those odd primes p for which $2^{p-1} \equiv 1 \pmod{p^2}$ have long been of interest. No doubt much of this interest has been generated by Wieferich's theorem, which states that if Fermat's equation $x^p + y^p + z^p = 0$ has a solution in integers with p an odd prime and $xyz \not\equiv 0 \pmod{p}$, then $2^{p-1} \equiv 1 \pmod{p^2}$.

Throughout, "p" and "q" will denote odd primes; "n" is a positive integer other than 1; "$2Rp$" indicates that 2 is a quadratic residue modulo p; "$o(2, p)$" is the exponent to which 2 belongs modulo p; and $F_n = 2^{2^n} + 1$ and $M_q = 2^q - 1$.

Our result follows immediately from the following theorem which proves a bit more than has been indicated so far.

THEOREM 1. *If p divides some F_n [some M_q], then $2^{(p-1)/2} \equiv 1 \pmod{F_n}$ [$2^{(p-1)/2} \equiv 1 \pmod{M_q}$].*

Proof. Let $p \mid F_n$, then $2^{2^n} \equiv -1 \pmod{p}$ and $2^{2^{n+1}} \equiv 1 \pmod{p}$ so that $o(2, p) \mid 2^{n+1}$ and $o(2, p) \nmid 2^n$. It follows that $o(2, p) = 2^{n+1}$. Now $2^{p-1} \equiv 1 \pmod{p}$ which implies that $2^{n+1} \mid (p-1)$ and

$$p \equiv 1 \pmod{8}\,. \tag{1}$$

Hence $2Rp$ and by Euler's criterion $2^{(p-1)/2} \equiv 1 \pmod{p}$ so that $2^{n+1} \mid ((p-1)/2)$. It follows that $(2^{2^{n+1}} - 1) \mid (2^{(p-1)/2} - 1)$. Clearly $F_n \mid (2^{2^{n+1}} - 1)$, and therefore $F_n \mid (2^{(p-1)/2} - 1)$.

Let $p \mid M_q$, then $2^q \equiv 1 \pmod{p}$ and $2^{q+1} \equiv 2 \pmod{p}$. Since $q + 1$ is even, we obtain that $2Rp$ and therefore

$$p \equiv \pm 1 \pmod{8}\,. \tag{2}$$

Also $o(2, p) \mid q$ so that $o(2, p) = q$. As before we get that

$$q \,\Big|\, \frac{p-1}{2} \tag{3}$$

so that $M_q \mid (2^{(p-1)/2} - 1)$ to complete the proof.

The two known primes p for which $2^{p-1} \equiv 1 \pmod{p^2}$ are 1093 and 3511.

THEOREM 2. *Neither* 1093 *nor* 3511 *divides any* F_n *or any* M_q.

Proof. We have $1093 \equiv 5 \pmod 8$ so by (1) and (2) of Theorem 1, it follows that 1093 cannot divide any F_n or any M_q.

Now $3511 \equiv -1 \pmod 8$, it then follows from (1) of Theorem 1 that 3511 cannot divide any F_n. Suppose that for some q, $3511 \mid M_q$; then by (3) of Theorem 1, $q \mid ((3511 - 1)/2)$. This means that q must be one of the three primes 3, 5, or 13. By direct computation 3511 does not divide M_3, M_5 or M_{13}.

Recevied October 10, 1966.

SAN DIEGO STATE COLLEGE
SAN DIEGO, CALIFORNIA