ON THE BOUND OF THE LEAST NON-RESIDUE OF nth POWERS*

BY

J. M. VINOGRADOV

1. In my paper *On the distribution of residues and non-residues of powers* (Journal of the Physico-Mathematical Society of Perm, 1919) I demonstrated that the least quadratic non-residue of a prime p is less than

$$p^{1/2e^{1/2}}(\log p)^2$$

for all sufficiently great values of p.

Using the same method one can establish a more general theorem:

THEOREM I. *If p is a prime and n a divisor of the number $p-1$ distinct from 1, the least non-residue of nth powers modulo p is less than*

$$p^{1/2k}(\log p)^2\ ;\ k = e^{(n-1)/n}$$

for all sufficiently great values of p.

This bound may be considerably lowered, by means of very simple changes in our method. For example one can demonstrate the following theorems:

THEOREM II. *If p is a prime and n a divisor of the number $p-1$ greater than 20, the least non-residue of nth powers modulo p is less than $p^{1/6}$ for all sufficiently great values of p.*

THEOREM III. *If p is a prime and n a divisor of the number $p-1$ greater than 204, the least non-residue of nth powers modulo p is less than $p^{1/8}$ for all sufficiently great values of p.*

We prove finally the general theorem:

THEOREM IV. *If p is a prime and n a divisor of the number $p-1$ greater than m^m, where m is an integer $\geqq 8$, the least non-residue of nth powers modulo p is less than $p^{1/m}$ for all sufficiently great values of p.*

2. First we shall demonstrate Theorem I. We use the notations

$$P = p^{1/2}(\log p)^2\ ;\ T = p^{1/2k}(\log p)^2\ ;\ k = e^{(n-1)/n},$$

*Presented to the Society, September 9, 1926; received by the editors in January, 1926.

and assume that there are no non-residues of nth powers modulo p less than T. Then only numbers divisible by integers greater than T and less than P can be non-residues of nth powers less than P. But evidently, of such numbers, there are not more than

$$\sum_{q>T}^{q<P} \left[\frac{P}{q}\right],$$

where q runs only over primes. Using the known law of distribution of primes, we may bring this expression to the form

$$P \log \frac{\log P}{\log T} + O\left(\frac{P}{\log p}\right) = P\left[\frac{n-1}{n} + \log \frac{1 + \dfrac{4 \log\log p}{\log p}}{1 + \dfrac{4k \log\log p}{\log p}}\right] + O\left(\frac{P}{\log p}\right)$$

$$= \left(\frac{n-1}{n} + \frac{(4-4k)\log\log p}{\log p}\right) + O\left(\frac{P}{\log p}\right).$$

On the other hand, according to my previous work, the number of residues of nth powers modulo p in the range

$$1, 2, \cdots, [P]$$

may be given as follows:

$$\frac{[P]}{n} + \Delta\,;\ |\Delta| < p^{1/2} \log p.$$

Thus the number of non-residues in the same range may be expressed by the formula

$$P\left(\frac{n-1}{n}\right) + \rho\,;\ |\rho| < p^{1/2} \log p + 1.$$

Hence

$$P\left(\frac{n-1}{n}\right) + \rho \leqq P\left(\frac{n-1}{n} + \frac{(4-4k)\log\log p}{\log p}\right) + O\left(\frac{P}{\log p}\right)$$

which brings us to the inequality

$$(4k-4)\log\log p \leqq O(1),$$

which is impossible for sufficiently great p. This proves Theorem I.

3. To prove Theorem II, let

$$P = p^{1/2}(\log p)^2\ ;\ T = p^{1/6},$$

and assume that there are no non-residues of nth powers modulo p less than T. Then only numbers divisible by primes greater than T and less than P can be non-residues less than P. The number of such numbers is evidently equal to

$$(1)\qquad \sum_{q>T}^{q<P}\left[\frac{P}{p}\right] - \sum_{q>T}^{q<P^{1/2}}\ \sum_{q_1>q}^{q_1<P/q}\left[\frac{P}{qq_1}\right] + \sum_{q>T}^{q<P^{1/3}}\ \sum_{q_1>q}^{q_1<(P/q)^{1/2}}\ \sum_{q_2>q_1}^{q_2<P/qq_1}\left[\frac{P}{qq_1q_2}\right],$$

where q, q_1, q_2 run over primes.

