$0 < t - x < 1/n$ implies $\frac{F(t) - F(x)}{(t - x)}^n \leq n$;

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 Vinogradov\(^1\) 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,

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

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.


\(^3\) 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
\[
\frac{p - 1}{\phi(p - 1)} \geq 2,
\]
the result is always better than that due to Vinogradov.

**Lemma 1.** Let \( p > 2 \), \( 1 \leq A < p \). For each non-principal character \( \chi(n) \), mod \( p \), we have
\[
\frac{1}{A + 1} \left| \sum_{n=0}^{A} \sum_{n=0}^{a} \chi(n) \right| \leq \frac{A + 1}{p^{1/2}}.
\]

**Proof.** Let \( \epsilon = e^{2\pi i/p} \) and let
\[
\tau(\chi) = \sum_{h=1}^{p-1} \chi(h) e^{\chi}.
\]
It is known that
\[
|\tau(\chi)| = p^{1/2}.
\]
For \( p \nmid n \), we have
\[
\sum_{h=1}^{p-1} \overline{\chi}(h) e^{\chi h n} = \chi(n) \sum_{h=1}^{p-1} \overline{\chi}(hn) e^{\chi h n} = \chi(n) \sum_{h=1}^{p-1} \overline{\chi}(h) e^{\chi h} = \chi(n) \tau(\overline{\chi}).
\]
The formula holds also for \( p \nmid n \), since \( \chi(n) = 0 \) for \( p \nmid n \) and
\[
\sum_{h=1}^{p-1} \overline{\chi}(h) = 0.
\]
Thus
\[
\tau(\chi) \sum_{a=0}^{A} \sum_{n=0}^{a} \chi(n) = \sum_{h=1}^{p-1} \overline{\chi}(h) \sum_{a=0}^{A} \sum_{n=0}^{a} e^{\chi h n}
\]
\[
= \sum_{h=1}^{p-1} \overline{\chi}(h) \left( \frac{\sin (A + 1) \pi h / p}{\sin \pi h / p} \right)^2.
\]

\(^4\) See, for example, Landau loc. cit., vol. 1, pp. 83–87.
Consequently
\[
\left| \sum_{a=0}^{A} \sum_{n=-a}^{a} \chi(n) \right| \leq \left| \sum_{h=1}^{p-1} \left( \frac{\sin (A + 1) \pi h/p}{\sin \pi h/p} \right)^2 \right|
\]
\[
= \sum_{h=1}^{p-1} \left( \sum_{a=0}^{A} \sum_{n=-a}^{a} e^{\chi n} \right)
\]
\[
= \sum_{a=0}^{A} \sum_{n=-a}^{a} \left( \sum_{h=1}^{p} e^{\chi n} - 1 \right)
\]
\[
= (A + 1)p - (A + 1)^2.
\]

**Lemma 2.** Let \( p > 2, 1 \leq A < (p - 1)/2 \). Then, for each non-principal character, mod \( p \), we have
\[
\left| \sum_{a=0}^{A} \sum_{n=A+1-a}^{A+1+a} \chi(n) \right| \leq p^{1/2} - \frac{A + 1}{p^{1/2}}.
\]

**Proof.** As in Lemma 1, we have
\[
\left| \sum_{a=0}^{A} \sum_{n=A+1-a}^{A+1+a} \chi(n) \right| = \left| \sum_{h=1}^{p-1} \bar{\chi}(h) e^{2\pi i h (A+1)p} \left( \frac{\sin (A + 1) \pi h/p}{\sin \pi h/p} \right)^2 \right|
\]
\[
\leq \sum_{h=1}^{p-1} \left( \frac{\sin (A + 1) \pi h/p}{\sin \pi h/p} \right)^2
\]
\[
= (A + 1)p - (A + 1)^2.
\]

**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 \( \chi \) 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 \( 1 \leq n < p \) there mentioned is not necessary.)

**Theorem 1.** We have \( |h(p)| < 2^n p^{1/2} \).

**Proof.** Let \( p > 2 \). By Lemma 3, we have
\[
0 = \sum_{k | p-1} \frac{\mu(k)}{\phi(k)} \sum_{\chi(k)} \chi^{(k)}(n).
\]
For \( k = 1 \), the right-hand side gives

License or copyright restrictions may apply to redistribution; see https://www.ams.org/journal-terms-of-use
On the other hand, for \( k \neq 1 \), we have, by Lemma 1 with \( A = \lvert h(p) \rvert - 1 \),

\[
\sum_{a=0}^{\lvert h(p) \rvert - 1} \sum_{n=-a}^a \chi^{(k)}(n) \leq \lvert h(p) \rvert \sqrt{p} - \frac{\lvert h(p) \rvert^2}{p^{1/2}}.
\]

Therefore

\[
\lvert h(p) \rvert^2 - \lvert h(p) \rvert \leq \left( \lvert h(p) \rvert \sqrt{p} - \frac{\lvert h(p) \rvert^2}{p^{1/2}} \right) \sum_{k \mid p-1} \frac{\mu(k)}{\phi(k)} \phi(k)
\]

\[
= 2^m \left( \lvert h(p) \rvert \sqrt{p} - \frac{\lvert h(p) \rvert^2}{p^{1/2}} \right).
\]

Then

\[
\lvert h(p) \rvert \leq \frac{2^m p^{1/2} + 1}{1 + 2^m p^{1/2}} < 2^m p^{1/2}.
\]

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

**Proof.** We have to show that \( \lvert h(p) \rvert \) is a primitive root. Suppose it is not. Then \( -\lvert h(p) \rvert \) is a primitive root and \( \lvert h(p) \rvert \) belongs to an exponent \( l \) where \( l \mid (p-1) \) and \( l < p-1 \), that is,

\[
\lvert h(p) \rvert^l \equiv 1 \pmod{p},
\]

\[
(h(p))^{2l} \equiv 1 \pmod{p}.
\]

Thus \( 2l = p-1 \) and \( \lvert h(p) \rvert^{(p-1)/2} \equiv 1 \pmod{p} \) so that \( \lvert h(p) \rvert \) is a quadratic residue. Since \( -1 \) is a quadratic residue, \( \pmod{p} \), \( -\lvert h(p) \rvert \) 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 \( p \equiv 3 \pmod{4} \),

\[
\lvert h(p) \rvert < 2^{m-1} p^{1/2}.
\]

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

\[
-1 = \chi^{(k)}(\chi^{(p-1)/2}) = e^{2\pi i (p-1)k / j},
\]
we have \(2^{\lfloor(p-1)/2\rfloor}\lambda/k\). 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 \(2\lambda\). Thus

\[
\sum_{a=0}^{2^{\lfloor(p-1)/2\rfloor}-1} \sum_{n=-a}^{a} \chi^{(k)}(n) = 0 \quad \text{for } 2 \mid k.
\]

Therefore

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

Then

\[
|h(p)| \leq \frac{2^{m-1}p^{1/2} + 1}{1 + 2^{m-1}/p^{1/2}} < 2^{m-1}p^{1/2}.
\]

**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

\[
0 = \sum_{k \mid (g - 1)/2} \phi(k) \sum_{A} \sum_{a=0}^{A} \sum_{n=A+1-a}^{A+1-a} \chi^{(k)}(n).
\]

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

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

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

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

\[
(g - 1)/2 < A + 1 \leq \frac{2^m p^{1/2}}{1 + 2^m/p^{1/2}},
\]

that is,

\[
g \leq \frac{2^{m-1}p^{1/2}}{1 + 2^m/p^{1/2}} + 1 < 2^{m+1}p^{1/2}.
\]