ON THE LEAST PRIMITIVE ROOT OF A PRIME

PAUL ERDÖS AND HAROLD N. SHAPIRO

1. Introduction. The problem of estimating the least positive primitive root $g(p)$ of a prime p seems to have been first considered by Vinogradov. His first result was [4, v. 2 part 7 chap. 14]

$$g(p) \leqq 2^m p^{1/2} \log p\,, \tag{1.1}$$

where m denotes the number of distinct prime factors of p-1. In 1930, [6], he improved this to

$$g(p) \leqq 2^m \frac{p-1}{\phi(p-1)} p^{1/2} \tag{1.2}$$

where $\phi(n)$ is the Euler ϕ-function. Next, in 1942, Hua [3] improved this to

$$g(p) < 2^{m+1} p^{1/2}\,, \tag{1.3}$$

and obtained also, for the primitive root of least absolute value, $h(p)$,

$$|h(p)| < 2^m p^{1/2}\,. \tag{1.4}$$

Lastly, Erdös [2] proved that for p sufficiently large

$$g(p) < p^{1/2}(\log p)^{17}\,. \tag{1.5}$$

This last result, of course, is not directly comparable with the others, giving better results for some primes and worse results for others.

In any event, all of the results are very weak (as is evidenced by a glance at tables of primitive roots [1]) in relationship to the conjecture that the true order of $g(p)$ is about $\log p$. In this connection, Pillai [5] has proved

$$g(p) > \log \log p \tag{1.6}$$

for infinitely many p.

In this note we shall give a very simple way of handling character sums, which not only yields (1.3) and (1.4) but allows a small improvement of these results; for example

$$g(p) = O(m^c p^{1/2})\,, \quad (c \text{ a constant})\,. \tag{1.7}$$

Received March 12, 1956.