The distribution of quadratic and higher residues.

By H. DAVENPORT and P. ERDŐS in London.

§ 1.

In this paper we discuss some of the many problems that can be propounded concerning the distribution of the quadratic residues and non-residues, or more generally the kth power residues and non-residues, to a large prime modulus p. If $k > 2$, we shall always suppose $p \equiv 1 \pmod{k}$; as is well known, this involves no loss of generality.

One of the simplest questions that presents itself is that of the order of magnitude of the least quadratic non-residue d to a large prime modulus p. It was proved by VINOGRADOV [1]) in 1919 that

$$d = O(p^{\alpha} \log^2 p), \text{ where } \alpha = \frac{1}{2\sqrt{e}}. \tag{1}$$

VINOGRADOV based his proof on an inequality discovered by him [2]), which is substantially equivalent to PÓLYA's inequality [3]) that

$$\sum_{n=1}^{x} \chi(n) = O(m^{\frac{1}{2}} \log m) \tag{2}$$

for any proper Dirichlet character $\chi(n)$ to modulus $m > 1$, and any positive integer x. For the proof of (1) one needs, of course, only the case of PÓLYA's inequality when m is a prime p and $\chi(n)$ is the Legendre symbol $\left(\frac{n}{p}\right)$.

In § 2 we prove that

$$d = O((p^{\frac{1}{2}} \log p)^{\beta}), \text{ where } \beta = \frac{1}{\sqrt{e}}. \tag{3}$$

This result is better than (1) only in the exponent of the logarithm, which is unimportant. But the proof is of some interest, in that an elementary identity

---

[1]) See *Trans. Amer. Math. Soc.*, **29** (1927), 209—217 and 218—226. The second of these papers gives a reference to the original publication in 1919.

[2]) See the first of the papers in [1]).

[3]) *Nachrichten K. Ges. Wiss. Göttingen*, Math. — phys. Klasse, 1918, 21—29.

[(4) below] is used in place of PÓLYA's or VINOGRADOV's inequality. It may be recalled that the proof of PÓLYA's inequality, though not very difficult, depends on the use of Gaussian sums; and VINOGRADOV's proof of his own inequality, though elementary, is not altogether simple.

In § 3 we give estimates for d_k, the least kth power non-residue (mod p), when k is fixed and p is arbitrarily large. For $k=3$, the result is the same as VINOGRADOV's [4]), but for larger values of k we obtain more precise estimates than his by making use of recent work of DE BRUIJN and others [5]) on the number of numbers up to x which are divisible by at least one prime greater than y.

Another problem that arises when $k>2$ is the order of magnitude of the least kth power non-residue in *any given one* of the $k-1$ classes of non-residues. In § 4 we give an estimate when $k=3$, and in § 5 we prove that an estimate of the form $O(p^{\frac{1}{2}-\eta})$, where $\eta=\eta(k)>0$, is valid for any k. The value of η is very small, but it is difficult to see how one can obtain a reasonably good result without making some assumption about the arithmetical nature of k.

Finally, in § 6 we add some general remarks about the distribution of the quadratic residues and non-residues in sets of consecutive integers. We draw attention to the problem of estimating the maximum number, say H, of consecutive quadratic residues or non-residues. All we are able to prove is that $H=O(p^{\frac{1}{2}})$.

§ 2.

Lemma 1. *Let $\chi(n)$ be a non-principal character to the prime modulus p, and let h be an integer with $0<h<p$. Then*

$$\sum_x \left|\sum_{n=1}^{h}\chi(x+n)\right|^2 = ph-h^2, \tag{4}$$

where the outer sum is over a complete set of residues (mod p).

Proof. The sum on the left of (4) is

$$\sum_x\sum_{n=1}^{h}|\chi(x+n)|^2+\sum_x\sum_{\substack{n_1=1\\ n_1\neq n_2}}^{h}\sum_{n_2=1}^{h}\chi(x+n_1)\,\overline{\chi}(x+n_2),$$

where the bar denotes the complex conjugate. Since $|\chi(x+n)|^2$ is 0 if $x+n\equiv 0$ (mod p) and 1 if $x+n\not\equiv 0$ (mod p), the value of the first double sum is

---

[4]) See the second paper referred to in [1]).