But, according to the law of the distribution of primes, the first sum may be written

$$P\log\frac{\log P}{\log T} + O\left(\frac{P}{\log p}\right) = P\log 3 + O\left(\frac{P\log\log p}{\log p}\right),$$

which for sufficiently great p is less than

$$P\cdot 1.0987.$$

The second double sum may be put into the form

$$P\sum_{q>T}^{q<P^{1/2}}\frac{1}{q}\log\frac{\log(P/q)}{\log p} + O\left(\frac{P}{\log p}\right) = P\sum_{q>p^{1/6}}^{q<p^{1/4}}\frac{1}{q}\log\frac{\log p^{1/2}}{\log q} + O\left(\frac{P\log\log p}{\log p}\right).$$

But applying the law of distribution of primes we have

$$P\int_{p^{1/6}}^{p^{1/4}}\log\frac{\log(p^{1/2}/z)}{\log z}\cdot\frac{dz}{z\log z} + O\left(\frac{P\log\log p}{\log p}\right) = P\int_{1/3}^{1/2}\log\frac{1-u}{u}\cdot\frac{du}{u} + O\left(\frac{P\log\log p}{\log p}\right),$$

which, for p sufficiently great, is greater than

$$P\cdot 0.147.$$

The last triple sum evidently is a quantity of the order

$$P\frac{\log\log p}{\log p},$$

so that the expression (1) for sufficiently great p is less than

$$P(1.0988 - 0.147) = P \cdot 0.9518.$$

On the other hand, the number of non-residues of nth powers modulo p in the series

$$1, 2, \cdots, [P],$$

as seen in § 2, is equal to

$$P\left(1 - \frac{1}{n}\right) + O\left(\frac{P}{\log p}\right).$$

So, for p sufficiently great, we have the inequality

$$P\left(1 - \frac{1}{n}\right) < P \cdot 0.952.$$

The impossibility of this inequality for $n>20$ proves Theorem II.

4. To prove Theorem III we let

$$P = p^{1/2}(\log p)^2 \; ; \; T = p^{1/8},$$

and assume that there are no non-residues of nth powers, modulo p, less than T. It is easy to show that the number of such numbers is less than

$$(2) \quad \sum_{q>T}^{q<P} \left[\frac{P}{q}\right] - \sum_{q>T}^{q<P^{1/2}} \sum_{q_1>q}^{q_1<P/q} \left[\frac{P}{qq_1}\right] + \sum_{q>T}^{q<P^{1/3}} \sum_{q_1>q}^{q_1<(P/q)^{1/2}} \sum_{q_2>q_1}^{q_2<P/qq_1} \left[\frac{P}{qq_1q_2}\right],$$

where q, q_1, q_2 run over primes only.

Applying the known laws of distribution of primes, we can put this expression into the form

$$\sum_{q>p^{1/8}}^{q<p^{1/2}} \frac{P}{q} - \sum_{q>p^{1/8}}^{q<p^{1/4}} \sum_{q_1>q}^{q_1<p^{1/2}/q} \frac{P}{qq_1} + \sum_{q>p^{1/8}}^{q<p^{1/6}} \sum_{q_1>q}^{q_1<p^{1/4}/q^{1/2}} \sum_{q_2>q}^{q_2<p^{1/2}/qq_1} \frac{P}{qq_1q_2}$$
$$+ O\left(\frac{P \log\log p}{\log p}\right).$$

The first sum may be put into the form

$$P \log 4 + O\left(\frac{P}{\log p}\right)$$

which for sufficiently great p is less than

$$P \cdot 1.3863.$$

Then as in the proof of Theorem II the second double sum may be given in the form

$$P\int_{1/4}^{1/2} \log\frac{1-u}{u}\,\frac{du}{u} + O\left(\frac{P}{\log p}\right),$$

which for sufficiently great p is less than

$$P \cdot 0.40609.$$

It remains to estimate the third triple sum. We have

$$\sum_{q_2>q_1}^{q_2<p^{1/2}/qq_1} \frac{P}{qq_1q_2} = \frac{P}{qq_1} \log \frac{\frac{1}{2}\log p - \log q - \log q_1}{\log q_1} + O\left(\frac{P}{qq_1 \log p}\right).$$

Noting this, it is easy to obtain

$$\sum_{q_1>q}^{q_1<p^{1/4}q^{1/2}} \sum_{q_2>q_1}^{q_2<p^{1/2}/qq_1} \frac{P}{qq_1q_2} = \frac{P}{q}\int_q^{p^{1/4}/q^{1/2}} \frac{dy}{y\log y} \cdot \log \frac{\frac{1}{2}\log p - \log q - \log y}{\log y}$$

$$+ O\left(\frac{P}{q\log p}\right) = \frac{P}{q}\int_v^{1/4-v/2} \frac{dz}{z} \log \frac{\frac{1}{2}-v-z}{z} + O\left(\frac{P}{q\log p}\right);\ v = \frac{\log q}{\log p}.$$

