Reprinted from the AMERICAN MATHEMATICAL MONTHLY
Vol. LVI, No. 9, November, 1949

ON THE CONVERSE OF FERMAT'S THEOREM

P. ERDÖS, University of Illinois

Following Lehmer we shall call an integer n a *pseudoprime* if $2^n \equiv 2 \pmod{n}$ and n is not a prime. The smallest pseudoprime is $341 = 11.31$. Recently Sierpinski[1] gave a very simple proof that there are infinitely many pseudoprimes, by proving that if n is a pseudoprime then $2^n - 1$ is also a pseudoprime. Lehmer[2] proved that there exist infinitely many pseudoprimes n with $v(n) = 3$, where $v(n)$ denotes the number of different prime factors of n. In the present note we prove the following theorem.

THEOREM. *For every k there exist infinitely many squarefree pseudoprimes with $v(n) = k$.*

First we repeat Lehmer's proof[3] that there are infinitely many pseudoprimes n with $v(n) = 2$. It is well known[4] that for every $m > 6$ both $2^m - 1$ and $2^m + 1$ have a primitive prime factor; that is, there exist primes p and q such that

$$2^m - 1 \equiv 0 \pmod{p}, \qquad 2^l - 1 \not\equiv 0 \pmod{p}, \qquad \text{for } 1 \leqq l < m;$$
$$2^m + 1 \equiv 0 \pmod{q}, \qquad 2^l + 1 \not\equiv 0 \pmod{q} \qquad \text{for } 1 \leqq l < m.$$

It is easy to see that $p \cdot q$ is a pseudoprime. In fact we have $p \equiv q \equiv 1 \pmod{2m}$, $2^{2m} \equiv 1 \pmod{p \cdot q}$, thus

$$2^{pq-1} \equiv 2^{(p-1)(q-1)} \cdot 2^{p-1} \cdot 2^{q-1} \equiv 1 \pmod{pq}.$$

Also it is immediate that to different values of m correspond different values of $p \cdot q$, which proves the theorem for $k = 2$.

The proof of the general case will be very similar to that of Lehmer. We use induction on k. Let $n_1 < n_2 < \cdots$ be an infinite sequence of pseudoprimes with $v(n_i) = k - 1$. Let p_i be one of the primitive prime factors of $2^{n_i-1} - 1$. We claim that $p_i \cdot n_i$ is a pseudoprime. In fact, by definition, $2^{n_i-1} \equiv 1 \pmod{p_i \cdot n_i}$, also $2^{p_i-1} \equiv 1 \pmod{p_i}$. Further, since $p_i - 1 \equiv 0 \pmod{(n_i - 1)}$, we have $2^{p_i-1} \equiv 1 \pmod{n_i}$ and finally $2^{n_i-1} \equiv 1 \pmod{n_i}$. Thus

[1] Colloquium Math., vol. 1 (1947), p. 9.

[2] This MONTHLY, vol. 56 (1949) p. 306.

[3] This MONTHLY, vol. 43 (1936), pp. 347–356.

[4] Bang, Tiddsskrift for Mat. 1886, pp. 130–137. See Also Birkhoff-Vandiver, Annals of Math., 1904.

$$2^{n_ip_i-1} = 2^{(n_i-1)(p_i-1)} \cdot 2^{n_i-1} \cdot 2^{p_i-1} \equiv 1 \pmod{p_in_i}.$$

Also $p_i > n_i$, since $p_i \equiv 1 \pmod{(n_i-1)}$ and n_i is not a prime. Thus $p_i \cdot n_i$ is squarefree, and $v(p_i \cdot n_i) = k$, and all the integers $p_i \cdot n_i$ are different; this completes the proof of the theorem.

Following Lehmer we call n an absolute pseudoprime if $a^n \equiv a \pmod{n}$ for every a prime to n. The smallest absolute pseudoprime is 561. It seems very difficult to determine whether there are infinitely many absolute pseudoprimes. A similar question is whether there exist any composite numbers n with $n-1 \equiv 0 \pmod{\phi(n)}$.

Two further questions are: Are there integers n so that 2^n-1 has more than k primitive prime factors? Are there infinitely many primes p for which 2^p-1 is composite? The smallest such prime is 11.

Denote by $f(x)$ the number of pseudoprimes not exceeding c. I can prove that

$$c_1 \cdot \log x < f(x) < c_2 \frac{x}{(\log x)^k}, \tag{1}$$

for every k if x is sufficiently large. In other words, the number of pseudoprimes is considerably smaller than the number of primes. The proof of (1) (second inequality) is complicated and we do not discuss it here.