[5]) *Proc. K. Akad. Wet. Amsterdam*, A, **49** (1951), 50—60. See the references given there to work by BUCHSTAB, CHOWLA and VIJAYARAGHAVAN, and RAMASWAMI.

$(p-1)h$. We shall prove that [6])

$$\sum_x \chi(x+n_1)\bar{\chi}(x+n_2) = -1 \tag{5}$$

for $n_1 \not\equiv n_2 \pmod p$. This will imply that the value of the triple sum above is $-h(h-1)$, whence the result.

To prove (5), it suffices to observe that the congruence

$$x+n_1 \equiv y(x+n_2) \pmod p$$

establishes a one-to-one correspondence between all x with $x \not\equiv -n_2$ and all y with $y \not\equiv 1$. Hence the sum in (5) is

$$\sum_{y \not\equiv 1} \chi(y) = -\chi(1) = -1.$$

Theorem 1. *Let d be the least positive quadratic non-residue to the prime modulus p. Then d satisfies* (3).

Proof. We take $h = [p^{\frac{1}{2}} \log p]$ in (4), and use only the terms $x = 1, \ldots, h$ in the sum. We have

$$\sum_{n=1}^{h} \left(\frac{x+n}{p}\right) = h - 2N(x, x+h),$$

where $N(x, x+h)$ denotes the number of quadratic non-residues m satisfying $x+1 \leqq m \leqq x+h$.

Since d is the least quadratic non-residue, every quadratic non-residue must be divisible by at least one prime $\geqq d$. Hence

$$N(x, x+h) \leqq \sum_{d \leqq q \leqq x+h} \left\{ \left[\frac{x+h}{q}\right] - \left[\frac{x}{q}\right] \right\}$$

$$\leqq \sum_{d \leqq q \leqq 2h} \left(\frac{h}{q} + 1\right),$$

where q runs through primes. By well known results in the elementary theory of primes, the last sum is

$$< h(\log\log 2h - \log\log d) + \frac{c_1 h}{\log d},$$

where c_1 is a constant. Hence

$$\sum_{n=1}^{h} \left(\frac{x+n}{p}\right) > h \left\{ 1 - 2\log\log 2h + 2\log\log d - \frac{2c_1}{\log d} \right\}$$

for $x = 1, \ldots, h$.

Applying (4), we obtain

$$1 - 2\log\log 2h + 2\log\log d - \frac{2c_1}{\log d} < \frac{p^{\frac{1}{2}}}{h} < \frac{2}{\log p}.$$

---

[6]) The relation (5) occurs in JACOBSTHAL's doctoral dissertation (Berlin, 1906), but may well have been known to GAUSS.

[It should be noted that if the expression on the left is negative the argument does not apply, but then the result is obviously valid.] We therefore have

$$\log \frac{\log 2h}{\log d} > \frac{1}{2} - \frac{c_2}{\log d},$$

$$\frac{\log 2h}{\log d} > e^{\frac{1}{2}}\left(1 - \frac{c_3}{\log d}\right),$$

$$\log d < e^{-\frac{1}{2}} \log 2h + c_4.$$

The conclusion (3) now follows.

§ 3.

Lemma 2. *Let* $\overline{\psi}(x, x^{\frac{1}{u}})$ *denote the number of positive integers not exceeding* x *which have at least one prime factor* $\geqq x^{\frac{1}{u}}$, *where* $u \geqq 1$ *is fixed. Then*

$$\lim_{x\to\infty} x^{-1}\overline{\psi}(x, x^{\frac{1}{u}}) = 1 - \varrho(u), \tag{6}$$

where $\varrho(u)$ *is the continuous positive and decreasing function defined by*

$$\begin{cases} \varrho(u) = 1 - \log u & \text{for } 1 \leqq u \leqq 2, \\ u\varrho'(u) = -\varrho(u-1) & \text{for } u \geqq 2. \end{cases} \tag{7}$$

Moreover

$$\varrho(u) = \exp(-u \log u - u \log\log u + O(u)) \tag{8}$$

for large u.

