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.

2. A lemma concerning character sums. We consider first an inequality for certain character sums on which our later estimates will depend. Let S and T be any two sets of integers, such that modulo a given prime p, no two integers of S are congruent, and no two integers of T are congruent. Denote by $N(S)$, $N(T)$ the number of integers in S and T respectively. We have

LEMMA. For χ a non-principal character modulo p,

$$\left|\sum_{\substack{u\in S\\ v\in T}}\chi(u+v)\right|\leqq p^{1/2}\sqrt{N(S)N(T)}\,. \tag{2.1}$$

Proof. Set

$$\tau(\chi)=\sum_{h=1}^{p}\chi(h)e^{2\pi ih/p}.$$

It is well known that $|\tau(\chi)|=p^{1/2}$, for χ a non-principal character. Also,

$$\tau(\bar{\chi})\chi(t)=\sum_{h=1}^{p}\bar{\chi}(h)e^{2\pi iht/p}\,.$$

From this we get

$$\tau(\bar{\chi})\sum_{\substack{u\in S\\ v\in T}}\chi(u+v)=\sum_{\substack{u\in S\\ v\in T}}\sum_{h=1}^{p}\bar{\chi}(h)e^{2\pi ih/p\cdot(u+v)}.$$

Then taking absolute values and using Schwarz's inequality

$$p^{1/2}\left|\sum_{\substack{u\in S\\ v\in T}}\chi(u+v)\right|\leqq\sum_{h=1}^{p}\left|\sum_{u\in S}e^{2\pi ihu/p}\right|\left|\sum_{v\in T}e^{2\pi ihv/p}\right|$$

$$\leqq\left\{\sum_{h=1}^{p}\left|\sum_{u\in S}e^{2\pi ihu/p}\right|^2\sum_{h=1}^{p}\left|\sum_{v\in T}e^{2\pi ihv/p}\right|^2\right\}^{1/2}.$$

But

$$\sum_{h=1}^{p}\left|\sum_{u\in S}e^{2\pi ihu/p}\right|^2=\sum_{h=1}^{p}\sum_{\substack{u_1\in S\\ u_2\in S}}e^{2\pi ih/p\cdot(u_1-u_2)}$$

$$=\sum_{\substack{u_1\in S\\ u_2\in S}}\sum_{h=1}^{p}e^{2\pi ih/p\cdot(u_1-u_2)}=pN(S)\,.$$

Similarly

$$\sum_{h=1}^{p}\left|\sum_{v\in T}e^{2\pi ihv/p}\right|^2=pN(T),$$

and the lemma follows immediately.

3. Another proof of Hua's result. By way of illustrating the manner in which the above lemma is to be applied we give here another proof of (1.3). It is well known that if t is not a primitive root modulo p then

$$P(t)=\sum_{d|p-1}\frac{\mu(d)}{\phi(d)}\sum_{o(\chi)=d}\chi(t)=0\,,$$

where $o(\chi)=d$ denotes that the inner summation is taken over all characters of order d.

Now if $x+1=g(p)$, the smallest positive primitive root mod p, we see that $P(t)=0$, $1\leqq t\leqq x$. Thus let $S=T$ denote the set of integers $1, 2, \cdots, [x/2]$; we have

$$0=\sum_{d|p-1}\frac{\mu(d)}{\phi(d)}\sum_{o(\chi)=d}\sum_{\substack{u\in S\\ v\in T}}\chi(u+v)$$

$$=[x/2]^2+\sum_{\substack{d|p-1\\ d>1}}\frac{\mu(d)}{\phi(d)}\sum_{o(\chi)=d}\sum_{\substack{u\in S\\ v\in T}}\chi(u+v)\,.$$

Applying the lemma, this gives

$$(2^m-1)p^{1/2}[x/2]\geqq[x/2]^2$$

or

$$[x/2]\leqq(2^m-1)p^{1/2}\,.$$

Since $2[x/2]+2\geqq x+1=g(p)$ this yields

$$g(p)\leqq 2^{m+1}p^{1/2}-2p^{1/2}+2<2^{m+1}p^{1/2}$$

which is Hua's result (1.3).

