A note on a recent paper of U. V. Linnik and A. I. Vinogradov by
P. D. T. A. Elliott (Nottingham)

In a recent paper [3], U. V. Linnik and A. I. Vinogradov proved that $r_{1}(p)$, the least prime quadratic residue (mod $p$), satisfies

$$r_{1}(p) \ll p^{1+\varepsilon}$$

for any fixed positive value of $\varepsilon$. It is the purpose of the present note to show that, with a simple additional argument, one may prove a conditionally stronger result.

Let $L(s, \chi)$ denote the Dirichlet series formed with the Lagendre symbol (mod $p$). Then we make the following

**Hypothesis.**

$$L(1, \chi) > \frac{c_1 (\log \log p)^k}{\log p},$$

where $c_1$ is a positive constant, and $k$ is a non-negative integer.

The estimation of $L(1, \chi)$ from below is important in many parts of number theory. Here we note that J. E. Littlewood [5] proved that, if an extended form of the Riemann hypothesis holds, then

$$L(1, \chi) > \frac{c_2}{\log \log p}.$$  

Indeed, with trivial modifications his proof shows that if

$$L(s, \chi) = 0, \quad \text{Re} s > 1 - \theta(p), \quad \theta(p) > 0,$$

then

$$L(1, \chi) > \frac{c_3 \theta(p)}{\log \log p}.$$  

Hence a sufficient condition that our hypothesis should hold, is that

$L(s, \chi)$ does not vanish in the region

$$\text{Re} s > 1 - \frac{c_4 (\log \log p)^{k+1}}{\log p}.$$
The result which we now prove is the

**Theorem.** Let \( L(1, \chi) \) satisfy the hypothesis with a constant \( c_0 > c_0 \). Then for any fixed \( \varepsilon > 0 \),

\[
r_2(p) \ll p^{(1+\varepsilon)(\log p)^{2}}.
\]

The constant \( c_0 \) is absolute and effective.

Before giving the proof we mention that if we assume that we may take \( \theta(p) = 1 \), then N. C. Ankeny [1] showed that \( n_2(p) \), the least prime quadratic non-residue \((\mod p)\), satisfied

\[
n_2(p) < (\log p)^{2}.
\]

The same proof gives a corresponding result for \( r_2(p) \). The novelty of the present result lies in the comparative weakness of the hypothesis.

**Proof.** We begin with a result of Linnik and Vinogradov, namely that

\[
\sum_{n=1}^{N} \left(1 - \frac{n}{x}\right) \sum_{d \mid n} \mu^2(d)2(d) = \frac{3}{\pi^{2}} xL(1, \chi) + O(xp^{-\varepsilon})
\]

holds uniformly for \( x \) satisfying \( x^{1+\varepsilon} < x < x^{2\varepsilon} \), with a certain \( \delta = \delta(\varepsilon) > 0 \). Actually they give a sketch of a similar result, pointing out such changes as are necessary in order to prove (1). The method rests heavily upon a result of D. A. Burgess [2] concerning character sums. This states that, in the present case, for any fixed \( \varepsilon > 0 \) there is an \( \eta = \eta(\varepsilon) > 0 \), so that for all \( H > x^{1+\varepsilon} \),

\[
\sum_{m \leq H} \mu(m) = op^{-\varepsilon}H.
\]

Since we know by Siegel's theorem [9] that \( L(1, \chi) > o(H)H^{-1} \), we see from (1) that for all large \( \delta \) we have

\[
\sum_{n=1}^{N} \left(1 - \frac{n}{x}\right) \sum_{d \mid n} \mu^2(d)2(d) > \frac{x}{6} L(1, \chi).
\]

For the application which they have in mind the result is therefore not effective. However it clearly will be in our case provided that the hypothesis holds for an effective \( c_0 \).

Consider now the integers \( n < x \) for which \( \nu(n) \), the number of distinct prime divisors of \( n \), is \( n \). It was proved by Hardy and Ramanujan [4], that the number of these does not exceed

\[
\frac{1}{(m-1)!} \left( \frac{c_0x}{\log x} + c_1 \right)^{m-1} \leq \frac{c_0x}{\log x} \frac{(c_0 \log x)^{m-1}}{(m-1)!}.
\]

Thus

\[
\sum_{m \leq x} \left(1 - \frac{m}{x}\right) \sum_{d \mid m} \mu^2(d)2(d) \ll \frac{2c_0x}{\log x} \sum_{m \leq x} \frac{(2c_0 \log x)^{m-1}}{(m-1)!} \ll \frac{2c_0x}{\log x} \sum_{n \leq x} \frac{(2c_0)^{n}}{n!} < \frac{x}{12} L(1, \chi)
\]

if \( x = p^{1+\varepsilon} \), and \( c_0 \) is sufficiently large.

From this and (2) it follows that

\[
\sum_{n \leq x} \left(1 - \frac{n}{x}\right) \mu^2(d)2(d) > \frac{x}{12} L(1, \chi) > 0.
\]

Thus we can find an integer \( \psi \), not exceeding \( x \), for which

\[
\int_{0}^{x} \mu^2(d)2(d) \neq 0.
\]

All of its prime divisors \( \psi \) must therefore be quadratic residues \((\mod p)\). There are more than \( \psi + 1 \) of them however, and so at least one does not exceed \( p^{1+\varepsilon} \). This completes the proof of the theorem.

**References**


**University of Nottingham**

**Reçu par la Rédaction le 15. 10. 1966**