For proofs see the paper referred to in [5]) and other papers cited in it.

Theorem 2. *Let* d_k *be the least positive* kth *power non-residue* (mod p), *where* $k > 2$ *is fixed, and* p *is a large prime* $\equiv 1 \pmod{k}$. *Then*

$$d_k = O(p^{\alpha_k + \varepsilon}) \tag{9}$$

for any fixed $\varepsilon > 0$, *where* $\alpha_k = (2u_k)^{-1}$ *and* u_k *is the (unique) solution of* $\varrho(u) = \frac{1}{k}$.

Proof. For simplicity we base the proof (which is essentially VINOGRADOV's) on PÓLYA's inequality (2) rather than on the identity (4), though this would also be possible. Let $\chi(n)$ be a primitive character (mod p) of order k. Then

$$\chi(n) + \chi^2(n) + \cdots + \chi^{k-1}(n)$$

has the value $k-1$ if n is a kth power residue and -1 if n is a kth power non-residue. Thus, for any positive integer x,

$$\sum_{n=1}^{x} (\chi(n) + \cdots + \chi^{k-1}(n)) = (k-1)x - kN(x),$$

where $N(x)$ is the number of kth power non-residues among $1, 2, \ldots, x$. It follows from PÓLYA's inequality that

$$N(x) = \left(1 - \frac{1}{k}\right) x + O(p^{\frac{1}{2}} \log p).$$

Any kth power non-residue is divisible by at least one prime $\geqq d_k$. Hence

$$N(x) \leqq \overline{\psi}(x, d_k),$$

in the notation of Lemma 2. Taking $x = [p^{\frac{1}{2}} \log^2 p]$, for example, we reach a contradiction if there are arbitrarily large primes p for which $d_k > x^{\frac{1}{r}}$, where r is any fixed number for which $\varrho(r) > \frac{1}{k}$; for then $x^{-1}\overline{\psi}(x, d_k)$ would be less than $1 - \frac{1}{k}$ by a fixed amount for such primes. This leads to the result stated.

Corollary. *The values of the exponent α_k for $k = 3, 4, 5$ are*

$$\alpha_3 = \frac{1}{2} e^{-\frac{2}{3}} = 0.2567\ldots,$$
$$\alpha_4 = 0.235\ldots,$$
$$\alpha_5 = 0.221\ldots.$$

Moreover for large (but fixed) k, we have

$$\alpha_k < \frac{1}{2} \frac{\log\log k}{\log k} + \frac{c_5}{\log k},$$

where c_5 is a constant.

Proof. The value for u_3, and hence for α_3, follows from the first part of the definition of $\varrho(u)$ in (7). For u_4 and u_5, we observe that, for $2 \leqq u \leqq 3$,

$$\varrho(u) = 1 - \log u + \int_1^{u-1} \frac{\log t}{1+t}\, dt. \tag{10}$$

On calculating the integral numerically, one is led to the values $u_4 = 2.124\ldots$, $u_5 = 2.257\ldots$, whence the values stated for α_4, α_5. The inequality for α_k when k is large follows at once from (8).

§ 4.

Theorem 3. *Let $\gamma = \frac{1}{2u} = 0.383$ approximately, where u denotes the solution of*

$$\log u + \int_1^{2u-1} \frac{\log t}{1+t}\, dt = \frac{1}{3}. \tag{11}$$

Then each class of cubic non-residues (mod p) *contains a positive integer less than* $p^{\frac{1}{3}+\varepsilon}$ *for any fixed positive* ε, *provided* p *is sufficiently large.*

Proof. Let d denote the least cubic non-residue (mod p). Let $\chi(n)$ be a character to the modulus p of order 3, and let $\chi(d)=\zeta$, so that ζ is one of the two complex cube roots of 1. Let f be the least positive integer for which $\chi(f)=\zeta^2$. Our object is to estimate f. Plainly

$$f \leqq d^2. \tag{12}$$

This in itself is useless as an estimate for f, but will be needed later.

