NOTE ON MERSENNE NUMBERS*

BY D. H. LEHMER†

The purpose of this note is to report the results of two investigations which show that $2^{149}-1$ and $2^{257}-1$ are composite numbers. The former result agrees with the statement of Mersenne‡ in 1644, while the latter contradicts it. The method is based on the following test§ for primality.

THEOREM. *The number 2^n-1 is prime or composite according as it does or does not divide the $(n-1)$st term of the sequence*

$$(1) \qquad s_1=4,\ s_2=14,\ s_3=194,\ s_4=37634,\ s_5=1416317954,\ \cdots,$$

in which $s_{k+1}=s_k^2-2$.

Inasmuch as the series (1) increases very rapidly, it is necessary to suppress multiples of 2^n-1 as often as they arise. That is, the series (1) is taken with respect to the modulus 2^n-1.

The test for $2^{149}-1$ required about 70 hours. It was found that s_{148} when divided by $2^{149}-1$ leaves the remainder

267073170 876646890 164052223 831706652 997781887.

The whole work was recomputed with respect to the moduli 10^9+1 and 10^8+1 in order to check its accuracy. A copy of the calculation has been deposited in the library of the American Mathematical Society, and is available to anyone wishing to verify the work.

The number $2^{257}-1$ was tested by M. Kraïtchik|| in 1922. It was found that s_{257} was not divisible by $2^{257}-1$. He was unwilling to guarantee the accuracy of his result however. In order to settle the question about the character of this largest Mersenne number, the writer made the same calculation and found that s_{256} when divided by $2^{257}-1$ leaves the remainder

* Presented to the Society, April 2, 1927.

† National Research Fellow.

‡ See for example Dickson's *History of the Theory of Numbers*, vol. 1, Chap. 1.

§ The proof of the sufficiency of this test for the case in which $n=4k+1$ was given by Lucas, American Journal of Mathematics vol. 1 (1877), p. 316. For the proof of the whole theorem see Annals of Mathematics, vol. 31, pp. 419–448.

|| Kraïtchik, *Théorie des Nombres*, vol. 2, p. 142.