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

by

J. Pintz (Budapest)

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

\[ P(p) < c(\varepsilon)p^{\varepsilon} \]

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

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

\[ P(p) < c(\varepsilon)p^{1/4+\varepsilon} \quad (\varepsilon > 0). \]

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 [3] and D. Wolke [8].

Linnik and Rényi showed that if $P(p) > p^{1/2}$ then

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

On the same condition Elliott proved

\[ L(1, \chi_p) \ll \left( \frac{\log \log p}{\log p} \right)^{3/2}, \]

Wolke proved

\[ L(1, \chi_p) \ll \frac{L^2}{\log p}. \]

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

\[ P(p) < c(\varepsilon)p^{1/2+\varepsilon}. \]
Besides this, Elliott uses a result of Hardy and Ramanujan [3], concerning the number of the natural numbers less than \( x \) and having exactly \( r \) distinct prime divisors. Wolke applies Brun's sieve method in order to prove

\[
\sum_{p \leq \sqrt{x}} 2^{v(p)} \ll \frac{x \log x}{\log^2 x}.
\]

Now we shall demonstrate that one can derive Linnik and A. I. Vinogradov's [6] 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

\[
\sum_{n \leq x} \frac{d(n)}{n} = \left( \frac{1}{2} + o(1) \right) \log^2 A.
\]

So we state

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

\[
P(p) < p^{1/4+\varepsilon} \quad \text{if} \quad p > p_0(\varepsilon).
\]

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

\[
P(p) > p^\varepsilon \gg P_0(\varepsilon)
\]

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

\[
L(1, \chi_p) = \sum_{p \leq x} \left( \frac{n}{p} \right) n^{-1} \ll \frac{24}{\varepsilon^3 \log p}
\]

holds.

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

\[
\left| \sum_{d \leq x} \chi(d) \right| \leq C(r) x^{1 - \frac{1}{r}} p^{\frac{r+1}{r}} \log x
\]

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 \( \chi \) (mod \( D \))

\[
L(1, \chi) > c(\eta) D^{-\eta}
\]

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

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

\[
P(p) > \varepsilon = p^{1/4+\varepsilon}
\]

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

Let \( r = \left\lceil \frac{1}{2 \varepsilon} \right\rceil \)

\[
g(n) = \sum_{d \mid n} \chi(d) = \prod_{p \mid n} \left( 1 + \chi(p) + \cdots + \chi^r(p) \right)
\]

and further

\[
A = C(r) x^{1 - \frac{1}{r}} p^{\frac{r+1}{r}} \log p \leq x, \quad y = \sqrt{A x} \leq x
\]

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

Then we see from (2.3) and (2.4), that for \( \eta \leq x \)

\[
g(n) = \begin{cases} 1, & \text{if } n = 1, \\ 0, & \text{if } n \neq 1, \end{cases}
\]

so we have

\[
\lvert \sum_{d \leq x} \chi(d) \rvert \leq \sum_{d \leq \sqrt{x}} \chi(d)^2 \leq A
\]

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

\[
\left| \sum_{d \leq x} \chi(d) \frac{x}{d} \right| \leq \left| \sum_{d \leq x} \chi(d) \frac{a}{d} \right| + \sum_{n \leq \sqrt{x}} \left| \sum_{d \leq \sqrt{x}} \chi(d) \frac{x}{d} \right|
\]

\[
\leq y + \frac{x}{y} A = \sqrt{A x} + \sqrt{A x} = 2 \sqrt{A x}.
\]

On the other hand (2.1) gives

\[
\left| \sum_{d \leq x} \chi(d) \rvert \leq C(r) x^{1 - \frac{1}{r}} p^{\frac{r+1}{r}} \log p
\]

and so by partial summation we get the inequality

\[
\left| \sum_{d \geq x} \chi(d) \frac{1}{d} \right| = \left| \int_x^\infty \frac{S_x(u)}{u^3} \, du \right| \leq \int_x^\infty \frac{1}{u^3} C(r) p^{\frac{r+1}{r}} \log p \, du
\]

\[
= r C(r) x^{1 - \frac{1}{r}} p^{\frac{r+1}{r}} \log p = \frac{r A}{x}.
\]
Thus from (2.7), (2.8) and (2.10) follows

\[ V_x \geq \sum_{n \leq x} g(n) \geq xL(1, \chi) - xA - 2xyA. \]

