$$0 < t - x < 1/n \text{ implies } [F(t) - F(x)]/(t - x) \leqq n;$$

the remainder of the proof is unaltered. The next lemma is a slight generalization of a theorem of Marcinkiewicz.

LEMMA 5.2. *If $f(x)$ is measurable on $[a, b]$, and has either a left major or a right major, and also has either a left minor or a right minor, then $f(x)$ is Perron integrable on $[a, b]$.*

The proof is that given by Saks, op. cit., p. 253; the principal change is that the reference to his Theorem 10.1 is replaced by a reference to our Lemma 5.1.

Since every P^*-integrable function $f(x)$ is measurable and has right majors and right minors, it is also Perron integrable by Lemma 5.2, and the equivalence of the integrals is established.

UNIVERSITY OF VIRGINIA

ON THE LEAST PRIMITIVE ROOT OF A PRIME

LOO-KENG HUA

It was proved by Vinogradow[1] that the least positive primitive root $g(p)$ of a prime p is $O(2^m p^{1/2} \log p)$ where m denotes the number of different prime factors of $p-1$. In 1930 he[2] improved the previous result to

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

or more precisely,

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

It is the purpose of this note, by introducing the notion of the average of character sums,[3] to prove that if $h(p)$ denotes the primitive root with the least absolute value, mod p, then

$$|h(p)| < 2^m p^{1/2};$$

Received by the editors December 3, 1941.

[1] See, Landau, *Vorlesungen über Zahlentheorie*, vol. 2, part 7, chap. 14. The original papers of Vinogradow are not available in China.

[2] Comptes Rendus de l'Académie des Sciences de l'URSS, 1930, pp. 7–11.

[3] The present note may be regarded as an introduction of a method which has numerous applications.

and that for $p\equiv 1 \pmod 4$, we have

$$g(p) < 2^m p^{1/2},$$

while, for $p\equiv 3 \pmod 4$, we have

$$g(p) < 2^{m+1} p^{1/2}.$$

Since

$$\frac{p-1}{\phi(p-1)} \geqq 2,$$

the result is always better than that due to Vinogradow.

LEMMA 1. *Let $p>2$, $1\leqq A<p$. For each non-principal character*[4] $\chi(n)$, mod p, *we have*

$$\frac{1}{A+1}\left|\sum_{a=0}^{A}\sum_{n=-a}^{a}\chi(n)\right| \leqq p^{1/2} - \frac{A+1}{p^{1/2}}.$$

PROOF. Let $\epsilon = e^{2\pi i/p}$ and let

$$\tau(\chi) = \sum_{h=1}^{p-1}\chi(h)\epsilon^h.$$

It is known that

$$|\tau(\chi)| = p^{1/2}.$$

For $p\nmid n$, we have

$$\sum_{h=1}^{p-1}\bar{\chi}(h)\epsilon^{hn} = \chi(n)\sum_{h=1}^{p-1}\bar{\chi}(hn)\epsilon^{hn}$$

$$= \chi(n)\sum_{h=1}^{p-1}\bar{\chi}(h)\epsilon^{h} = \chi(n)\tau(\bar{\chi}).$$

The formula holds also for $p|n$, since $\chi(n)=0$ for $p|n$ and

$$\sum_{h=1}^{p-1}\bar{\chi}(h) = 0.$$

Thus

$$\tau(\bar{\chi})\sum_{a=0}^{A}\sum_{n=-a}^{a}\chi(n) = \sum_{h=1}^{p-1}\bar{\chi}(h)\sum_{a=0}^{A}\sum_{n=-a}^{a}\epsilon^{hn}$$

$$= \sum_{h=1}^{p-1}\bar{\chi}(h)\left(\frac{\sin (A+1)\pi h/p}{\sin \pi h/p}\right)^2.$$

[4] See, for example, Landau loc. cit., vol. 1, pp. 83–87.

