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.

$$2^{N-1} \equiv 1 \pmod{N},$$
$$2^{(N-1)/19} = 8708025 = r.$$

If we take the G.C.D. of $r-1$ and N, we get $\delta = 35113$, so that $N/\delta = 457$ and we are able to say that the factors of 457 are of the form $19n+1$. The factors of δ may be obtained by applying Theorem 4 in which a new value of m is chosen. The modulus may be taken as δ.

Theorem 4 has been applied to the number

$$N = (2^{61} + 1)/3 = 768614336404564651.$$

This number has been listed as a prime but the writer could not find any account of its investigation.*

The factorization of $N-1$ is

$$N - 1 = 2(2^{60}-1)/3 = 2 \cdot 3 \cdot 5^2 \cdot 7 \cdot 11 \cdot 13 \cdot 31 \cdot 41 \cdot 61 \cdot 151 \cdot 331 \cdot 1321.$$

It was found that

$$3^{(N-1)/5} \equiv 754529885435533861 = r_1,$$
$$3^{(N-1)/3} \equiv 243065045915817725 = r_2,$$
$$3^{N-1} \equiv 1. \pmod{N}.$$

It happens that r_1-1 and r_2-1 are both prime to N. Hence the factors of N belong to the forms

$$\left.\begin{matrix} 3n+1 \\ 25n+1 \\ 61n+1 \end{matrix}\right\} 4575n+1.$$

By making use of the fact that N has no factor $<300{,}000$ and by seeking to represent N as the difference of two squares it was easily shown to be a prime.

Two more numbers dividing $10^n \pm 1$ have also been tested recently. The first of these is $(10^{37}-1)/9$ or

$$N = 1{,}111{,}111{,}111{,}111{,}111{,}111{,}111{,}111{,}111{,}111{,}111.$$

* Cunningham and Woodall, *Factorisation of* $y^n \pm 1$, London, 1925, p. 1.

It was found that

$$7^{N-1} \equiv 618,117,398,624,349,204,361,513,620,865,505,749 \pmod{N}.$$

Hence N is composite. This number furnishes another example of the scarcity of primes of this form. The next such number which has any chance of primality consists of 47 of the digits 1.

The second number tested is $(10^{41}+1)/11$ or

$$N = 9,090,909,090,909,090,909,090,909,090,909,090,909,091.$$

In this case it was found that

$$3^{N-1} \equiv 763,287,007,500,473,474,161,903,784,495,157,879,509 \pmod{N}.$$

It follows, then, that N is also composite. This result represents the sixth attempt and failure to discover a larger prime than $2^{127}-1$ found by Lucas in 1877.

THE UNIVERSITY OF CALIFORNIA

ON THE APPROXIMATE REPRESENTATION OF ANALYTIC FUNCTIONS*

BY DUNHAM JACKSON

The purpose of this paper is to discuss the convergence of approximating polynomials determined by a least-square criterion, together with certain auxiliary conditions. Let $f(x)$ be a given function over the interval $a \leqq x \leqq b$. For each positive integral value of n, let p_n be a positive integer $\leqq n$. A polynomial of the nth degree may be required, for example, to coincide in value with $f(x)$ at p_n specified points of the interval; and among the infinitely many polynomials of the

* Presented to the Society, September 8, 1927.