THE LUCAS-LEHMER TEST FOR MERSENNE NUMBERS

SIDNEY KRAVITZ
Dover, New Jersey

The purpose of this note is to present certain computer calculations relating to the Lucas-Lehmer Test for the primality of Mersenne Numbers.

The Lucas-Lehmer Test states that the Mersenne number $M_p = 2^p - 1$ is prime if and only if $S_{p-1} \equiv 0 \mod M_p$ where

$$S_{i+1} = S_i^2 - 2 \tag{1}$$

and $S_1 = 4$. Lehmer further states* that this test is valid not only for $S_1 = 4$ but for S_1 equal to 2^{p-2} different numbers mod M_p. These 2^{p-2} starting values, $S_{1,i}$, $(i = 1, 2, \cdots, 2^{p-2})$ are determined by

$$S_{1,i+1} = 14\, S_{1,i} - S_{1,i-1} \tag{2}$$

where $S_{1,1} = S_1 = 4$ and $S_{1,2} = 52$.

Figure 1 demonstrates the Lucas-Lehmer Test for $M_7 = 2^7 - 1 = 127$. Each of the $2^{p-2} = 32$ starting values, $S_{1,i}$, as determined by Eq. (2) leads to $S_6 = 0 \mod M_7$ following Eq. (1). There are 16 different values of S_2, 8 different values of S_3, etc. Note that $S_7 = -2$ and $S_8 = 2 \mod M_7$. The result is that $2^{p-1} + 1 = 65$ different numbers mod M_p are involved in the Lucas-Lehmer test.

What happens to the other $q^{p-1} - 2 = 62$ numbers mod M_7 when we apply Eq. (1)? This is shown in Fig. 2. We see that successive terms do not lead to a zero term, but instead are repetitive in cycles whose periods are divisors of $(p - 1)$. Figure 2 shows four cycles of double sixes and two cycles of double threes.

A computer program was used to determine the structure of the Lucas-Lehmer Test for M_7, M_{13} and M_{17} with the following results.

---

*D. H. Lehmer, "An Extended Theory of Lucas' Functions," Annals of Math., (2) 31 (1930), pages 419-448.

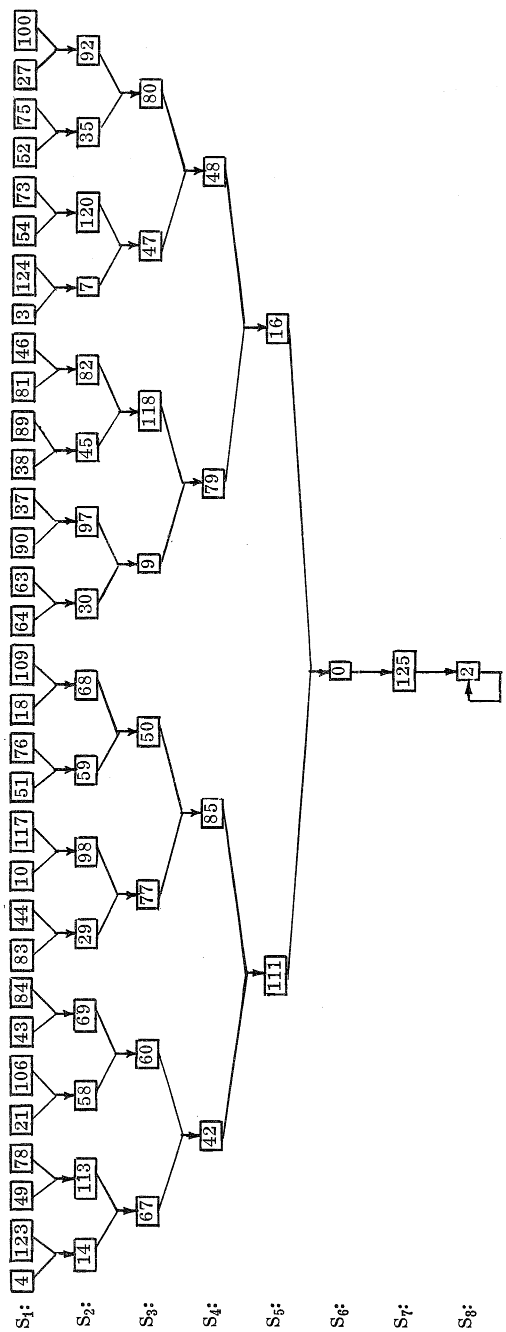

Fig. 1 The Lucas-Lehmer Test for $M_7 = 127$ Involving 65 Numbers mod 127

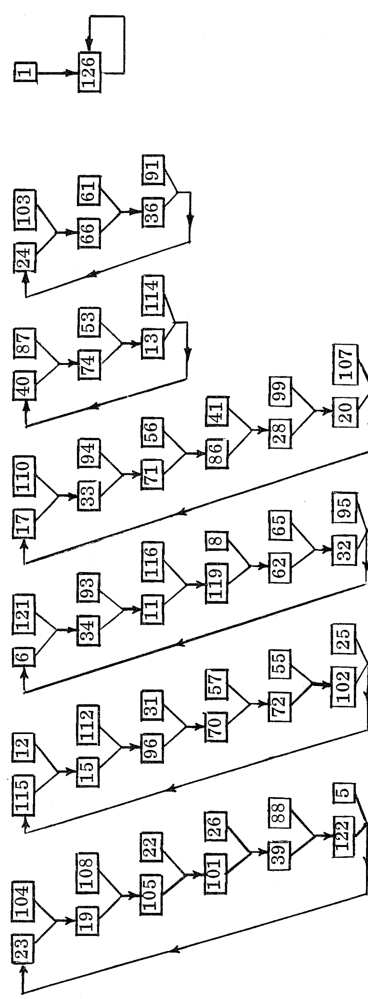

Fig. 2 The 62 Numbers Mod 127 Which are not Involved in the Lucas-Lehmer Test for M_7. There are four cycles of double sixes and two cycles of double threes.

For $M_7 = 127$

A Lucas-Lehmer pattern of $2^{p-1} + 1$ terms	making 65 terms
4 cycles of double sixes	making 48 terms
2 cycles of double threes	making 12 terms
The two terms ± 1	making 2 terms
	Total 127 terms

For $M_{13} = 8191$

A Lucas-Lehmer pattern of $2^{p-1} + 1$ terms	making 4097 terms
165 cycles of double twelves	making 3960 terms
9 cycles of double sixes	making 108 terms
1 cycle of double fours	making 8 terms
2 cycles of double threes	making 12 terms
1 cycle of double twos	making 4 terms
The two terms ± 1	making 2 terms
	Total 8191 terms

For $M_{17} = 131,071$

A Lucas-Lehmer pattern of $2^{p-1} + 1$ terms	making 65537 terms
2032 cycles of double sixteens	making 65024 terms
30 cycles of double eights	making 480 terms
3 cycles of double fours	making 24 terms
1 cycle of double twos	making 4 terms
The two terms ± 1	making 2 terms
	Total 131071 terms

For $M_{19} = 524287$

A Lucas-Lehmer pattern of $2^{p-1} + 1$ terms	making 262145 terms
7252 cycles of double eighteens	making 261072 terms
56 cycles of double nines	making 1008 terms
4 cycles of double sixes	making 48 terms
2 cycles of double threes	making 12 terms
The two terms ± 1	making 2 terms
	Total 524287 terms

* * * * *