TESTS FOR PRIMALITY BASED ON SYLVESTERS CYCLOTOMIC NUMBERS

MORGAN WARD

Introduction. Lucas, Carmichael [1] and others have given tests for primality of the Fermat and Mersenne numbers which utilize divisibility properties of the Lucas sequences (U) and (V); in this paper we are concerned only with the first sequence;

$$(U):\ U_0,\ U_1,\ U_2,\ \cdots,\ U_n = \frac{\alpha^n - \beta^n}{\alpha - \beta},\ \cdots .$$

Here α and β are the roots of a suitably chosen quadratic polynomial $x^2 - Px + Q$, with P and Q coprime integers. (For an account of these tests, generalizations and references to the early literature, see Lehmer's Thesis [2]).

I develop here a test for primality of a less restrictive nature which utilizes a divisibility property of the Sylvester cyclotomic sequence [3]:

$$(Q) : Q_0 = 0,\ Q_1 = 1,\ Q_2,\ \cdots,\ Q_n = \prod_{\substack{1 \le r \le n \\ (r,n)=1}} (\alpha - e^{\frac{2\pi i r}{n}}\beta),\ \cdots$$

Here α and β have the same meaning as before. (U) and (Q) are closely connected [4]; in fact

$$U_n = \prod_{d \mid n} Q_d\ . \tag{1.1}$$

The divisibility property is expressed by the following theorem proved in § 3 of this paper.

THEOREM. *If m is an odd number dividing some cyclotomic number Q_n whose index n is prime to m, then every divisor of m greater than one has the same rank of apparition n in the Lucas sequence (U) connected with (Q).*

Here the rank of apparition or rank, of any number d in (U) means as usual the least positive index x such that $U_x \equiv 0 \pmod d$.

The following primality test is an immediate corollary.

Primality test. If m is odd, greater than two, and divides some cyclotomic number Q_n whose index n is both prime to m and greater than the square root of m, then m is a prime number except in two trivial cases: $m = (n-1)^2$, $n-1$ a prime greater than 3, or $m = n^2 - 1$ with $n-1$ and $n+1$ both primes.

Received January 14, 1959.