If p occurs in the set (12), $p-8$ is not in it except for $p=232, 240, 472, 480$. For these four, $p-8\cdot 2^4$ is not in the set (12). This proves Theorem 4.

9. Corresponding results for cubes are obtained in the writer's paper in the American Mathematical Monthly for April, 1927. Assistance has been provided by the Carnegie Institution for the more elaborate investigation of fifth and higher powers.

THE UNIVERSITY OF CHICAGO

TESTS FOR PRIMALITY BY THE CONVERSE OF FERMAT'S THEOREM*

BY D. H. LEHMER

There are, generally speaking, two distinct methods for determining the primality of a large integer without trying possible divisors. Up to this time the method which goes by the name of Lucas' test† has yielded the most results. It is particularly well adapted to the investigation of Mersenne numbers and has consequently led to the identification of the three largest primes heretofore known, namely, $2^{89}-1$, $2^{107}-1$ and $2^{127}-1$. The other method is based on the converse of Fermat's theorem. It is the purpose of this paper to discuss certain improvements in this method, and to apply it to some numbers of the form $10^n \pm 1$.

It has long been known that the simple converse of Fermat's theorem, namely: *If* $a^x \equiv 1 \pmod N$ *for* $x=N-1$, *then* N *is a prime*, is *not* true, as is shown by the simple example: $4^{14} \equiv 1 \pmod{15}$. A true converse of this theorem was first given by Lucas‡ in 1876: *If* $a^x \equiv 1 \pmod N$ *for* $x=N-1$, *but not for* $x<N-1$, *then* N *is a prime.* In 1891 he proved the following theorem.§

---

* Presented to the Society, San Francisco Section, April 2, 1927.

† American Journal, vol. 1 (1878), pp. 184–220.

‡ Lucas, loc. cit., p. 302.

§ *Théorie des Nombres*, 1891, pp. 423, 441.