Zbl 079.06304
Erdős, Paul; Shapiro, Harold N.
On the least primitive root of a prime. (In English)
Pac. J. Math. 7, 861-865 (1957). [0030-8730]

Let $g(p)$ be the least positive primitive root of a prime p. The authors prove that $g(p) = O(m^c p^{1/2})$ where c is a constant and m is the number of distinct prime factors of $p-1$. As m large, it is an improvement of a result of the reviewer: $g(p) \le 2^{m+1}p^{1/2}$. The authors introduce a lemma and then apply Brun's method to obtain the result. The lemma runs as following: Let S and T be two sets with distinct integers, mod p. Then for any non-principal character χ, we have

$$\left|\sum_{u\in S, v\in T} \chi(u+v)\right|^2 \le p \sum_{u\in S} 1 \sum_{v\in T} 1.$$

L.K.Hua

Classification:
11N69 Distribution of integers in special residue classes
11A07 Congruences, etc.