The third triple sum may be given in the form

$$P\int_{1/8}^{1/6} \frac{dv}{v}\int_v^{1/4-v/2} \frac{dz}{z}\left(\log\left(\frac{1}{2}-v\right) - \log z - \frac{z}{\frac{1}{2}-v} - \frac{z^2}{2(\frac{1}{2}-v)^2}\right.$$

$$\left. - \frac{z^3}{3(\frac{1}{2}-v)^3} - \cdots\right) + O\left(\frac{P}{\log p}\right)$$

$$= P\int_{1/8}^{1/6} \log\frac{\frac{1}{2}(\frac{1}{2}-v)}{v} \log\left(\frac{2(\frac{1}{2}-v)}{v}\right)^{1/2} \frac{dv}{v}$$

$$- P\int_{1/8}^{1/6} \left(\frac{1}{2} + \frac{1}{4\cdot 4} + \frac{1}{8\cdot 9} + \frac{1}{16\cdot 16} + \cdots\right)\frac{dv}{v}$$

$$+ P\int_{1/8}^{1/6} \left(\frac{v}{\frac{1}{2}-v} + \frac{1}{4}\left(\frac{v}{\frac{1}{2}-v}\right)^2 + \frac{1}{9}\left(\frac{v}{\frac{1}{2}-v}\right)^3 + \cdots\right)\frac{dv}{v}.$$

Introducing in the first integral the substitution

$$\frac{\frac{1}{2}-v}{v} = u,$$

and in the third the substitution

$$\frac{v}{\frac{1}{2}-v}=u,$$

we easily obtain

$$P\int_2^3 \log\frac{u}{2}\log 2u^{1/2}\frac{du}{1+u}-P\left(\frac{1}{2}+\frac{1}{4\cdot 4}+\frac{1}{8\cdot 9}+\cdots\right)\log\frac{4}{3}$$

$$+P\int_{1/3}^{1/2}\left(1+\frac{1}{4}u+\frac{1}{9}u^2+\cdots\right)\frac{du}{1+u}+O\left(\frac{P}{\log p}\right).$$

But this expression for sufficiently great p is less than

$$P\cdot 0.01489.$$

Comparing this result with those obtained for simple and double sums we find that the expression (2) for sufficiently great p is less than

$$P(1.38631-0.40609+0.01489)<P\left(1-\frac{1}{205}\right),$$

whence, reasoning as in Theorem II, we prove Theorem III.

5. Passing to the demonstration of Theorem IV let us prove first the following lemma:

LEMMA. *If k be a positive number increasing indefinitely, and s an integer $\geqq 2$, then the number T of numbers less than t_s and not divisible by primes greater than k, where t_s is any number satisfying the condition*

$$k^s<t_s\leqq k^{s+1/(s+2)},$$

is greater than

$$\frac{t_s}{s!(s+2)^s}$$

for all sufficiently great values of k.

Demonstration. Let

$$\epsilon=\frac{1}{s+2}.$$

(i) Taking any number t_1 such that

$$k<t_1<k^{2-2\epsilon},$$

we find a lower bound of the number T_1 of numbers which are $\leqq t_1$ and divisible at least by one prime greater than $k^{1-\epsilon}$ and $\leqq k$. Evidently

$$T_1 = \sum_{q>k^{1-\epsilon}}^{q\leqq k} \left[\frac{t_1}{q}\right],$$

where q runs over primes only. Considering certain laws of distribution of primes, this number may be written in the form

$$t_1 \log \frac{\log t_1}{(1-\epsilon)\log k} + O\left(\frac{t_1}{\log k}\right).$$

But this last expression is greater than

$$t_1 \log \frac{1}{1-\epsilon} + O\left(\frac{t_1}{\log k}\right)$$

which for sufficiently great k is greater than ϵt_1.

So for sufficiently great k we have

$$T_1 > \epsilon t_1.$$

(ii) Taking any number t_2,

$$k^2 < t_2 \leqq k^{3-3\epsilon},$$

we find a lower bound of the number T_2 of numbers which are $\leqq t_2$ and divisible by the product of any two primes, greater than $k^{1-\epsilon}$ and $\leqq k$. Products differing in the order of divisors, we shall consider as different.

