

Pacific Journal of Mathematics

ON THE LEAST PRIMITIVE ROOT OF A PRIME

PAUL ERDŐS AND HAROLD NATHANIEL SHAPIRO

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]

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

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

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

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

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

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

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

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

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

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

$$(1.6) \quad g(p) > \log \log p$$

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

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

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 ,

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

Proof. Set

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

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

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

From this we get

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

Then taking absolute values and using Schwarz's inequality

$$\begin{aligned} p^{1/2} \left| \sum_{\substack{u \in S \\ v \in T}} \chi(u + v) \right| &\leq \sum_{h=1}^p \left| \sum_{u \in S} e^{2\pi i h u/p} \right| \left| \sum_{v \in T} e^{2\pi i h v/p} \right| \\ &\leq \left\{ \sum_{h=1}^p \left| \sum_{u \in S} e^{2\pi i h u/p} \right|^2 \sum_{h=1}^p \left| \sum_{v \in T} e^{2\pi i h v/p} \right|^2 \right\}^{1/2} . \end{aligned}$$

But

$$\begin{aligned} \sum_{h=1}^p \left| \sum_{u \in S} e^{2\pi i h u/p} \right|^2 &= \sum_{h=1}^p \sum_{\substack{u_1 \in S \\ u_2 \in S}} e^{2\pi i h/p \cdot (u_1 - u_2)} \\ &= \sum_{\substack{u_1 \in S \\ u_2 \in S}} \sum_{h=1}^p e^{2\pi i h/p \cdot (u_1 - u_2)} = pN(S) . \end{aligned}$$

Similarly

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

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 $P(t)=0, 1 \leq t \leq x$. Thus let $S=T$ denote the set of integers $1, 2, \dots, [x/2]$; we have

$$\begin{aligned} 0 &= \sum_{d|p-1} \frac{\mu(d)}{\phi(d)} \sum_{o(\chi)=d} \sum_{\substack{u \in S \\ v \in T}} \chi(u+v) \\ &= [x/2]^2 + \sum_{\substack{d|p-1 \\ d > 1}} \frac{\mu(d)}{\phi(d)} \sum_{o(\chi)=d} \sum_{\substack{u \in S \\ v \in T}} \chi(u+v). \end{aligned}$$

Applying the lemma, this gives

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

or

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

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

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

which is Hua's result (1.3).

Similarly, if in the above argument we use for $S=T$ the set of nonzero integers $-[x/2], \dots, [x/2]$ 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

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

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

$$\begin{aligned}
 F_x(d) &= \frac{1}{d} \sum_{\substack{u \in S \\ v \in S}} \sum_{\substack{o(x) \equiv 1 \pmod{d} \\ o(x) > 1}} \chi(u + v) \\
 &= \frac{1}{d} [x/2]^2 + \frac{1}{d} \sum_{\substack{o(x) \equiv 1 \pmod{d} \\ o(x) > 1}} \sum_{\substack{u \in S \\ v \in S}} \chi(u + v).
 \end{aligned}$$

Applying the lemma of § 2 we obtain

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

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

$$(4.2) \quad N(x) = \sum_{d|p-1} \mu(d) F_x(d).$$

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

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

or

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

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

$$(4.4) \quad x = O\left(\frac{p-1}{\phi(p-1)} m^c p^{1/2}\right).$$

Finally since

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

(where p_i denotes the i th prime), (4.4) gives

$$x = O(m^c p^{1/2}),$$

and hence

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

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. Erdős, *Least primitive root of a prime*, 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

PACIFIC JOURNAL OF MATHEMATICS

EDITORS

H. L. ROYDEN
Stanford University
Stanford, California

R. A. BEAUMONT
University of Washington
Seattle 5, Washington

A. R. WHITEMAN
University of Southern California
Los Angeles 7, California

E. G. STRAUS
University of California
Los Angeles 24, California

ASSOCIATE EDITORS

E. F. BECKENBACH
C. E. BURGESS
M. HALL
E. HEWITT

A. HORN
V. GANAPATHY IYER
R. D. JAMES
M. S. KNEBELMAN

L. NACHBIN
I. NIVEN
T. G. OSTROM
M. M. SCHIFFER

G. SZEKERES
F. WOLF
K. YOSIDA

SUPPORTING INSTITUTIONS

UNIVERSITY OF BRITISH COLUMBIA
CALIFORNIA INSTITUTE OF TECHNOLOGY
UNIVERSITY OF CALIFORNIA
MONTANA STATE UNIVERSITY
UNIVERSITY OF NEVADA
OREGON STATE COLLEGE
UNIVERSITY OF OREGON
UNIVERSITY OF SOUTHERN CALIFORNIA

STANFORD UNIVERSITY
UNIVERSITY OF UTAH
WASHINGTON STATE COLLEGE
UNIVERSITY OF WASHINGTON
* * *
AMERICAN MATHEMATICAL SOCIETY
CALIFORNIA RESEARCH CORPORATION
HUGHES AIRCRAFT COMPANY
THE RAMO-WOOLDRIDGE CORPORATION

Printed in Japan by Kokusai Bunken Insatsusha
(International Academic Printing Co., Ltd.), Tokyo, Japan

Richard Davis Anderson, <i>Zero-dimensional compact groups of homeomorphisms</i>	797
Hans-Joachim Bremermann, <i>Holomorphic functionals and complex convexity in Banach spaces</i>	811
Hugh D. Brunk, G. M. Ewing and W. R. Utz, <i>Minimizing integrals in certain classes of monotone functions</i>	833
Philip David, <i>Uniqueness theory for asymptotic expansions in general regions</i>	849
Paul Erdős and Harold Nathaniel Shapiro, <i>On the least primitive root of a prime</i>	861
Watson Bryan Fulks, <i>Regular regions for the heat equation</i>	867
William Robert Gaffey, <i>A real inversion formula for a class of bilateral Laplace transforms</i>	879
Ronald Kay Gettoor, <i>On characteristic functions of Banach space valued random variables</i>	885
Louis Guttman, <i>Some inequalities between latent roots and minimax (maximin) elements of real matrices</i>	897
Frank Harary, <i>The number of dissimilar supergraphs of a linear graph</i>	903
Edwin Hewitt and Herbert S. Zuckerman, <i>Structure theory for a class of convolution algebras</i>	913
Amnon Jakimovski, <i>Some Tauberian theorems</i>	943
C. T. Rajagopal, <i>Simplified proofs of "Some Tauberian theorems" of Jakimovski</i>	955
Paul Joseph Kelly, <i>A congruence theorem for trees</i>	961
Robert Forbes McNaughton, Jr., <i>On the measure of normal formulas</i>	969
Richard Scott Pierce, <i>Distributivity in Boolean algebras</i>	983
Calvin R. Putnam, <i>Continuous spectra and unitary equivalence</i>	993
Marvin Rosenblum, <i>Perturbation of the continuous spectrum and unitary equivalence</i>	997
V. N. Singh, <i>Certain generalized hypergeometric identities of the Rogers-Ramanujan type</i>	1011
Peter Swerling, <i>Families of transformations in the function spaces H^p</i>	1015