Let $x=[p^{\frac{1}{2}}\log^2 p]$. It follows from PÓLYA's inequality that the number $N_2(x)$ of positive integers $n \leqq x$ for which $\chi(n)=\zeta^2$ satisfies

$$N_2(x)=\frac{1}{3}x+O(p^{\frac{1}{2}}\log p). \tag{13}$$

Any such number n must either have a prime factor $\geqq f$ or have two prime factors each $\geqq d$. Hence

$$N_2(x) \leqq \sum_{f \leqq q \leqq x}\left[\frac{x}{q}\right]+\sum_{\substack{d \leqq q \leqq q' \\ qq' \leqq x}}\sum\left[\frac{x}{qq'}\right], \tag{14}$$

where q and q' run through primes. We can replace d in the limits of the double summation by $f^{\frac{1}{2}}$, in virtue of (12).

We can suppose that $f^{\frac{1}{2}} > x^{\frac{1}{3}}$, since otherwise $f < p^{\frac{1}{3}+\varepsilon}$ and the desired result holds. Under these circumstances we have the identity

$$\bar{\psi}(x, f^{\frac{1}{2}}) = \sum_{f^{\frac{1}{2}} \leqq q \leqq x}\left[\frac{x}{q}\right]-\sum_{\substack{f^{\frac{1}{2}} \leqq q < q' \\ qq' \leqq x}}\sum\left[\frac{x}{qq'}\right]. \tag{15}$$

For the first sum counts how many multiples $\leqq x$ there are of primes $\geqq f^{\frac{1}{2}}$, and the second counts how many multiples $\leqq x$ there are of two distinct primes each $\geqq f^{\frac{1}{2}}$. The latter are counted twice in the first sum. Hence we obtain the number of numbers $\leqq x$ which have at least one prime factor $\geqq f^{\frac{1}{2}}$, which is $\bar{\psi}(x, f^{\frac{1}{2}})$.

Adding (14), with d replaced by $f^{\frac{1}{2}}$, to (15), we obtain

$$N_2(x)+\bar{\psi}(x, f^{\frac{1}{2}}) \leqq \sum_{f \leqq q \leqq x}\left[\frac{x}{q}\right]+\sum_{f^{\frac{1}{2}} \leqq q \leqq x}\left[\frac{x}{q}\right]+o(x),$$

the term $o(x)$ being an allowance for the fact that the double sum in (14) has $q \leqq q'$ whereas that in (15) has $q < q'$.

Using (13) and approximating to the sums in the usual way, we obtain

$$\frac{1}{3} < \log \frac{\log x}{\log f} + \log \frac{2 \log x}{\log f} - x^{-1} \bar{\psi}(x, f^{\frac{1}{2}}) + o(1).$$

If $f = x^{\frac{1}{v}}$, this gives

$$\frac{1}{3} < \log v + \log 2v - (1 - \varrho(2v)) + o(1),$$

by Lemma 2. Since $2 < 2v < 3$, it follows from (10) that

$$\log v + \log 2v - 1 + \varrho(2v) = \log v + \int_1^{2v-1} \frac{\log t}{1+t}\, dt.$$

This leads to the result stated.

§ 5.

Throughout this section k will be a fixed positive integer greater than 2.

Theorem 4. *There exists a positive number η, depending only on k, with the following property: for every sufficiently large prime $p \equiv 1 \pmod k$, each of the $k-1$ classes of kth power non-residues $\pmod p$ contains a positive integer less than $p^{\frac{1}{2}-\eta}$.*

Proof. We define positive numbers $\delta_1 > \delta_2 > \ldots$, depending only on k, as follows:

$$\delta_1 = \frac{1}{k+1}, \qquad \delta_{s+1} = \frac{1}{2k^2}(\delta_s)^2. \tag{16}$$

Let r denote the total number of prime factors of k (multiple prime factors counted according to their multiplicity). Let

$$\delta = \frac{1}{2k+1}(\delta_r)^2. \tag{17}$$

Let

$$x = p^{\frac{1}{2}} \log^2 p. \tag{18}$$

We shall prove that, for sufficiently large p, each class of kth power non-residues contains a positive integer less than $x^{1-\delta}$. This implies the result, on taking η to be any fixed number less than $\frac{1}{2}\delta$.

