PACIFIC JOURNAL OF MATHEMATICS
Vol. 98, No. 2, 1982

A CLASS OF PRIMALITY TESTS FOR TRINOMIALS WHICH INCLUDES THE LUCAS-LEHMER TEST

H. C. WILLIAMS

When n is an odd prime, the well-known Lucas-Lehmer test gives a necessary and sufficient condition for primality of 2^n-1. In this paper,primality tests of a similar character are developed for certain integers of the form $Ab^{2n}+Bb^n-1$ and a criterion which generalizes the Lucas-Lehmer test is obtained.

1. Introduction. Let $N = 2^n - 1$ where n is an odd prime. The Lucas-Lehmer test for the primality of N reads as follows:

If we put $T_0 = 4$ and define $T_h \pmod N$ by setting $T_{k+1} \equiv T_k^2 - 2 \pmod N$ for $k \geqq 0$, then N is prime if and only if $N \mid T_{n-2}$.

(For proof, see [10, p. 443] or [13, p. 194]. This very elegant test has attracted a great deal of attention (see Williams [17] for a bibliography.) It is also the means by which the largest known primes have been found over the past twenty years.

While the Lucas-Lehmer criterion would only be used when n is a prime, it should be noted that it holds for any odd $n \geqq 3$. When viewed in this way, it falls into a class of primality tests characterized by the following three properties.

(i) The test is restricted to values of N given by some function involving an exponent n which usually belongs to some fixed congruence class and exceeds a certain bound.

(ii) A sequence $\{T_h\colon h \geqq 0\}$ is employed, where T_0 is an easily calculated integer and T_{k+1} is defined $(\mathrm{mod}\, N)$ for $k \geqq 0$ by $T_{k+1} \equiv f(T_k) \pmod N$ where f is some polynomial such that $f(Z) \subseteqq Z$.

(iii) Write $T[k]$ for T_k where $k = m_i$. Then N is prime if and only if $h(T[m_i]\colon 1 \leqq i \leqq \ell) \equiv 0 \pmod N$ where h is a Z-valued polynomial over Z^ℓ for some $\ell \geqq 1$ and the m_i depend on n.

We say that any test with the properties i) through iii) is a primality test of Lucas-Lehmer (or LL) type. Such tests have been given for integers of the form $Ac^n - 1$ with $c = 2$ (Lehmer [10, p. 445]; Riesel [11], [12]; Inkeri [5]; Stechkin [14] and with $c = 3$ (Williams [16]). In this paper, we develop some tests of LL type for integers of the form $Ab^2 + B^nb^n - 1$ and in particular a criterion (Theorem 2) is obtained when $b = 2$ which yields a large number of examples including of original LL test ($A = 2$, $B = 0$) and the new case $A = 2$, $B = \pm 3$. Further, we are able to show that an LL primality test exists even for integers of the form