ON A GENERAL THEOREM CONCERNING THE DISTRIBUTION OF THE RESIDUES AND NON-RESIDUES OF POWERS*

BY

J. M. VINOGRADOV

In the present paper I offer a new method for solving some questions regarding the distribution of residues and non-residues of powers.

The difference between the present method and the methods developed in my papers of 1916–18 lies in its entirely elementary character.

The chief idea of this method consists of two different ways of calculating the number of numbers of the form $\alpha(ax+b)$, where α ranges over all the different least positive residues of numbers congruent to $Ax^n \pmod{p}$ and where x independently of α assumes all values $0, 1, \cdots, h-1 (h<p)$.

I shall deal here with the demonstration of the chief formula only, which gives for the prime p the number of numbers congruent to $Ax^n \pmod{p}$ in the progression $ax+b$; $x=0, 1, \cdots, h-1$, with an approximation of order $< \sqrt{p}\log p$.

Other results, such as the law of distribution of the primitive roots, the upper bound $p^{1/2k}(\log p)^2$, $k=e^{(n-1)/n}$, for the least positive non-residues of degree n, modulo p $(p-1=nd)$, and others, follow from this theorem in the same way as in my previous researches on these questions.

In the near future I hope to publish further applications of this method to the demonstration of the chief theorem and to some other important questions of the asymptotic theory of numbers.

LEMMA I. *If p be a prime number >2, α an integer prime to p, and k a positive integer, then there exist relatively prime integers x and y which satisfy the conditions*

$$\alpha x \equiv y \pmod{p};\ 0 < x \leqq k;\ 0 < |y| < p/k.$$

Proof. Let us consider the system of congruences

$$\alpha r \equiv \beta_r \pmod{p} \qquad (r = 1, 2, \cdots, k),$$

the right hand members of which are least positive residues of the left hand ones. Arranging these congruences in such a way that the β_r are ascending,

* Presented to the Society, September 9, 1926; received by the editors in July, 1925.

and adjoining to them the obvious congruence $\alpha \cdot 0 \equiv p \pmod{p}$, we obtain the following system:

$$\begin{aligned} \alpha\gamma_1 &\equiv \lambda_1 && \pmod{p}, \\ \alpha\gamma_2 &\equiv \lambda_2 && \pmod{p}, \\ &\cdots \\ \alpha\gamma_k &\equiv \lambda_k && \pmod{p}, \\ \alpha.0 &\equiv p. && \pmod{p}. \end{aligned}$$

Subtracting one congruence from the other as shown we come to the following system:

$$\begin{aligned} \alpha\gamma_1 &\equiv \lambda_1 && \pmod{p}, \\ \alpha(\gamma_2 - \gamma_1) &\equiv \lambda_2 - \lambda_1 && \pmod{p}, \\ \alpha(\gamma_3 - \gamma_2) &\equiv \lambda_3 - \lambda_2 && \pmod{p}, \\ &\cdots\cdots \\ \alpha(-\gamma_k) &\equiv p - \lambda_k && \pmod{p}. \end{aligned}$$

Among the numbers $\lambda_1, \lambda_2-\lambda_1, \lambda_3-\lambda_2, \cdots, p-\lambda_k$ there is certain to be at least one $\leqq p(k+1)^{-1}$, for the number of these numbers is equal to $k+1$, every one of them is greater than 0, and their sum is p. Among the congruences of the last system there must therefore be at least one of the form

$$\alpha x_1 \equiv y_1 \pmod{p}\ ; \quad 0 < x_1 \leqq k; \quad 0 < |y| \leqq p(k+1)^{-1}.$$

Hence, observing that the numbers x_1 and y_1 can always be reduced to be relatively prime by dividing by their common divisor, we arrive at the conclusion that the lemma is true.

LEMMA* II. *Let k be any number $\geqq 1$, q a positive integer $\leqq k$, c an integer, m a positive integer $\leqq kq^{-1}$, B an arbitrary number and A a number of the form*

$$A = \frac{t}{q} + \frac{\theta}{kq}$$

where t is an integer prime to q, and $|\theta| < 1$. Then, denoting in general by the symbol $\{z\}$ the fractional part of z we have

$$S = \sum_{x=c}^{c+mq-1} \{Ax + B\} = \frac{1}{2} mq + \frac{1}{2} \rho(m+1)\ ; \ |\rho| < 1.$$

* The same lemma somewhat differently formulated is proved in my paper *A new method for obtaining asymptotical expressions of arithmetical functions*, Bulletin of the Russian Academy of Sciences, 1917.