Consequently

$$p^{1/2}\left|\sum_{a=0}^{A}\sum_{n=-a}^{a}\chi(n)\right| \leqq \sum_{h=1}^{p-1}\left(\frac{\sin (A+1)\pi h/p}{\sin \pi h/p}\right)^2$$
$$= \sum_{h=1}^{p-1}\sum_{a=0}^{A}\sum_{n=-a}^{a}\epsilon^{hn}$$
$$= \sum_{a=0}^{A}\sum_{n=-a}^{a}\left(\sum_{h=1}^{p}\epsilon^{hn}-1\right)$$
$$= (A+1)p-(A+1)^2.$$

LEMMA 2. *Let $p>2$, $1\leqq A<(p-1)/2$. Then, for each non-principal character*, mod p, *we have*

$$\frac{1}{A+1}\left|\sum_{a=0}^{A}\sum_{n=A+1-a}^{A+1+a}\chi(n)\right| \leqq p^{1/2}-\frac{A+1}{p^{1/2}}.$$

PROOF. As in Lemma 1, we have

$$p^{1/2}\left|\sum_{a=0}^{A}\sum_{n=A+1-a}^{A+1+a}\chi(n)\right| = \left|\sum_{h=1}^{p-1}\bar{\chi}(h)e^{2\pi ih(A+1)p}\left(\frac{\sin (A+1)\pi h/p}{\sin \pi h/p}\right)^2\right|$$
$$\leqq \sum_{h=1}^{p-1}\left(\frac{\sin (A+1)\pi h/p}{\sin \pi h/p}\right)^2$$
$$= (A+1)p-(A+1)^2.$$

LEMMA 3. *Let $p>2$. If n is not a primitive root*, mod p, *then*

$$\sum_{k|p-1}\frac{\mu(k)}{\phi(k)}\sum_{\chi^{(k)}}\chi^{(k)}(n) = 0,$$

where $\chi^{(k)}$ runs over all characters χ satisfying the condition that k is the least positive integer such that $(\chi)^k$ is the principal character.

(See Landau, loc. cit., p. 496. The condition $1\leqq n<p$ there mentioned is not necessary.)

THEOREM 1. *We have* $|h(p)|<2^m p^{1/2}$.

PROOF. Let $p>2$. By Lemma 3, we have

$$0 = \sum_{k|p-1}\frac{\mu(k)}{\phi(k)}\sum_{\chi^{(k)}}\sum_{a=0}^{|h(p)|-1}\sum_{n=-a}^{a}\chi^{(k)}(n).$$

For $k=1$, the right-hand side gives

$$\sum_{a=0}^{|h(p)|-1} \sum_{n=-a}^{a} \chi^{(1)}(n) = \sum_{a=0}^{|h(p)|-1} 2a.$$
$$= | h(p) |^2 - | h(p) |.$$

On the other hand, for $k \neq 1$, we have, by Lemma 1 with $A = |h(p)| - 1$,

$$\left| \sum_{a=0}^{|h(p)|-1} \sum_{n=-a}^{a} \chi^{(k)}(n) \right| \leqq | h(p) | p^{1/2} - \frac{| h(p) |^2}{p^{1/2}}.$$

Therefore

$$| h(p) |^2 - | h(p) | \leqq \left(| h(p) | p^{1/2} - \frac{| h(p) |^2}{p^{1/2}} \right) \sum_{k | p-1} \frac{| \mu(k) |}{\phi(k)} \phi(k)$$
$$= 2^m \left(| h(p) | p^{1/2} - \frac{| h(p) |^2}{p^{1/2}} \right).$$

Then

$$| h(p) | \leqq \frac{2^m p^{1/2} + 1}{1 + 2^m / p^{1/2}} < 2^m p^{1/2}.$$

COROLLARY. *For* $p \equiv 1 \pmod 4$, *we have* $g(p) = |h(p)| < 2^m p^{1/2}$.