Similarly, if in the above argument we use for $S=T$ the set of nonzero integers $-[x/2], \cdots, [x/2]$ where $x+1=|h(p)|$, we are led immediately to the result (1.4).

4. A small improvement in the estimate. The facility with which the lemma of § 2 enables us to handle the relevant character sums makes possible an improvement of the estimates for $g(p)$ and $h(p)$. We consider only the case of $g(p)$, since a similar estimate for $h(p)$ then follows automatically.

Let $F_x(d)$ denote the number of integers among

$$u+v,\ 1\leqq u\leqq[x/2],\ 1\leqq v\leqq[x/2]$$

such that $u+v$ is a dth power residue modulo p. Then, letting S denote the set of integers $1, 2, \cdots, [x/2]$, we have

$$F_x(d)=\frac{1}{d}\sum_{\substack{u\in S\\ v\in S}}\sum_{o(\chi)\mid d}\chi(u+v)$$

$$=\frac{1}{d}[x/2]^2+\frac{1}{d}\sum_{\substack{o(\chi)\mid d\\ o(\chi)>1}}\sum_{\substack{u\in S\\ v\in S}}\chi(u+v)\,.$$

Applying the lemma of § 2 we obtain

$$F_x(d)=\frac{x^2}{4d}+O(xp^{1/2})\,. \tag{4.1}$$

If we let $N(x)$ denote the numbers among the

$$u+v,\quad u\in S,\quad v\in S$$

which are primitive roots modulo p, it is easily seen that

$$N(x)=\sum_{d\mid p-1}\mu(d)F_x(d)\,. \tag{4.2}$$

Applying Brun's method to (4.2), in conjunction with (4.1), in order to make a lower estimate for $N(x)$, one obtains

$$N(x)>\frac{x^2}{4}\sum_{d\mid p-1}\frac{\mu(d)}{d}+O(m^cp^{1/2}x)$$

or

$$N(x)>\frac{\phi(p-1)}{p-1}\,\frac{x^2}{4}+O(m^cp^{1/2}x)\,. \tag{4.3}$$

Thus if we take $x+1=g(p)$, $N(x)=0$ and (4.3) yields

$$x=O\Big(\frac{p-1}{\phi(p-1)}\,m^cp^{1/2}\Big)\,. \tag{4.4}$$

Finally since

$$\frac{p-1}{\phi(p-1)}=\prod_{q\mid p-1}\frac{1}{1-1/q}<\prod_{i=1}^{m}\frac{1}{1-1/p_i}=O(\log m)=O(m^\varepsilon)$$

(where p_i denotes the ith prime), (4.4) gives

$$x=O(m^cp^{1/2})\,,$$

and hence

$$g(p)=O(m^cp^{1/2})\,,$$

which is the desired result.

REFERENCES

1. Allan Cunningham, H. J. Woodall and T. G. Creak, *On least primitive roots*, Proc. London Math. Soc. 2nd series, **21** (1922–23), 343–358.
2. P. Erdös, *Least primitive root of a primc*, Bull. Amer. Math. Soc., **55** (1945), 131–132.
3. L. K. Hua, *On the least primitive root of prime*, Bull. Amer. Math. Soc., **48** (1942), 726–730.
4. E. Landau, *Vorlesungen über Zahlentheorie*, Leipzig 1927, (New York 1947).
5. S. Pillai, *On the smallest primitive root of a prime*, J. Indian Math. Soc., **8** (1944), 14–17.
6. I. M. Vinogradov, *On the least primitive root of a prime*, Dokl. Akad. Nauk, S.S.S.R. (1930), 7–11.

NOTRE DAME UNIVERSITY
NEW YORK UNIVERSITY