Let $P_s = x^{\delta_s}$ for $s = 1, 2, \ldots, r+1$, so that $P_1 > P_2 > \cdots$. The primes $\leqq P_s$ belong to certain classes of kth power residues and non-residues, and these classes generate a subgroup $\mathfrak{H}_s$ of the group $\mathfrak{G}$ formed by all the k classes. Plainly

$$\mathfrak{H}_{r+1} \subset \mathfrak{H}_r \subset \cdots \subset \mathfrak{H}_1 \subset \mathfrak{G}.$$

Since the order of a subgroup is a factor of the order of the group, the group $\mathfrak{G}$ cannot have a chain of distinct subgroups, each contained in the next, which comprises more than ν subgroups in addition to $\mathfrak{G}$ itself. Hence either $\mathfrak{H}_1 = \mathfrak{G}$ or $\mathfrak{H}_{s+1} = \mathfrak{H}_s$ for some s with $1 \leqq s \leqq \nu$.

Let A be any particular class of kth power non-residues (mod p). We shall assume that every number belonging to the class A is $\geqq x^{1-\delta}$, and shall deduce a contradiction.

If the class A is contained in the subgroup $\mathfrak{H}_1$, the argument is very simple. The subgroup $\mathfrak{H}_1$ is generated by the classes of the primes $\leqq P_1$, and so the class A is representable as

$$A = C_1^{m_1} \cdots C_r^{m_r},$$

where $C_1, \ldots, C_r$ are the classes of various primes $\leqq P_1$, and $m_1, \ldots, m_r$ are positive integers. We can suppose that $m_1 + \cdots + m_r \leqq k$. For otherwise the classes

$$C_1^{t_1} \ (1 \leqq t_1 \leqq m_1), \quad C_1^{m_1} C_2^{t_2} \ (1 \leqq t_2 \leqq m_2), \ldots, \quad C_1^{m_1} \cdots C_{r-1}^{m_{r-1}} C_r^{t_r} \ (1 \leqq t_r \leqq m_r)$$

could not all be distinct, and on dividing two such identical classes we would have a representation of the unit class with non-negative exponents not exceeding $m_1, \ldots, m_r$ respectively. This would lead to a representation of A with smaller exponents, and eventually to a representation with $m_1 + \cdots + m_r \leqq k$. Such a representation implies that there is a positive integer in the class A which is

$$\leqq P_1^{m_1 + \cdots + m_r} \leqq P_1^k = x^{k\delta_1} = x^{1-\delta_1} < x^{1-\delta},$$

and this is contrary to the hypothesis.

We can now suppose that the class A is not contained in the subgroup $\mathfrak{H}_1$. This implies in particular that $\mathfrak{H}_1 \neq \mathfrak{G}$, and consequently that

$$\mathfrak{H}_{s+1} = \mathfrak{H}_s$$

for some value of s. This value of s will be fixed throughout the subsequent argument.

We can factorize each number m in the class A into primes as follows:

$$m = q_1^{\alpha_1} q_2^{\alpha_2} \ldots r_1^{\beta_1} r_2^{\beta_2} \ldots = qr, \text{ say,}$$

where $q_1, \ldots$ are primes which do not belong to classes in the subgroup $\mathfrak{H}_s (= \mathfrak{H}_{s+1})$, and $r_1, \ldots$ are primes which do belong to classes in that subgroup. Plainly

$$q_i \geqq P_s. \tag{19}$$

Moreover,

$$q \geqq x^{1-\delta-k\delta_{s+1}}. \tag{20}$$

For since r belongs to a class in the subgroup $\mathfrak{H}_{s+1}$, we can find, by the argument used above, a number r' in the same class as r and satisfying

$r' \leqq (P_{s+1})^k = x^{k\delta_{s+1}}$. If q did not satisfy (20), the number qr' would be in the class A and would be less than $x^{1-\delta}$, contrary to the hypothesis.

