ACTA ARITHMETICA
XXXII (1977)

Elementary methods in the theory of L-functions, VI
On the least prime quadratic residue $(\bmod p)$

by

J. Pintz (Budapest)

1. I. M. Vinogradov conjectured more than 50 years ago, that the least prime quadratic residue $\bmod p$ (p is a prime)

$$P(p) < c(\varepsilon)p^{\varepsilon} \tag{1.1}$$

where ε is an arbitrary positive number and $c(\varepsilon)$ a constant depending on ε.

Yu. V. Linnik and A. I. Vinogradov proved in 1964 [5], that

$$P(p) < c(\varepsilon)p^{1/4+\varepsilon} \quad (\varepsilon > 0). \tag{1.2}$$

The somewhat roughly outlined proof uses complex integration, Burgess's inequality [1], and Siegel's lower bound [7] for $L(1, \chi)$.

Conditional results connecting the hypothesis of I. M. Vinogradov mentioned above with the value of $L(1, \chi_p)$ — where $\chi_p(n) = (n/p)$ — were achieved by Linnik and Rényi [4], P. D. T. A. Elliott [2] and D. Wolke [8].

Linnik and Rényi showed that if $P(p) > p^{1/k}$ then

$$L(1, \chi_p) = \sum_{n=1}^{\infty} \frac{\left(\frac{n}{p}\right)}{n} \ll 1. \tag{1.3}$$

On the same condition Elliott proved

$$L(1, \chi_p) \ll \frac{(\log\log p)^k}{\log p}, \tag{1.4}$$

Wolke proved

$$L(1, \chi_p) \ll \frac{k^2}{\log p}. \tag{1.5}$$

The results of Elliott and Wolke were based on a lemma, which is the essential part of the work of Linnik and A. I. Vinogradov [5], mentioned above in which they proved the inequality

$$P(p) < c(\varepsilon)p^{1/4+\varepsilon}.$$

Besides this, Elliott uses a result of Hardy and Ramanujan [3], concerning the number of the natural numbers less than x and having exactly ν distinct prime divisors. Wolke applies Brun's sieve method in order to prove

$$\sum_{\substack{n\leqslant x\\ p|n\to p\geqslant y}} 2^{\nu(n)} \leqslant \frac{x\log x}{\log^2 y}.$$

Now we shall demonstrate that one can derive Linnik and A. I. Vinogradov's [5] result from Burgess's inequality and Siegel's theorem in a simple elementary way (which, however, is somewhat similar to the non-elementary original proof [5]). We shall also give a simple, elementary proof for Wolke's result in which besides a lemma, proved in [6] in an elementary way, we use only the relation

$$\sum_{n\leqslant A}\frac{d(n)}{n} = \left(\frac{1}{2}+o(1)\right)\log^2 A. \tag{1.6}$$

So we state

THEOREM 1. *For an arbitrary positive ε there is an ineffective constant $p_0(\varepsilon)$, depending only on ε, that the least prime quadratic residue $P(p)$* (mod p) *(where p is a prime)*

$$P(p) < p^{1/4+\varepsilon} \quad \textit{if} \quad p > p_0(\varepsilon). \tag{1.7}$$

THEOREM 2. *If the least prime quadratic residue* (mod p) *(where p is a prime)*

$$P(p) > p^{\varepsilon} \geqslant P_0 \tag{1.8}$$

(where $\varepsilon \leqslant \frac{1}{2}$, P_0 is an absolute constant), then the inequality

$$L(1,\chi_p) = \sum_{n=1}^{\infty}\left(\frac{n}{p}\right)n^{-1} \leqslant \frac{24}{\varepsilon^2\log p} \tag{1.9}$$

holds.

2. To prove Theorem 1 we use Burgess's inequality [1], according to which if p is a prime, r an integer, and $\chi(d) = (d/p)$ then the inequality

$$\left|\sum_{d=N+1}^{N+H}\chi(d)\right| \leqslant C(r)H^{1-\frac{1}{r}}p^{\frac{r+1}{4r^2}}\log p \tag{2.1}$$

holds, where $C(r)$ is a constant depending on r.

Further we use Siegel's theorem [7], which states, that for an arbitrary $\eta > 0$ and for a real non-principal character χ (mod D)

$$L(1,\chi) > c(\eta)D^{-\eta} \tag{2.2}$$

with a constant $c(\eta)$ depending only on η.