Proof. (i) Let us assume that $q>1$. We have then

$$Ax+B=\frac{tx}{q}+\frac{\theta x}{kq}+B=\frac{tx+f(x)}{q}\,;\ f(x)=Bq+\frac{\theta x}{k}.$$

The set of values of the function $f(x)$ for $x=c, c+1, \cdots, c+mq-1$ forms an arithmetical progression. We shall consider only the case $\theta\geqq 0$. The case $\theta<0$ can be investigated in a similar way. Let $n=[f(c)]$. Two cases are possible:

(α) All values of the function $f(x)$ are less than $n+1$.

(β) One of them at least $\geqq n+1$.

(α) Expanding the sum S in the form of a series of sums

$$S=\sum_{x=c}^{c+q-1}+\sum_{x=c+q}^{c+2q-1}+\cdots+\sum_{x=c+mq-q}^{c+mq-1}\,, \tag{1}$$

let us consider one of these sums

$$I_s=\sum_{x=c+sq}^{c+sq+q-1}\left\{\frac{tx+n+\lambda(x)}{q}\right\},$$

where $\lambda(x)=f(x)-n$. Replacing the numbers $tx+n$ by their least positive residues r, modulo q (which is permissible since $\{z\}$ does not alter by adding to z an integer), and putting $\lambda(x)=\nu(r)$ we get

$$I_s=\sum_{r=0}^{q-1}\left\{\frac{r+\nu(r)}{q}\right\}=\sum_{r=0}^{q-1}\frac{r+\nu(r)}{q}.$$

Therefore

$$I_s=\frac{1}{2}q-\frac{1}{2}+\frac{1}{q}\sum_{r=0}^{q-1}\nu(r)=\frac{1}{2}q-\frac{1}{2}+\theta'\,;\ 0\leqq\theta'<1.$$

Hence

$$I_s=\frac{1}{2}q+\frac{1}{2}\rho_s\,;\ |\rho_s|\leqq 1, \tag{2}$$

$$S=\frac{1}{2}mq+\frac{1}{2}m\rho\,;\ |\rho|\leqq 1,$$

which proves the case (α) of our lemma.

Let us now consider the case (β). Let σ be the greatest integer that satisfies the condition $f(c+\sigma q)<n+1$; then, putting in the sums I_s of the series (1) where $s\leqq\sigma$, $\lambda(x)=f(x)-n$, and in those where $s>\sigma$, $\lambda(x)=f(x)-n-1$, and considering any sum I_s, $s\gtrless\sigma$, we shall get $0\leqq\lambda(x)<1$ and therefore, where $s \lessgtr \sigma$, we shall have as before the equation (2). Equation (2) holds good also when $s=\sigma$, if $\lambda(c+\sigma q+q-1)<1$.

There remains consequently to consider the sum I_σ under the following conditions: $\lambda(c+\sigma q)<1\leqq\lambda(c+\sigma q+q-1)<2$. We have

$$\frac{1}{2} \leqq \frac{1}{q} \sum_{x=c+\sigma q}^{c+\sigma q+q-1} \lambda(x) < \frac{3}{2}\cdot$$

Reducing as in case (α) the sum I_σ to the form

$$I_\sigma = \sum_{r=0}^{q-1} \left\{\frac{r+\nu(r)}{q}\right\},$$

we may write down the equation

$$\left\{\frac{r+\nu(r)}{q}\right\} = \frac{r+\nu(r)}{q}$$

only when $r=0, 1, \cdots, q-2$ (for now the case $1\leqq\nu(r)<2$ is possible), but when $r=q-1$ this equation must be replaced by

$$\left\{\frac{r+\nu(r)}{q}\right\} = \frac{r+\nu(r)}{q} - \delta,$$

where δ may be equal to 0 or 1. Thus we get

$$I_\sigma = \frac{1}{2}q - \frac{1}{2} + \frac{1}{q} \sum_{x=c+\sigma q}^{c+\sigma q+q-1} \lambda(x)^{-\delta} = \frac{1}{2}q + \rho_\sigma ;\ |\rho_\sigma| < 1.$$

Substituting this expression for I_σ and expression (2) for I_s, $s \lessgtr \sigma$, in the equation (1), the validity of the lemma becomes obvious.

