ACTA ARITHMETICA
XIII (1967)

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 $r_2(p)$, the least prime quadratic residue $(\bmod p)$, satisfies

$$r_2(p) \ll p^{1/4+\varepsilon}$$

for any fixed positive value of ε. 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 $(\bmod p)$. 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

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

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

$$\operatorname{Re} s > 1 - \frac{c_4(\log\log p)^{k+1}}{\log p}.$$

The result which we now prove is the

THEOREM. *Let $L(1,\chi)$ satisfy the hypothesis with a constant $c_1 > c_0$. Then for any fixed $\varepsilon > 0$,*

$$r_2(p) \ll p^{\frac{1}{4}(1+\varepsilon)/(k+2)}.$$

The constant c_0 is absolute and effective.

Before giving the proof we mention that if we assume that we may take $\theta(p) = \frac{1}{2}$, then N. C. Ankeny [1] showed that $n_2(p)$, the least prime quadratic non-residue $(\bmod p)$, satisfied

$$n_2(p) \ll (\log p)^2.$$

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

$$\sum_{n<x}\left(1-\frac{n}{x}\right)\sum_{d|n}\mu^2(d)\chi(d) = \frac{3}{\pi^2}xL(1,\chi)+O(xp^{-\delta}) \tag{1}$$

holds uniformly for x satisfying $p^{1/4+\varepsilon} < x \leqslant p^{1/2}$, 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 $H > p^{1/4+\varepsilon}$,

$$\Big|\sum_{m<H}\chi(m)\Big| < cp^{-\eta}H.$$

Since we know by Siegels' theorem [6] that $L(1,\chi) > c(\delta)p^{-\frac{1}{2}\delta}$, we see from (1) that for all large primes p,

$$\sum_{n<x}\left(1-\frac{n}{x}\right)\sum_{d|n}\mu^2(d)\chi(d) > \frac{x}{6}L(1,\chi). \tag{2}$$

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_1.

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

$$\frac{1}{(m-1)!}\cdot\frac{c_5x}{\log x}(\log\log x + c_6)^{m-1} < \frac{c_5x}{\log x}\cdot\frac{(c_4\log\log x)^{m-1}}{(m-1)!}.$$

Thus

$$\sum_{\substack{n<x\\ \nu(n)\leqslant k+1}}\left(1-\frac{n}{x}\right)\sum_{d|n}\mu^2(d)\chi(d) < \frac{2c_5x}{\log x}\sum_{m=1}^{k+1}\frac{(2c_4\log\log x)^{m-1}}{(m-1)!}$$

$$< \frac{2c_5x(\log\log x)^k}{\log x}\sum_{m=0}^{\infty}\frac{(2c_1)^m}{m!} < \frac{x}{12}L(1,\chi)$$

if $x = p^{1/4+\varepsilon}$, and c_1 is sufficiently large.

From this and (2) it follows that

$$\sum_{\substack{n<x\\ \nu(n)>k+1}}\left(1-\frac{n}{x}\right)\mu^2(d)\chi(d) > \frac{x}{12}L(1,\chi) > 0.$$

Thus we can find an integer n, not exceeding x, for which

$$\prod_{q|n}\big(1+\chi(q)\big) = \sum_{d|n}\mu^2(d)\chi(d) \neq 0.$$

All of its prime divisors q must therefore be quadratic residues $(\bmod p)$. There are more than $k+1$ of them however, and so at least one does not exceed $x^{1/(k+2)}$. This completes the proof of the theorem.

References

[1] N. C. Ankeny, *The least quadratic non-residue*, Ann. Math. 55 (1952), pp. 65-72.

[2] D. A. Burgess, *On character sums and primitive roots*, Proc. Lond. Math. Soc. (3) 12 (1962), pp. 179-192.

[3] А. И. Виноградов и Ю. В. Линник, *Гиперэллиптические кривые и наименьший простой квадратный вичет*, Докл. Акад. Наук СССР 168 (2) (1966), pp. 259-261.

[4] G. H. Hardy and S. Ramanujan, *The normal number of prime factors of a number n*, Quart. J. Math. 48 (1917), pp. 76-92. See also: *Collected papers of S. Ramanujan*, Cambridge 1927, pp. 262-275.

[5] J. E. Littlewood, *On the class number of the corpus $P(\sqrt{-k})$*, Proc. Lond. Math. Soc. (2) 27 (1927), pp. 358-372.

[6] K. Prachar, *Primzahlverteilung*, Berlin 1957, pp. 145-146.

UNIVERSITY OF NOTTINGHAM

Reçu par la Rédaction le 13. 10. 1966