PRIMALITY TESTING OF MERSENNE NUMBERS USING MATHEMATICA

M.I.M. ISHAK

Department of Mathematics, Faculty of Science, University of Peradeniya

Let n be a positive integer. Then $M_n = 2^n - 1$ is defined to be the n^{th} Mersenne Number. It is easy to see that if M_n is prime, then n is prime. If both p and M_p are primes, then M_p is called a *Mersenne prime*. It has been conjectured that there are infinitely many Mersenne primes. In 1644, Mersenne conjectured that M_p is prime for $p = 2, 3, 5, 7, 13, 17, 19, 31, 67, 127, 257$, and it is composite for all the other integers greater than 1 and less than 257. The complete list of positive integers less than 258 for which M_p is prime was not available until 1940. The complete list is

$$p = 2, 3, 5, 7, 13, 17, 19, 31, 61, 89, 107, \text{ and } 127.$$

The largest one in this list was verified by Lucas in 1876. The test used for this was later simplified by Lehmer in 1940 and is now known as the *Lucas-Lehmer test*. A proof of this is not freely available in the recommended books for undergraduate Number Theory curriculum.

Lucas-Lehmer Test. Let p be a prime. Let (r_k) be the sequence defined by $r_1 = 4$, and for $k \geq 2$, $r_k = r_{k-1}^{\ 2} - 2 \pmod{M_p}$, $0 \leq r_k < M_p$. Then M_p is prime if and only if $r_{p-1} \equiv 0 \pmod{M_p}$.

In this study, a detailed proof of the *Lucas-Lehmer test* is given that can be comprehended by undergraduates. Further a computer programme to test the primality of Mersenne numbers written in *Mathematica* is also included. Using this programme, primality of M_p for $p \leq 257$ (Mersenne's range) is tested. The largest M_p tested using this programme is for $p = 21701$.