Let q be a prime greater than $k^{1-\epsilon}$ and $\leqq k$. The numbers not surpassing t_2 and divisible by q are

$$q, 2q, \cdots, \left[\frac{t_2}{q}\right]q.$$

Consequently, we must find how many numbers of the series

$$1, 2, \cdots, \left[\frac{t_2}{q}\right]$$

are still divisible by primes greater than $k^{1-\epsilon}$ and $\leqq k$. Since

$$k = k^{2-1} < \frac{t_2}{q} < k^{3-3\epsilon-(1-\epsilon)} = k^{2-2\epsilon},$$

then, according to (i), we find that this number for sufficiently great k is greater than

$$\epsilon \frac{t_2}{q}.$$

Hence, as in (i), we find that

$$T_2 > \epsilon^2 t_2$$

for all sufficiently great values of k.

(iii) Arguing thus, we finally find that, if t_s is any number satisfying the condition

$$k^s < t_s \leqq k^{s+1-(s+1)\epsilon},$$

and T_s denotes the number of numbers $\leqq t_s$ and divisible by the product of s primes greater than $k^{1-\epsilon}$ and $\leqq k$ (considering as different the products with different order of divisors), then for sufficiently great k

$$T_s > \epsilon^s t_s = \frac{t_s}{(s+2)^s}.$$

Noting that

$$T > \frac{T_s}{s!},$$

we prove the lemma.

Demonstration of Theorem IV. We have seen that, if n is a divisor of $p-1$ differing from 1, the number R of residues of nth powers modulo p less than $p^{1/2}(\log p)^2$ can be written in the form

$$R = \frac{p^{1/2}(\log p)^2}{n} + O(p^{1/2} \log p). \tag{3}$$

Taking any integer $m \geqq 8$, and letting $k = p^{1/m}$; $s = m/2$ for m even; $s = (m+1)/2$ for m odd, according to the lemma the number of numbers less than $p^{1/2}(\log p)^2$, divisible only by primes less than $p^{1/m}$, is for p sufficiently great, greater than

$$\frac{p^{1/2}(\log p)^2}{s!(s+2)^s}.$$

Assuming that among the numbers less than $p^{1/m}$ there are no non-residues of nth powers modulo p, we have

$$R > \frac{p^{1/2}(\log p)^2}{s!(s+2)^s}.$$

Comparing this inequality with equation (3) we have $(1/n) + O(1/\log p) > 1/(s!(s+2)^s)$ whence $n < s!(s+2)^s + \delta$, where δ goes to 0 with increasing p. But applying the formula of Stirling, we have $s!(s+2)^s < m^m$, from which it follows that, for sufficiently great values of p, $n < m^m$, which is impossible for $n > m^m$. This proves the Theorem IV.

Remark. Evidently the bound $n > m^m$ is very rough. Thus, with $m=8$, we get here the inequality $n > 16777216$ instead of the inequality $n > 204$ found above.

6. We know that to find a primitive root of a prime p it is enough, having found different primitive divisors $2, q_1, q_2, \cdots, q_r$ of the number $p-1$, to find one further non-residue $\nu_0, \nu_1, \cdots, \nu_r$ of each of the powers $2, q_1, \cdots, q_r$. By means of the numbers $\nu_0, \nu_1, \cdots, \nu_r$ it is quite easy to find the primitive root. Applying the established theorems it is easy to prove that

(i) If p is sufficiently great, all the numbers $\nu_0, \nu_1, \cdots \nu_r$ are found in the range

$$1, 2, \cdots, [p^{1/2e^{1/3}}(\log p)^2]. \tag{4}$$

(ii) If p is not of the form $8N+1$, and the numbers $q_1, q_2, \cdots, q_r$ are sufficiently large, then instead of the range (4) we can take shorter ranges, depending on the lowest bound Q of the numbers q. For example, if $Q > 20$, we take the range

$$-1, 1, 2, \cdots, [p^{1/6}]; \tag{5}$$

if $Q > 204$, then

$$-1, 1, 2, \cdots, [p^{1/8}], \tag{6}$$

and finally if $Q > m^m$, when m is an integer $\geqq 8$,

$$-1, 1, 2, \cdots, [p^{1/m}]. \tag{7}$$

These results can be formulated in a different manner.

(i) If p is a sufficiently great prime, then a complete system of residues modulo p can be got by multiplying the powers of the numbers of the range (4).

(ii) If p is not of the form $8N+1$, and all the numbers $q_1, q_2, \cdots, q_r$ are not less than Q, then instead of the range (4) we can take the range (5) for $Q > 20$, the range (6) for $Q > 204$, and finally the range (7) for $Q = m^m$; $m \geqq 8$.

LENINGRAD, RUSSIA