PROOF. We have to show that $|h(p)|$ is a primitive root. Suppose it is not. Then $-|h(p)|$ is a primitive root and $|h(p)|$ belongs to an exponent l where $l | (p-1)$ and $l < p-1$, that is,

$$| h(p) |^l \equiv 1 \pmod p,$$
$$(h(p))^{2l} \equiv 1 \pmod p.$$

Thus $2l = p-1$ and $|h(p)|^{(p-1)/2} \equiv 1 \pmod p$ so that $|h(p)|$ is a quadratic residue. Since -1 is a quadratic residue, mod p, $-|h(p)|$ is also a quadratic residue and $\{-|h(p)|\}^{(p-1)/2} \equiv 1 \pmod p$. This contradicts the fact that $-|h(p)|$ is a primitive root.

REMARK. Sometimes Theorem 1 may be improved by the fact that

$$\sum_{n=-a}^{a} \chi^{(k)}(n) = 0,$$

for $\chi^{(k)}(-1) = -1$ and hence $\chi^{(k)}(n) = -\chi^{(k)}(-n)$. Thus for $p \equiv 3 \pmod 4$,

$$| h(p) | < 2^{m-1} p^{1/2}.$$

In fact, we have $g^{(p-1)/2} \equiv -1 \pmod p$ and $\chi^{(k)}(g) = e^{2\pi i \lambda / k}$. Since

$$-1 = \chi^{(k)}(g^{(p-1)/2}) = e^{\pi i (p-1) \lambda / k},$$

we have $2\nmid(p-1)\lambda/k$. The terms appearing in the formula of Lemma 3 are those with square-free k. Thus $\chi^{(k)}(-1)=-1$ holds only for the case $p\equiv 3 \pmod 4$, and $2\nmid\lambda$. Thus

$$\sum_{a=0}^{|h(p)|-1}\sum_{n=-a}^{a}\chi^{(k)}(n)=0 \qquad \text{for } 2\mid k.$$

Therefore

$$|h(p)|^2-|h(p)|\leqq\left(|h(p)|p^{1/2}-\frac{|h(p)|^2}{p^{1/2}}\right)\sum_{k\mid(p-1)/2}|\mu(k)|$$
$$=2^{m-1}\left(|h(p)|p^{1/2}-\frac{|h(p)|^2}{p^{1/2}}\right).$$

Then

$$|h(p)|\leqq\frac{2^{m-1}p^{1/2}+1}{1+2^{m-1}/p^{1/2}}<2^{m-1}p^{1/2}.$$

THEOREM 2. *We have* $g(p)<2^{m+1}p^{1/2}$.

PROOF. Let A be the greatest integer not exceeding $(g-1)/2$. Then

$$0=\sum_{k\mid p-1}\frac{\mu(k)}{\phi(k)}\sum_{\chi^{(k)}}\sum_{a=0}^{A}\sum_{n=A+1-a}^{A+1+a}\chi^{(k)}(n).$$

For $k=1$, the right-hand side gives

$$\sum_{a=0}^{A}\sum_{n=A+1-a}^{A+1+a}\chi^{(1)}(n)=\sum_{a=0}^{A}(2a+1)=(A+1)^2.$$

For $k\neq 1$, we have

$$\left|\sum_{a=0}^{A}\sum_{n=A+1-a}^{A+1+a}\chi^{(k)}(n)\right|\leqq(A+1)p^{1/2}-\frac{1}{p^{1/2}}(A+1)^2.$$

Therefore, as in the proof of Theorem 1, we have

$$(A+1)^2<2^m\left((A+1)p^{1/2}-\frac{1}{p^{1/2}}(A+1)^2\right),$$

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

that is,

$$g\leqq\frac{2^{m-1}p^{1/2}}{1+2^m/p^{1/2}}+1<2^{m+1}p^{1/2}.$$

NATIONAL TSING HUA UNIVERSITY