(ii) Now putting $q = 1$, it is evident that

$$-\frac{1}{2}m \leqq S - \frac{1}{2}mq \leqq \frac{1}{2}m.$$

The lemma is thus completely proved.

LEMMA III. *Let p be a prime number > 2, α an integer not divisible by p, h a positive integral number $< p$ and β_α any integer which depends on α. Further let*

$$S_\alpha = \sum_{x=0}^{h-1} \left\{\frac{\alpha x+\beta_\alpha}{p}\right\};\ L_\alpha = S_\alpha - \frac{1}{2}h;$$

then the sum $\sum |L_\alpha|$ extended over all numbers of the set

(3) $$1, 2, \cdots, p-1$$

is less than

$$T = \sum_{x=1}^{h} \sum_{y=1}^{px-1} \left(\frac{p}{xy} + 1\right),$$

where for every x the summation for y extends only over the numbers prime to x.

Proof. As a first step let us consider any single sum S_α. Supposing in Lemma I that $k = h$ we can then find two relatively prime numbers x_0, y_0 which satisfy the conditions

$$\alpha x_0 \equiv y_0 \,(\operatorname{mod} p) \ ; \ 0 < x_0 \leqq h \ ; \ 0 < |y_0| < \frac{p}{h} \cdot$$

Hence we find $\alpha x_0 = y_0 + t_0 p$, where t_0 is an integer. Moreover

$$\frac{\alpha}{p} = \frac{t_0}{x_0} + \frac{y_0}{x_0 p} = \frac{t_0}{x_0} + \frac{\theta_0}{x_0 h}\,; \quad |\theta_0| < 1.$$

Supposing $m = [hx_0^{-1}]$, $h_1 = h - mx_0$, we get

$$S_\alpha = \sum_{x=0}^{mx_0-1} \left\{\frac{\alpha x + \beta_\alpha}{p}\right\} + S_\alpha' \ ; \ S_\alpha' = \sum_{x=m x_0}^{mx_0+h_1-1} \left\{\frac{\alpha x + \beta_\alpha}{p}\right\} ; 0 \leqq h_1 < h.$$

Hence, applying Lemma II, we find

$$S_\alpha = \frac{1}{2} mx_0 + \frac{1}{2}\rho(m+1) + S_\alpha' = \frac{1}{2}(h - h_1) + \frac{1}{2}\rho_0\left(\frac{h}{x_0} + 1\right) + S_\alpha' \ ;$$
$$|\rho_0| < 1.$$

Putting $k_1 = h_1$ and applying to the sum S_α' the same treatment as used in the case of the sum S_α, we obtain

$$S_\alpha' = \frac{1}{2}(h_1 - h_2) + \frac{1}{2}\rho_1\left(\frac{h_1}{x_1} + 1\right) + S_\alpha'' \ ; \ |\rho_1| < 1 \ ; \ 0 \leqq h_2 < h_1,$$

where the sum S_α'' consists of h_2 terms. In the same manner we find

$$S_\alpha'' = \frac{1}{2}(h_2 - h_3) + \frac{1}{2}\rho_2\left(\frac{h_2}{x_2} + 1\right) + S_\alpha''' \ ; \ |\rho_2| < 1 \ ; 0 \leqq h_3 < h_2,$$

and so on, until we reach some $h_{n+1} = 0$. Thus we find finally

$$S_\alpha = \frac{1}{2} h + \frac{1}{2}\sigma\left[\left(\frac{h}{x_0} + 1\right) + \left(\frac{h_1}{x_1} + 1\right) + \cdots + \left(\frac{h_n}{x_n} + 1\right)\right]; \ |\sigma| < 1.$$

