

Pacific Journal of Mathematics

ON THE SQUARE-FREENESS OF FERMAT AND MERSENNE NUMBERS

LEROY J. WARREN AND HENRY GILBERT BRAY

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

$$(1) \quad p \equiv 1 \pmod{8}.$$

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

$$(2) \quad p \equiv \pm 1 \pmod{8}.$$

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

$$(3) \quad q \mid \frac{p-1}{2}$$

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} .

Received October 10, 1966.

SAN DIEGO STATE COLLEGE
SAN DIEGO, CALIFORNIA

PACIFIC JOURNAL OF MATHEMATICS

EDITORS

H. SAMELSON

Stanford University
Stanford, California

J. P. JANS

University of Washington
Seattle, Washington 98105

J. DUGUNDJI

University of Southern California
Los Angeles, California 90007

RICHARD ARENS

University of California
Los Angeles, California 90024

ASSOCIATE EDITORS

E. F. BECKENBACH

B. H. NEUMANN

F. WOLF

K. YOSIDA

SUPPORTING INSTITUTIONS

UNIVERSITY OF BRITISH COLUMBIA
CALIFORNIA INSTITUTE OF TECHNOLOGY
UNIVERSITY OF CALIFORNIA
MONTANA STATE UNIVERSITY
UNIVERSITY OF NEVADA
NEW MEXICO STATE UNIVERSITY
OREGON STATE UNIVERSITY
UNIVERSITY OF OREGON
OSAKA UNIVERSITY
UNIVERSITY OF SOUTHERN CALIFORNIA

STANFORD UNIVERSITY
UNIVERSITY OF TOKYO
UNIVERSITY OF UTAH
WASHINGTON STATE UNIVERSITY
UNIVERSITY OF WASHINGTON
* * *
AMERICAN MATHEMATICAL SOCIETY
CHEVRON RESEARCH CORPORATION
TRW SYSTEMS
NAVAL ORDNANCE TEST STATION

Mathematical papers intended for publication in the *Pacific Journal of Mathematics* should be typewritten (double spaced). The first paragraph or two must be capable of being used separately as a synopsis of the entire paper. It should not contain references to the bibliography. Manuscripts may be sent to any one of the four editors. All other communications to the editors should be addressed to the managing editor, Richard Arens at the University of California, Los Angeles, California 90024.

50 reprints per author of each article are furnished free of charge; additional copies may be obtained at cost in multiples of 50.

The *Pacific Journal of Mathematics* is published monthly. Effective with Volume 16 the price per volume (3 numbers) is \$ 8.00; single issues, \$ 3.00. Special price for current issues to individual faculty members of supporting institutions and to individual members of the American Mathematical Society: \$ 4.00 per volume; single issues \$ 1.50. Back numbers are available.

Subscriptions, orders for back numbers, and changes of address should be sent to Pacific Journal of Mathematics, 103 Highland Boulevard, Berkeley 8, California.

Printed at Kokusai Bunken Insatsusha (International Academic Printing Co., Ltd.), 7-17, Fujimi 2-chome, Chiyoda-ku, Tokyo, Japan.

PUBLISHED BY PACIFIC JOURNAL OF MATHEMATICS, A NON-PROFIT CORPORATION

The Supporting Institutions listed above contribute to the cost of publication of this Journal, but they are not owners or publishers and have no responsibility for its content or policies.

Wai-Mee Ching and James Sai-Wing Wong, <i>Multipliers and H^* algebras</i>	387
P. H. Doyle, III and John Gilbert Hocking, <i>A generalization of the Wilder arcs</i>	397
Irving Leonard Glicksberg, <i>A Phragmén-Lindelöf theorem for function algebras</i>	401
E. M. Horadam, <i>A sum of a certain divisor function for arithmetical semi-groups</i>	407
V. Istrăţescu, <i>On some hyponormal operators</i>	413
Harold H. Johnson, <i>The non-invariance of hyperbolicity in partial differential equations</i>	419
Daniel Paul Maki, <i>On constructing distribution functions: A bounded denumerable spectrum with n limit points</i>	431
Ronald John Nunke, <i>On the structure of Tor. II</i>	453
T. V. Panchapagesan, <i>Unitary operators in Banach spaces</i>	465
Gerald H. Ryder, <i>Boundary value problems for a class of nonlinear differential equations</i>	477
Stephen Simons, <i>The iterated limit condition and sequential convergence</i>	505
Larry Eugene Snyder, <i>Stolz angle convergence in metric spaces</i>	515
Sherman K. Stein, <i>Factoring by subsets</i>	523
Ponnaluri Suryanarayana, <i>The higher order differentiability of solutions of abstract evolution equations</i>	543
Leroy J. Warren and Henry Gilbert Bray, <i>On the square-freeness of Fermat and Mersenne numbers</i>	563
Tudor Zamfirescu, <i>On l-simplicial convexity in vector spaces</i>	565
Eduardo H. Zarantonello, <i>The closure of the numerical range contains the spectrum</i>	575