[1] Kryloff, N., and Bogoliuboff, N.; *Introduction á la Mécanique non linéaire*, Kieff, 1937; also free English translation by S. Lefschetz, Princeton University Press, 1943.

[2] Poincaré, H., "Sur l'équilibre d'une masse fluide," *Acta Mathematica*, Vol. 7; *Figures d'équilibre d'une masse fluide*, Paris, 1903. Liapounoff, A., Problème général de la stabilité du mouvement. *Ann. de la Fac, d. Sc. de Toulouse*, **9**, 203 (1907). Andronow, A., and Chaikin, S., *Theory of Oscillations*, Moscow, 1937.

FIRST PROOF THAT THE MERSENNE NUMBER M_{157} IS COMPOSITE

By H. S. Uhler

Sloane Physics Laboratory, Yale University

Communicated September 9, 1944

The form of a Mersenne number is $M_p = 2^p - 1$ where p is prime. Just three hundred years ago Mersenne published, in effect, the statement that the only values of p not greater than 257 which make M_p prime are 2, 3, 5, 7, 13, 17, 19, 31, 67, 127 and 257. The prime or composite character of all of the 55 numbers included under this conjecture, except the six corresponding, respectively, to p = 157, 167, 193, 199, 227 and 229, had been investigated prior to the year 1935. Contrary to Mersenne's surmise it was found that for p = 67 and 257 M_p is composite, and that M_p is prime for p = 61, 89 and 107. The data presented above have been derived from a comprehensive paper by R. C. Archibald.[1]

The present contribution marks the first fruits of a friendly suggestion made last year by Professor Archibald and seconded by Professor D. H. Lehmer that the author turn his attention to problems of factorization in general, beginning with the special problem of the character of the six heretofore uninvestigated Mersenne numbers.

The modern technique of this problem is based explicitly upon the following theorem, discovered by E. Lucas and clarified by D. H. Lehmer,[2] namely: "*The number $N = 2^n - 1$, where n is an odd prime, is a prime if, and only if, N divides the $(n - 1)$-st term of the series,*

$$S_1 = 4, \qquad S_2 = 14, \qquad S_3 = 194, \ldots, S_k, \ldots,$$

where $S_k = S_{k-1}^2 - 2$."

Since the number M_{157}, which is the subject of the present study, equals 182 68770 46663 62864 77546 06040 89535 37745 69915 67871 and since the above theorem requires that this 48-digit number be used as a divisor 149 times (8 to 156, inclusive) it should be obvious that the prospective investigator would focus attention upon this aspect of the computation. The procedure followed by R. E. Powers[3] in showing that M_{241} is composite appealed at first to the author and hence it was used as far as the 34th member of the Lucasian sequence. At this stage Powers' technique was abandoned because it had proved to involve an inordinate amount of writing and mental arithmetic and especially because it did not make use of a computing machine exclusively.

The patent idea of substituting for division multiplication by the reciprocal of the divisor overcame all of the objections entertained by the writer against all of the schemes for direct machine-division which he had read in the literature. Consider $s_k' = N \cdot q_k + r_k$. Then $(1/N) \cdot s_k' = q_k + r_k/N$. Hence if we multiply any term ($>N$) of a congruently equivalent Lucasian sequence by $1/N$ the succession of figures to the left of the decimal point will represent the integer q_k, while the digits to the right of the decimal point will constitute an approximation to the incommensurable decimal fraction r_k/N. Theoretically r_k may be obtained by multiplying r_k/N by N without evaluating a single q_k at any stage of the work. This procedure was not followed because it involves a greater number of figures than the alternative process of multiplying q_k by N and then subtracting $N \cdot q_k$ from s_k', that is, defining r_k as $s_k' - N \cdot q_k$.

