Therefore, $k_m = k_n$, and we have the relation

$$p_m(z) = z^{m-n}p_n(z) = z^{m-n}(k_n z^n + l_n).$$

We have assumed, until now, that the sequence $p_2(0)$, $p_3(0)$, $\cdots$ contained a nonzero term. If this is not the case, the last result still holds with $n=1$, as may be seen from (4) in the same way as before.

Now we have, if $m \geqq n$, $m' \geqq n$, $m \neq m'$,

$$\int_{-\pi}^{+\pi} f(\theta)e^{i(m-m')\theta}\,|\,k_n z^n + l_n\,|^2 d\theta = 0, \qquad z = e^{i\theta}.$$

Whence, except on a set of measure zero, we have

$$f(\theta) = \text{const.}\ |\,k_n z^n + l_n\,|^{-2}, \qquad z = e^{i\theta}. \tag{11}$$

We conclude the proof with the obvious remark that the polynomials $1, z, z^2, \cdots, z^{n-1}$ are orthogonal on the unit circle $|z| = 1$ with the weight function (11).

STANFORD UNIVERSITY

A FACTORIZATION THEOREM APPLIED TO A TEST FOR PRIMALITY*

D. H. LEHMER

Certain tests for primality based on the converse of Fermat's theorem and its generalizations have been devised and applied by the writer during the past ten years.† Perhaps the most useful test for the investigation of a large number N of no special form may be given as follows:‡

THEOREM 1. *If N divides $a^{N-1}-1$ but is relatively prime to $a^{(N-1)/p}-1$, where p is a prime, then all the possible factors of N are of the form $p^\alpha x+1$, if $N-1$ is divisible by p^α, $(\alpha \geqq 1)$.*

Strictly speaking this is not a test for primality since the theorem merely gives a restriction on the factors of N. If $p^\alpha > N^{1/2}$ then, obviously, N is a prime. If p^α is only fairly large, the theorem gives

* Presented to the Society, February 26, 1938.

† This Bulletin, vol. 33 (1927), pp. 327–340; vol. 34 (1928), pp. 54–56; vol. 35 (1929), pp. 349–350; vol. 38 (1932), pp. 383–384; vol. 39 (1933), pp. 105–108; Annals of Mathematics, (2), vol. 31 (1930), pp. 419–448; Journal of the London Mathematical Society, vol. 10 (1935), pp. 162–165; American Mathematical Monthly, vol. 43 (1936), pp. 347–354.

‡ This Bulletin, vol. 33 (1927), p. 331.