We shall assume that for $0 < \varepsilon < \frac{1}{4}$

$$P(p) > x = p^{1/4+\varepsilon} \tag{2.3}$$

(where $p > p_0(\varepsilon)$).

Let $r = \left[\frac{1}{2\varepsilon}\right]$,

$$g(n) = \sum_{d|n}\chi(d) = \prod_{p_i^{\alpha_i}\|n}\left(1+\chi(p_i)+\ldots+\chi^{\alpha_i}(p_i)\right) \tag{2.4}$$

and further

$$A = C(r)x^{1-\frac{1}{r}}p^{\frac{r+1}{4r^2}}\log p \leqslant x, \quad y = \sqrt{Ax} \leqslant x \tag{2.5}$$

(if $p > p_0(\varepsilon)$).

Then we see from (2.3) and (2.4), that for $n \leqslant x$

$$g(n) = \begin{cases}1, & \text{if} \quad n = l^2,\\ 0, & \text{if} \quad n \neq l^2.\end{cases} \tag{2.6}$$

So we have

$$[\sqrt{x}] = \sum_{n\leqslant x}g(n) = \sum_{d\leqslant x}\chi(d)\left[\frac{x}{d}\right] = x\sum_{d\leqslant x}\frac{\chi(d)}{d} - \sum_{d\leqslant x}\chi(d)\left\{\frac{x}{d}\right\}. \tag{2.7}$$

Here using (2.1) and Abel's inequality we get the inequality

$$\left|\sum_{d\leqslant x}\chi(d)\left\{\frac{x}{d}\right\}\right| \leqslant \left|\sum_{d\leqslant y}\chi(d)\left\{\frac{x}{d}\right\}\right| + \sum_{m\leqslant\frac{x}{y}}\left|\sum_{\left[\frac{x}{d}\right]=m}\chi(d)\left\{\frac{x}{d}\right\}\right| \tag{2.8}$$

$$\leqslant y + \frac{x}{y}A = \sqrt{Ax}+\sqrt{Ax} = 2\sqrt{Ax}.$$

On the other hand (2.1) gives

$$|S_x(u)| = \left|\sum_{x<d\leqslant u}\chi(d)\right| \leqslant C(r)u^{1-\frac{1}{r}}p^{\frac{r+1}{4r^2}}\log p \tag{2.9}$$

and so by partial summation we get the inequality

$$\left|\sum_{d>x}\frac{\chi(d)}{d}\right| = \left|\int_x^{\infty}\frac{S_x(u)}{u^2}\,du\right| \leqslant \int_x^{\infty}\frac{u^{1-\frac{1}{r}}}{u^2}C(r)p^{\frac{r+1}{4r^2}}\log p\,du \tag{2.10}$$

$$= rC(r)x^{-\frac{1}{r}}p^{\frac{r+1}{4r^2}}\log p = r\frac{A}{x}.$$

Thus from (2.7), (2.8) and (2.10) follows

$$(2.11)\qquad \sqrt{x} \geqslant \sum_{n\leqslant x} g(n) \geqslant xL(1,\chi) - rA - 2\sqrt{Ax}.$$

Hence as

$$A \leqslant x \quad \text{and} \quad \frac{1}{3\varepsilon} \leqslant r = \left[\frac{1}{2\varepsilon}\right] \leqslant \frac{1}{2\varepsilon}$$

we have

$$(2.12)\qquad L(1,\chi) \leqslant (r+3)\sqrt{\frac{A}{x}} = (r+3)\sqrt{C(r)\log p}\sqrt{\frac{p^{\frac{r+1}{4r^2}}}{p^{\frac{1}{4r}+\frac{\varepsilon}{r}}}}$$

$$< C'(r)\sqrt{\log p}\,p^{-\frac{1}{2r}\left(\varepsilon - \frac{1}{4r}\right)} < c(\varepsilon)\sqrt{\log p}\,p^{-\varepsilon\cdot\frac{\varepsilon}{4}},$$

which contradicts to Siegel's theorem (2.2) (with $\eta = \varepsilon^2/5$) if p exceeds a certain ineffective constant $p_0(\varepsilon)$.