The following details of the actual computation should make the matter perfectly clear. Ribbon A of cross-ruled paper has transcribed in nonads along the lower edge a sufficient number of figures of the reciprocal of $N(M_{157})$ thus: $1/N = 0 \cdot$(47 zeros) 547382212 626881668 329581868 472623488 781352321 048510246 $\cdots$. Similarly the bottom line of ribbon B reads: $N =$ 182687704 666362864 775460604 089535377 456991567 871.000000. Ribbons A and B do not have to be changed throughout the work from $k = 8$ to $k = 156$. On the other hand, each value of k requires three ribbons of its own. Along the top line of a longer ribbon of cross-ruled paper is written, for example, the value of r_{155} as 744260418 487541370 275270351 147668949 680082908 44.0000000. This number was machine-squared by D. N. Lehmer's[4] algorithm and recorded along the lowest line of the same ribbon. After subtracting 2 this line read $s_{156}' =$ 553923570 527250212 304427560 946230012 742643893 708358589 871125964 130378182 986908821 472209423 2334. The undiminished squared number was carefully checked with the moduli $10^3 + 1$, $10^4 + 1$ and $10^7 + 1$. Next ribbon A was laid on the longer ribbon so that the nonads of $1/N$ were juxtaposed above and in exact register with the first six nonads of s_{156}'. The multiplication of s_{156}' by $1/N$ was then effected and the resulting value of the integer q_{156} presented itself on the bottom line of a fourth strip of paper. This short act of multiplying was always repeated as a preliminary check on its accuracy. Actually $q_{156} =$ 303207909 661388759 507868593 612664030 922503212 07. Finally ribbon B was aligned with the nonads of q_{156} and a portion of the product $N \cdot q_{156}$ was recorded on the second line from the bottom of a fifth strip of cross-ruled paper. This multiplication was performed only on the nonads from the fifth to the eleventh, inclusive, since the first four sums-of-products would have reproduced a part of s_{156}' and not of r_{156}. (All of the nonads after the sixth were composed entirely of supplied zeros both for N and q_{156}.) The last figures of s_{156}' were copied on the third line from the bottom of the fifth strip so that by forming the difference between the second and third lines the required value of r_{156} came out on the bottom line. This remainder was found on Aug. 11, 1944, to be 118 57508 80382 71696 98184 73569 85091 23773 18030 92037. Since this residue is not zero it follows that M_{157} is composite and incidentally that M_{127} still retains the position of being the largest known prime number. For every value of k from 8 to 156 the numbers on the three corresponding strips were found to satisfy the relation $s_k' = N \cdot q_k + r_k$ for each of the moduli $10^3 + 1$, $10^4 + 1$ and $10^7 + 1$. The author desires to announce that he has already begun to investigate M_{167}.

[1] Archibald, R. C., *Scripta Mathematica*, **3**, 112–119 (1935).

[2] Lehmer, D. H., *Jour. London Math. Soc.*, **9–10**, 162–165 (1934–1935).

[3] Powers, R. E., *Bull. Amer. Math. Soc.*, **40**, 883 (1934).

[4] Lehmer, D. N., *Amer. Math. Monthly*, **30**, 67, 68 (1923).

---

*ON THE STABILITY OF TWO-DIMENSIONAL PARALLEL FLOWS**

BY C. C. LIN

GUGGENHEIM LABORATORY, CALIFORNIA INSTITUTE OF TECHNOLOGY

Communicated August 24, 1944

1. *Introduction.*—Heisenberg's[1] remarkable contribution to the hydrodynamic stability of two-dimensional parallel flows has not been favorably accepted and properly appreciated, because his paper is not completely free from obscure points. Nor has the work of Tietjens,[2] Tollmien[3] and Schlichting[4] been properly estimated. As a result, the theory to account for the instability of laminar flow at high Reynolds numbers has become very confused, and its further development has been very much retarded. Various authors suggest that it is necessary (1) to consider disturbances of finite amplitudes, (2) to include the effect of compressibility or even (3) to modify the Navier-Stokes equations. The present situation of our knowledge may be seen from the general lectures given by G. I. Taylor[5] and J. L. Synge.[6]

Recently the present writer carried out some investigations in an attempt to clarify the situation. The theory of Heisenberg was critically examined, somewhat modified and further developed. These developments were made with particular emphasis on the general criteria of instability