

MECHANICAL DEVICE FOR TESTING MERSENNE NUMBERS FOR PRIMES.

THOS. E. MASON.

Lucas,* in a note in "Récréations Mathématiques," gives a method of testing numbers of the form $2^{4q+3}-1$ for primes. The purpose of this note is to show how the labor of that method can be shortened, and how a machine could be constructed which would do most of the labor. If such a machine were constructed the labor of verifying the Mersenne numbers would be reduced to hours where it now requires weeks and months, for example, for numbers like $2^{127}-1$.

Lucas makes use of the following theorem: In order that the number $p=2^{4q+3}-1$ shall be prime, it is necessary and sufficient that the congruence

$$\sqrt{-1} \equiv 2 \cos \frac{\pi}{2^{4q+2}}, \pmod{p},$$

shall be satisfied, that is, that

$$\sqrt{-1} \equiv \sqrt{2 - \sqrt{2 + \sqrt{2 + \sqrt{2 + \dots}}}}, \pmod{p},$$

shall be verified after the successive removal of the radical. In other words, if we form the set of numbers V_n ,

$$V_0=1, V_1=3, V_2=7, V_3=47, V_4=2207, \dots,$$

such that each after the second is the square of the preceding diminished by 2 units, and then consider only the residues, modulo p , if the residue of the number V_n , where $n=4q+2$, is zero the number p is prime.

The process of Lucas makes use of the binary system of numeration. In this system multiplication consists simply in the longitudinal displacement of the multiplicand. It is evident also that the residue of the division of 2^m by 2^n-1 is equal to 2^r , r designating the residue of the division of m by n ; consequently, in trying 2^7-1 , it is sufficient to operate upon numbers having at most 7 of the figures 0 or 1. Figure I gives the calculation of V_4 deduced from the calculation of V_3 by the formula

$$V_4 = V_3^2 - 2 \pmod{2^7 - 1};$$

the dark squares represent the units of different orders of the binary system

*Lucas, Récréations Mathématiques, Vol. 2, pp. 230-235.

and the white squares the zeros. The first line is the residue of V_3 ; the 7 lines numbered 0 to 6 represent the residues (mod 2^7-1) of the partial products in

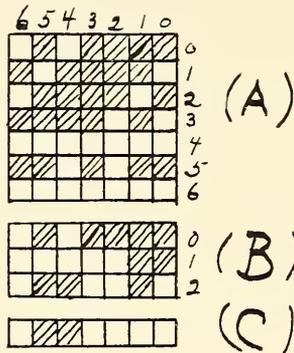


FIG. 1.

squaring V_3 ; the lines below, numbered 0 and 1 represent the addition of the partial products above and reduction modulo 2^7-1 , and line 2 represents the addition of 0 and 1; the single line below gives the residue of the square of V_3 with 2 subtracted, which is the residue of V_4 . In order to complete the test of 2^7-1 it is necessary to find V_6 . If the residue of V_6 is zero, then 2^7-1 is prime. This briefly is the plan as given by Lucas except that he used a different illustrative example.

In order to test a large number, say $2^{127}-1$, it would be necessary to make 126 of these square tables such as Figure I, each having 127^2 small squares. This would entail considerable labor and require a great deal of time. A simple device will reduce the labor of writing each line in the large square (A) to counting. Let us set down the work of squaring a number written in the binary system, for example, 13, which in the binary system is 1101.

$$\begin{array}{r}
 \hline
 1011 \qquad (S) \\
 \hline
 1101 \\
 1101 \\
 \hline
 1101 \\
 1101 \\
 1101 \\
 \hline
 10101001
 \end{array}$$

Now, if we write the number with the digits in reverse order on a slip of paper (S) and place it above the number itself as shown above, we see that the digits which occur in the third column of the partial products are the digits which come together, or correspond, when the slip of paper (S) is placed so that the first digit of the number, when digits are reversed, is placed over the third column. This is possible in no other scale, because the product of two digits in the binary scale does not give a number of more than one place. We can give the following rule for squaring a number written in the binary scale:

Write the number with the digits equally spaced and write the same number with the digits reversed on a slip of paper, using the same spacing. Place the slip of paper above the number so that the first digit in the reversed order comes above the last digit of the number. Move the slip of paper a single space to the left each time. Count the correspondences at each step. The number of correspondences at each step is the number which belongs in that place in the result which is immediately beneath the first digit on the slip. Continue this until there are no more correspondences.

It is easily seen that by means of the above rule the process described by Lucas can be followed out by counting the correspondences and will lead to the result in the lines marked (B) in Figure I, without having to write the part (A).

It would be possible to construct a machine which would have two parallel bars in which could be set pins for the places where 1 occurs in the number. The pins on one bar would be in reverse order. The bars could be turned over and the number of pins striking could be recorded automatically. At the same time one bar could be moved along one place and be in readiness for the next turn. From the machine then would come the data for compiling the part (B) of Figure I. Or, a more complicated machine could be constructed which would give the part (C) at once. This would so shorten the work of testing the Mersenne numbers that it would be possible to check the results on all of them again with a reasonable expenditure of time.

*Purdue University,
LaFayette, Indiana.*