3. To prove Theorem 2 we use Lemma 1 of [6]:

LEMMA. *If χ is a real non-principal character* mod D, $x \geqslant \sqrt{D}\log^2 D$, $g(n) = \sum_{d|n}\chi(d)$, *then the equality*

$$(3.1)\qquad \sum_{n\leqslant x}\frac{g(n)}{n} = L'(1,\chi) + L(1,\chi)(\log x + c) + O\left(\sqrt{\frac{\sqrt{D}\log D\log x}{x}}\right)$$

holds, where c denotes Euler's constant.

If we use this for $\chi(n) = \left(\frac{n}{p}\right)$ $(D = p)$ and for the values $x_1 = p$, $x_2 = p^2$, subtracting the first equality from the second we have the equality

$$(3.2)\qquad \sum_{p<n\leqslant p^2}\frac{g(n)}{n} = \log p\cdot L(1,\chi_p) + o(1).$$

On the other hand if $P(p) > p^\varepsilon$ (where $0 < \varepsilon \leqslant \frac{1}{2}$) we assert the inequality

$$(3.3)\qquad \sum_{\substack{q\leqslant p^\varepsilon\\ \mu(q)\neq 0}}\frac{d(q)}{q}\sum_{p<n\leqslant p^2}\frac{g(n)}{n} \leqslant \sum_{p<m\leqslant p^{2+\varepsilon}}\frac{d(m)}{m}$$

where $d(m)$ is the number of divisors of m.

To prove (3.3) first we show that an arbitrary integer m, for which $p < m \leqslant p^{2+\varepsilon}$ can be written in at most one way in the form $m = qn$,

where $q \leqslant p^\varepsilon$, $\mu(q) \neq 0$ and $g(m) \neq 0$. Indeed, if

$$(3.4)\qquad g(n) = \prod_{p_i^{a_i}\|n}\left(1 + \chi(p_i) + \ldots + \chi^{a_i}(p_i)\right) \neq 0$$

then for all the prime factors p_i of n with the property $\chi(p_i) = -1$ and so for all $p_i \leqslant p^\varepsilon$, a_i must be even, so if $m = l^2 t$ $(\mu(t) \neq 0)$ then necessarily

$$(3.5)\qquad q = \prod_{\substack{p_i|t\\ p_i\leqslant p^\varepsilon}} p_i \quad \text{and} \quad n = l^2\prod_{\substack{p_j|t\\ p_j>p^\varepsilon}} p_j.$$

We can also see from (3.4) that if $n = ab$, where $p_i|a \to p_i > p^\varepsilon$ and $p_i|b \to p_i \leqslant p^\varepsilon$, then since $g(n)$ is multiplicative and $g(b) = 0$ or 1 (see (3.4)) we have

$$0 \leqslant g(n) = g(a)g(b) \leqslant g(a) \leqslant d(a)$$

and thus the inequality

$$d(q)g(n) \leqslant d(q)d(a) = d(aq) \leqslant d(nq) = d(m)$$

holds, which proves (3.3).

We shall further use the relation

$$(3.6)\qquad \sum_{m=1}^{\infty}\frac{d(m^2)}{m^2} = \prod_p\left(1 + \frac{1}{p^2}\right)\left(\sum_{n=1}^{\infty}\frac{1}{n^2}\right) = c_0 < \frac{32}{7}.$$

Hence as $d(uv) \leqslant d(u)d(v)$, we have

$$(3.7)\qquad c_0\sum_{\substack{q\leqslant p^\varepsilon\\ \mu(q)\neq 0}}\frac{d(q)}{q} > \sum_{\substack{q\leqslant p^\varepsilon\\ \mu(q)\neq 0}}\frac{d(q)}{q}\sum_{m^2\leqslant p^\varepsilon/q}\frac{d(m^2)}{m^2} > \sum_{r\leqslant p^\varepsilon}\frac{d(r)}{r}.$$