The lemma will be proved if we can show that

$$\Omega = \frac{1}{2} \sum_{\alpha} \left[\left(\frac{h}{x_0} + 1 \right) + \left(\frac{h_1}{x_1} + 1 \right) + \cdots + \left(\frac{h_n}{x_n} + 1 \right) \right] < T,$$

where the summation extends over all numbers of the set (3). It is necessary to notice that the number n, as well as the numbers $h_1, h_2, \cdots, h_n, x_0, x_1, \cdots, x_n$, depends on the value attributed to α, and for a given α the numbers $x_0, x_1, \cdots, x_n$ are different. In order to estimate the sum Ω we shall first determine an upper bound of the sum of those terms $k/x+1$ which correspond to the same value of x. The given x can correspond only to those values of α which satisfy the congruence $\alpha x \equiv y \pmod{p}$, where y is an integer prime to x and $|y| < pk^{-1}$ and therefore also $|y| < px^{-1}$. Hence for a given x,y can take only the values $\pm 1, \pm 2, \cdots, \pm [px^{-1}]$ prime to x. For every such y we shall find a corresponding value of α. To every admissible system of numbers x,y,α corresponds some k, which satisfies the condition $|y| < pk^{-1}$, or $k < p|y|^{-1}$. Therefore the sum of all the terms in the sum Ω which correspond to a given x will be less than

$$\sum_{y=1}^{px^{-1}} \left(\frac{p}{xy} + 1 \right),$$

where y ranges over numbers prime to x. From this Lemma III follows immediately.

Lemma IV. *Let p be a prime number > 2, β or β_α an integer which may depend on α, and h and γ integers which satisfy the conditions $0 < h < p$; $0 < \gamma < p$. Let us denote by the symbol R_α the number of least positive residues of*

$$\alpha x + \beta_\alpha \qquad (x = 0, 1, \cdots, h-1)$$

which are less than a given number γ, and let us suppose

$$R_\alpha = h\gamma p^{-1} + H_\alpha;$$

then extending the summation over all $\alpha = 1, 2, \cdots, p-1$ we shall get

$$\sum |H_\alpha| < 2T.$$

Proof. According to Lemma III and putting

$$S_\alpha' = \sum_{x=0}^{h-1} \left\{ \frac{\alpha x + \beta - \gamma}{p} \right\} = \frac{1}{2} h + L_\alpha'; \; S_\alpha = \sum_{x=0}^{h-1} \left\{ \frac{\alpha x + \beta}{p} \right\} = \frac{1}{2} h + L_\alpha,$$

we have

$$\sum |L_\alpha'| < T; \; \sum |L_\alpha| < T; \; \sum |S_\alpha' - S_\alpha| < 2T.$$

It is easy to see that

(i) if
$$\left\{\frac{\alpha x+\beta}{p}\right\}<\frac{\gamma}{p},$$
then
$$\left\{\frac{\alpha x+\beta-\gamma}{p}\right\}=\left\{\frac{\alpha x+\beta}{p}\right\}+1-\frac{\gamma}{p};$$

(ii) if
$$\left\{\frac{\alpha x+\beta}{p}\right\}\geqq\frac{\gamma}{p},$$
then
$$\left\{\frac{\alpha x+\beta-\gamma}{p}\right\}=\left\{\frac{\alpha x+\beta}{p}\right\}-\frac{\gamma}{p}.$$

Therefore
$$S_\alpha'-S_\alpha=R_\alpha-\frac{h\gamma}{p}=H_\alpha,$$
which proves the lemma since $\sum|S_\alpha'-S_\alpha|<2T$.

THEOREM. *Let p be a prime number >2, e a factor of $p-1$, a an integer not divisible by p and b any given integer. Distributing all the numbers* $1,2,\cdots,$ $p-1$ *into e classes and referring to the ith class all those, the indices of which are congruent to i* (mod e), *the number of numbers of any class, which belong* (mod p) *to an arithmetical progression $ax+b$; $x=0,1,\cdots,h-1$ $(0<h<p)$ can be represented in the form*
$$\frac{h}{e}+\Delta\,;\ \Delta^2<T+\frac{1}{2}p.$$

Proof. Let $(p-1)e^{-1}=f$ and let us consider a set of fh numbers of the form

$$\alpha(ax+b),\tag{4}$$

where α ranges over all the numbers of the ith class, while x, independently of α, ranges over all the numbers $0,1,\cdots,h-1$. To every number of the set (4) we can find one and only one number u, which satisfies the conditions
$$au+b\equiv\alpha(ax+b)\pmod p\,;\quad 0<u<p,$$
and where the number u, after introduction of a' by means of the congruence $aa'\equiv 1$ (mod p), can be determined by the following conditions:

$$u\equiv\alpha x+\beta_\alpha\pmod p\,;\quad \beta_\alpha=\alpha ba'-ba'\,;\quad 0\leqq u<p.\tag{5}$$

Let D be the number of numbers u, which are $< h$, obtained in this way. The idea of the following proof consists in evaluating the number D by two different methods.

