MATHEMATICS OF COMPUTATION, VOLUME 29, NUMBER 129
JANUARY 1975, PAGES 181–182

A Note on Primality Testing Using Lucas Sequences

By Michael A. Morrison

Dedicated to D. H. Lehmer on his 70th birthday

Abstract. For an odd integer $N > 1$, thought to be prime, a test is given which uses Lucas sequences and which can establish that any prime divisors of N are $\equiv \pm 1$ modulo the factored portion of $N+1$.

For an odd integer $N > 1$, the complete factorization of $N + 1$ or $N - 1$ provides sufficient information to establish whether or not N is prime (see [1], [2]). Unfortunately, when N is large, it is generally very difficult and time-consuming to complete such a factorization. In such a case, the partial factorization can be extremely useful, since it can be used to restrict any possible divisors of N to a small number of arithmetic sequences with (hopefully) large differences.

The theory of Lucas sequences becomes useful when considering $N + 1$. A theorem of D. H. Lehmer [1] asserts that, if p is a prime such that $p^\alpha \| N + 1$, and if there exists a Lucas sequence with certain properties, then any divisor of N is of the form $ap^\alpha \pm 1$. Thus, if s distinct primes were known to divide $N + 1$, there would be 2^s different sequences which might contain a factor of N. The following theorem shows that it is possible to reduce these 2^s sequences to only two: namely, $\{aP + 1\}$ and $\{aP - 1\}$, where P is the factored portion of $N + 1$.

THEOREM. *Let D be an integer such that the Jacobi symbol $(D/N) = -1$, and let $N + 1 = R\prod_{i=1}^s p_i^{\alpha_i}$ where, for all i, p_i is prime and $(R, p_i) = 1$. If for each i there exists a Lucas sequence $\{U_k^{(i)}\}$ with discriminant D such that*

$$N \mid U_{N+1}^{(i)} \tag{1}$$

and

$$(U_{(N+1)/p_i}^{(i)}, N) = 1, \tag{2}$$

then every prime divisor n of N satisfies $n \equiv \pm 1 \pmod{\prod_{i=1}^s p_i^{\alpha_i}}$.

PROOF. Let n be a prime divisor of N and let $\omega_i(n)$ denote its rank of apparition in $\{U_k^{(i)}\}$. Then $n \mid U_k^{(i)}$ if and only if $\omega_i(n) \mid k$, and thus (1) implies that for each i, $\omega_i(n)$ exists and divides $N + 1$. But (2) implies that $\omega_i(n) \nmid (N + 1)/p_i$, and thus $p_i^{\alpha_i} \mid \omega_i(n)$ for each i.

Received July 12, 1974.

AMS (MOS) subject classifications (1970). Primary 10A25; Secondary 10A35.

Key words and phrases. Primality testing, Lucas sequences.

However, since n is prime, $n \mid U^{(i)}_{n-(D/n)}$. Hence, $\omega_i(n) \mid n - (D/n)$ for each i, which implies that $p_i^{\alpha_i} \mid n - (D/n)$ for each i. Therefore, $n \equiv (D/n) = \pm 1 \pmod{\Pi_{i=1}^{s} p_i^{\alpha_i}}$.
$\pm 1 \pmod{\Pi_{i=1}^{s} p_i^{\alpha_i}}$.

Department of Mathematics
University of California
Los Angeles, California 90024

1. D. H. LEHMER, "An extended theory of Lucas functions," *Ann. of Math.*, v. 31, 1930, pp. 442–443.

2. E. LUCAS, "Théorie des fonctions numériques simplement périodiques," *Amer. J. Math.*, v. 1, 1878, p. 302.