So using (1.6) from the formulae (3.2), (3.3), (3.6) and (3.7) we get the inequality

$$(3.8)\qquad \log p\cdot L(1,\chi_p) + o(1)$$

$$= \sum_{p<n\leqslant p^2}\frac{g(n)}{n} \leqslant c_0\left(\sum_{p<m\leqslant p^{2+\varepsilon}}\frac{d(m)}{m}\right)\left(\sum_{r\leqslant p^\varepsilon}\frac{d(r)}{r}\right)^{-1}$$

$$= \frac{c_0\left(\frac{1}{2}\left[(2+\varepsilon)^2 - 1\right] + o(1)\right)\log^2 p}{\left(\frac{1}{2} + o(1)\right)\varepsilon^2\log^2 p} \leqslant \frac{c_0\left(\frac{21}{4} + o(1)\right)}{\varepsilon^2}.$$

Hence

$$(3.9)\qquad L(1,\chi_p) \leqslant \frac{c_0\left(\frac{21}{4} + o(1)\right)}{\varepsilon^2\log p} < \frac{24}{\varepsilon^2\log p}. \blacksquare$$

References

[1] D. A. Burgess, *On character sums and L-series I*, Proc. London Math. Soc. 12 (1962), pp. 179–192.
[2] P. D. T. A. Elliott, *A note on a recent paper of U. V. Linnik and A. I. Vinogradov*, Acta Arith. 13 (1967), pp. 103–106.
[3] G. H. Hardy and S. Ramanujan, *The normal number of prime factors of a number n*, Quart. J. Math. 48 (1917), pp. 76–92.
[4] Yu. V. Linnik and A. Rényi, *On some hypothesis of the theory of Dirichlet characters* (in Russian), Izv. Akad. Nauk 11 (1947), pp. 539–546.
[5] Yu. V. Linnik and A. I. Vinogradov, *Hyperelliptic curves and the least prime quadratic residue* (in Russian), Dokl. Akad. Nauk 168 (2) (1966), pp. 259–261.
[6] J. Pintz, *Elementary methods in the theory of L-functions, II. On the greatest real zero of a real L-function*, Acta Arith. 31(1976), pp. 273–289.
[7] C. L. Siegel, *Über die Classenzahl quadratischer Zahlkörper*, ibid., 1 (1935), pp. 83–86.
[8] D. Wolke, *A note on the least prime quadratic residue* (mod p), ibid., 16 (1969), pp. 85–87.

EÖTVÖS LORÁND UNIVERSITY
DEPARTMENT OF ALGEBRA AND NUMBER THEORY
Budapest, Hungary

Received on 8. 9. 1975 (763)

ACTA ARITHMETICA
XXXII (1977)

Values of integer-valued multiplicative functions in residue classes

by

W. Narkiewicz (Wrocław)

1. An integer-valued arithmetical function f is said to be *weakly uniformly distributed* (mod N) [WUD (mod N)] provided the set $\{n: (f(n), N) = 1\}$ is infinite and the values of f prime to N are asymptotically uniformly distributed in residue classes (mod N) prime to N. This notion was studied in [2] in the case of polynomial-like multiplicative functions (i.e. functions f satisfying the condition $f(p^k) = W_k(p)$ for every prime p, $k = 1, 2, \ldots$ with suitable $W_k(x) \in Z[x]$) and a necessary and sufficient condition for such a function to be WUD (mod N) was found. This condition makes sense for arbitrary integer-valued multiplicative functions and it was shown in [3] that it is equivalent to the Dirichlet-weakly uniform distribution (mod N) of f, which seems to be essentially weaker than WUD (mod N).

The purpose of this note is to show that for an important class of multiplicative functions WUD (mod N) and Dirichlet-WUD (mod N) coincide and so in view of [3] a necessary and sufficient condition for f from that class to be WUD (mod N) results.

2. We shall consider integer-valued multiplicative functions f from the class F_N consisting of all functions of this type for which the series

$$\sum_{\substack{p \\ (f(p),N)>1}} \frac{1}{p}$$

converges.

We need a lemma, which for $r = 1$ is a special case of Theorem 1 of [1] whose proof carries without any change to our case, being a simple application of a theorem of E. Wirsing [4]:

Lemma. *Let for $k = 1, 2, \ldots, r$ f_k be an integer-valued additive function, $N_k \geq 2$ an integer and j_k an integer prime to N_k. Let $S = S(f_1, \ldots, f_r; N_1, \ldots, N_r; j_1, \ldots, j_r)$ be the set of all integers $n \geq 1$ for which*

$$f_k(n) \equiv j_k \pmod{N_k}$$