Hence as

\[ A \leq x \quad \text{and} \quad \frac{1}{3e} \leq r = \left[ \frac{1}{2e} \right] \leq \frac{1}{2e}, \]

we have

\[ L(1, \chi) \leq (r + 3) \sqrt{\frac{x}{A}} = (r + 3)\sqrt{\frac{1}{x}} \leq \frac{1}{x}, \]

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

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

**Lemma.** If \( \chi \) is a real character modulo \( D \), \( x \geq \sqrt{D} \log^2 x \),

\[ g(n) = \sum_{d \mid n} \chi(d), \]

then the equality

\[ \sum_{\substack{n \leq x \leq 2x \leq p^2 \leq n}} \frac{g(n)}{n} = L'(1, \chi) + L(1, \chi)(\log x + o(1)) + O\left( \sqrt{\log D \log x} \right), \]

holds, where \( \omega \) 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

\[ \sum_{p < x \leq p^2} \frac{g(n)}{n} = \log p \cdot L(1, \chi_p) + o(1). \]

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

\[ \sum_{\substack{q < p \leq x \leq p^2 \leq q^2 \leq p^2 \leq r \leq \infty}} \frac{d(q)}{q} \cdot \sum_{\substack{n \leq p \leq q^2 \leq p^2 \leq x}} \frac{g(n)}{n} \leq \sum_{p < x \leq p^2} \frac{d(m)}{m}, \]

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

To prove (3.3) first we show that an arbitrary integer \( m \), for which \( p < m \leq p^{1+\varepsilon} \) can be written in at most one way in the form \( m = gn \),

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

\[ g(n) = \prod_{\substack{p \mid n \neq p^e \neq n}} (1 + \chi(p_i) + \ldots + \chi^{e}(p_i)) = 0, \]

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

\[ \prod_{p_i \neq p^e} P t \quad \text{and} \quad n = \prod_{p_i \neq p^e} P t, \]

We can also see from (3.4) that if \( n = ab \), where \( p_i \mid a \Rightarrow p_i > p^e \) and \( p_i \mid b \Rightarrow p_i \leq p^e \), then since \( g(n) \) is multiplicative and \( g(b) = 0 \) or 1 (see (3.4)) we have

\[ 0 \leq g(n) = g(a)g(b) \leq g(a) \leq p^e \]

and thus the inequality

\[ d(q)g(n) \leq d(q)d(a) = d(aq) \leq d(an) = d(m) \]

holds, which proves (3.3).

We shall further use the relation

\[ \sum_{a=1}^{\infty} \frac{d(m^2)}{m^2} = \prod_{p} \left( 1 + \frac{1}{p^2} \right) \left( \sum_{n=1}^{\infty} \frac{1}{n^2} \right) = c_0 \frac{\zeta(2)}{\zeta(2) - 1} \]

Hence as \( d(n) \leq d(n)d(n) \), we have

\[ c_0 \sum_{p^e \leq p \leq x} \frac{d(q)}{q} > \sum_{\substack{q < p \leq x \leq p^2 \leq m \leq \infty}} \frac{d(m)}{m^2} > \sum_{\substack{q < p \leq x \leq p^2 \leq \infty}} \frac{d(r)}{r}. \]

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

\[ \log p \cdot L(1, \chi_p) + o(1) \]

\[ = \sum_{p < x \leq p^2} \frac{g(n)}{n} \leq c_0 \left( \sum_{p < m < p^2} \frac{d(m)}{m} \right) \left( \sum_{r < p^2} \frac{d(r)}{r} \right)^{-1} \]

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

Hence

\[ L(1, \chi_p) \leq \frac{c_0}{\varepsilon^4 \log^2 p} < \frac{24}{\varepsilon^4 \log p}. \]
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 $W_k(x) \in \mathbb{Z}[x]$) 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 $\mathcal{F}_N$ consisting of all functions of this type for which the series

$$\sum_{(p, N_k) = 1} \frac{1}{p}$$

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 $f_k$ 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

$$f_k(n) = j_k (\text{mod } N_k)$$