ON FERMAT'S SIMPLE THEOREM

JACK CHERNICK

1. **Introduction.** Fermat's simple theorem may be stated as follows: *If a is any integer prime to m, and if m is prime, then*

$$a^{m-1} \equiv 1 \pmod{m}. \tag{1}$$

The question naturally arises, "Do there exist composite integers for which the same congruence holds?" For particular values of a the existence of such numbers has long been established.* In 1910, R. D. Carmichael† treated the congruence (1) in the stricter sense indicated. He established several criteria which may be condensed into the following theorem:

THEOREM 1. *Fermat's theorem holds for composite integers if and only if m may be expressed as a product of distinct odd primes $p_1, \cdots, p_n$, $(n>2)$, and $m-1 \equiv 0 \pmod{p_i - 1}$ where i ranges from* 1 *to n.*

Carmichael listed several such m with $n=3$ and one with $n=4$. Many others have since been found by P. Poulet.‡ It is our purpose to continue the study of these numbers in the present paper.

Fermat's theorem is sometimes stated thus: *If m is any prime and a any integer, then*

$$a^{m} \equiv a \pmod{m}. \tag{2}$$

The congruences (1) and (2) are likewise equivalent if m is composite, as is easily shown by the use of Theorem 1.

Despite the apparent promise of Fermat's theorem of yielding a complete and practical test for primes, no modification of it has as yet achieved this goal. However, the recent work of D. H. Lehmer,§ based upon a list of solutions of (2) for $a=2$, now provides such a test for integers in the range 10^7 to 10^8.

2. **Proof of Theorem** 1. We present a short, independent proof of Theorem 1. Let m be a composite number for which (1) holds. First, suppose $m=2^v$, $(v>1)$. But $a^{2^v-1} \equiv 1 \pmod{2^v}$ will not hold for

* Dickson, *History of the Theory of Numbers*, vol. 1, pp. 92–95.

† This Bulletin, vol. 16 (1910), pp. 232–238; also American Mathematical Monthly, vol. 19 (1912), pp. 22–27.

‡ D. H. Lehmer informs us that all m's under $5 \cdot 10^7$ and all, with $n=3$, under 10^8 have been tabulated by Poulet.

§ American Mathematical Monthly, vol. 43 (1936), pp. 347–354.