A FURTHER NOTE ON THE CONVERSE OF FERMAT'S THEOREM

BY D. H. LEHMER

In a previous paper* the writer had discussed the converse of Fermat's theorem as a means of establishing the primality or non-primality of a large integer. Use was made chiefly of the following theorem:

THEOREM 3. *If* $a^x \equiv 1 \pmod{N}$ *for* $x = N-1$ *and if* $a^x \equiv r \not\equiv 1$ *for* $x = (N-1)/p$ *and if* $r-1$ *is prime to* N, *then all the factors of* N *belong to the form* $np^\alpha + 1$ *where* α *is the highest power of the prime* p *contained in* $N-1$.

It is the purpose of this note to give a more general theorem in which the third part of the hypothesis of Theorem 3 is removed.

THEOREM 4. *If* $a^x \equiv 1 \pmod{N}$ *for* $x = N-1$ *and* $a^x \equiv r \not\equiv 1$ *for* $x = (N-1)/p$, *then all the factors of* N/δ *are of the form* $np^\alpha + 1$, *where* α *is the highest power of the prime* p *contained in* $N-1$ *and where* δ *is the G.C.D. of* $r-1$ *and* N.

Let k be a prime factor of N/δ and let ω be the exponent to which a belongs modulo k. Then ω divides $N-1$ and $k-1$ but not $m = (N-1)/p$; for if ω divided m we would have $a^m \equiv 1 \pmod{k}$ so that $r-1$ would divide by k. But this is impossible, since k divides N/δ which is prime to $r-1$. From here on, the proof is the same as in Theorem 3 with the result that $k = np^\alpha + 1$.

Ordinarily, we have $\delta = 1$ so that the two theorems become identical. An example in which this is not the case is the following: Let $N = 16{,}046{,}641$. $N-1 = 2^4 \times 3^3 \times 5 \times 17 \times 19 \times 23$. It will be found that

* This Bulletin, vol. 33 (1927), pp. 327–340.