(i) If we leave α constant, then β_α also does not vary, and therefore, in view of congruence (5), the number of values of u less than h, which correspond to all the numbers of the set

$$\alpha(ax + b) \qquad (x = 0, 1, \cdots, h - 1)$$

may be represented in accordance with Lemma IV in the form

$$\frac{h^2}{p} + H_\alpha,$$

where on extending the summation not only over numbers α of the ith class, but over all $\alpha = 1, 2, \cdots, p-1$, we shall obtain

$$\sum | H_\alpha | < 2T\,; \tag{6}$$

and since the number of numbers α of the ith class is f,

$$D = f\frac{h^2}{p} + \sum\nolimits_i H_\alpha,$$

where $\sum_i$ denotes the sum extended over all numbers of the ith class.

(ii) Let there be in the set

$$ax + b \qquad (x = 0, 1, \cdots, h - 1) \tag{7}$$

c_0 numbers of class 0, c_1 numbers of class 1, $\cdots$, c_{e-1} numbers of class $e-1$. The symbol c_s we shall later use also, when $s \geqq e$, denoting by it the number of numbers of the class, the index of which is the lowest positive residue of number s, modulo e. Multiplying one of the numbers of the jth class of the set (7) by all numbers of the ith class, and putting instead of these products the numbers $au+b$, $0 \leqq u < p$, congruent to them modulo p, we shall obtain f numbers $au+b$ which evidently belong to the class $i+j$. Among these numbers $au+b$ there will obviously be c_{i+j} numbers for which $u < h$. Therefore taking into consideration that j can take only the values $0, 1, \cdots, e-1$ we find

$$D = c_0\, c_i + c_1\, c_{i+1} + c_2\, c_{i+2} + \cdots + c_{e-1}\, c_{i+e-1}.$$

Comparing this value of D with that obtained before, we get

$$c_0c_i + c_1c_{i+1} + \cdots + c_{e-1}c_{i+e-1} = f\frac{h^2}{p} + \sum\nolimits_i H_\alpha.$$

Let

$$c_s = \frac{h}{e} + \delta_s\,;$$

then, since $c_0 + c_1 + \cdots + c_{e-1}$ may be represented in the form $h - \sigma$, $\sigma = 0$, or 1 (because one of the numbers (7) may be divisible by p), we shall have $\delta_0 + \delta_1 + \cdots + \delta_{e-1} = -\sigma$; whence we obtain

$$\frac{h^2}{e} - \frac{2h\sigma}{e} + \delta_0\delta_i + \delta_1\delta_{i+1} + \cdots + \delta_{e-1}\delta_{i+e-1} = f\frac{h^2}{p} + \sum\nolimits_i H_\alpha. \tag{8}$$

From this, extending the summation over all $i = 1, 2, \cdots, e-1$, we find

$$\frac{h^2(e-1)}{e} - 2h\sigma\frac{e-1}{e} + \sigma^2 - \delta_0^2 - \delta_1^2 - \cdots - \delta_{e-1}^2$$

$$= \frac{f(e-1)h^2}{p} + \sum_{i=1}^{e-1} \sum\nolimits_i H_\alpha,$$

and hence

$$\sum_{s=0}^{e-1} \delta_s^2 < \sum_{i=1}^{e-1} \left| \sum\nolimits_i H_\alpha \right| + p\,\frac{e-1}{e}\cdot$$

Also putting $i = 0$ in (8) we get

$$\sum_{s=0}^{e-1} \delta_s^2 < \left| \sum\nolimits_0 H_\alpha \right| + \frac{p}{e}.$$

Adding the two last inequalities, and dividing by 2, we obtain

$$\sum_{s=0}^{e-1} \delta_s^2 < T + \frac{1}{2}p$$

and, in particular, for each r

$$\delta_r^2 < T + \frac{1}{2}p\,;\ \left(c_r - \frac{h}{e}\right)^2 < T + \frac{1}{2}p,$$

which proves the theorem.

Note. Evident transformations give an upper bound of $|\Delta|$ less than $\sqrt{p}\log p$.

LENINGRAD, RUSSIA