By PÓLYA's inequality and the definition of x in (18), the number of numbers m in the class A satisfying $m \leqq x$ is

$$\frac{x}{k} + O\left(\frac{x}{\log p}\right).$$

On the other hand, each such number m is divisible by some number q which satisfies (20) and whose prime factors all satisfy (19). Hence the number of numbers $m \leqq x$ in the class A does not exceed

$$\sum_{q \leqq x} \left[\frac{x}{q}\right],$$

where q runs through numbers of the above kind. It follows, writing $y = x^{1-\delta-k\delta_{s+1}}$, that

$$\sum_{y \leqq q \leqq x} \frac{1}{q} > \frac{1}{k} - \frac{c_6}{\log p}, \tag{21}$$

where every prime factor of q satisfies (19), and where c_6 is a constant.

To estimate the sum on the left of (21) we use the following device, which has the advantage of simplicity, though the result it gives is no doubt crude. We express each q as $q_1 t$, where q_1 is a prime $\geqq P_s$ and t is either 1 or is composed entirely of primes $\geqq P_s$. Then

$$\sum_{y \leqq q \leqq x} \frac{1}{q} \leqq \sum_{t \leqq x} \frac{1}{t} \sum_{\substack{P_s \leqq q_1 \leqq \frac{x}{t} \\ q_1 \geqq \frac{y}{t}}} \frac{1}{q_1}, \tag{22}$$

where q_1 is restricted to primes and t is either 1 or is composed of primes $\geqq P_s$.

The prime q_1 is restricted to an interval $P \leqq q_1 \leqq Q$, where $P \geqq P_s$ and $\frac{Q}{P} \leqq \frac{x}{y}$. Hence, by the well known estimate for a sum of reciprocals of primes, we have

$$\begin{aligned}
\sum \frac{1}{q_1} &< \log \frac{\log Q}{\log P} + O\left(\frac{1}{\log P}\right) \\
&\leqq \log \frac{\log P + \log \frac{x}{y}}{\log P} + O\left(\frac{1}{\log P}\right) \\
&\leqq \log \frac{\log P_s + \log \frac{x}{y}}{\log P_s} + O\left(\frac{1}{\log p}\right) \\
&= \log \frac{\delta_s + \delta + k\delta_{s+1}}{\delta_s} + O\left(\frac{1}{\log p}\right) \\
&< \frac{\delta + k\delta_{s+1}}{\delta_s} + O\left(\frac{1}{\log p}\right).
\end{aligned}$$

As regards $\sum \frac{1}{t}$, we have obviously

$$\sum \frac{1}{t} < \prod_{P_s \leqq \tilde{\omega} \leqq x} \left(1 - \frac{1}{\tilde{\omega}}\right)^{-1} = \frac{1}{\delta_s} + O\left(\frac{1}{\log p}\right),$$

where $\tilde{\omega}$ runs through primes.

On substituting these estimates in (21) and (22), we obtain

$$\frac{\delta + k\delta_{s+1}}{(\delta_s)^2} > \frac{1}{k} - \frac{c_7}{\log p},$$

where c_7 is a constant. By (16) this implies

$$\begin{aligned} \delta &\geqq \frac{1}{2k}(\delta_s)^2 - \frac{c_8}{\log p} \\ &\geqq \frac{1}{2k}(\delta_v)^2 - \frac{c_8}{\log p}. \end{aligned}$$

In view of (17), we now have a contradiction if p is sufficiently large. This proves Theorem 4.

§ 6.

It is natural to consider the possibility of generalizing the identity of Lemma 1 so as to obtain an asymptotic formula for the corresponding sum with the exponent 2 replaced by any positive integer. The result is given in the following lemma. It does not seem to throw any light on the problem of the magnitude of the least quadratic non-residue, but it enables us to prove (in Theorem 5 below) that the distribution of the sum

$$S_h(x) = \sum_{n=x+1}^{x+h} \left(\frac{n}{p}\right) \tag{23}$$

for large p is normal (or Gaussian) provided h is taken to be a function of p satisfying appropriate conditions.

Lemma 3. *Let p be an arbitrarily large prime and let h be any integer satisfying $0 < h < p$. Let r be a fixed positive integer. Then*

$$\sum_x (S_h(x))^{2r} = 1.3 \ldots (2r-1)(p - \vartheta r)(h - \vartheta' r)^r + O(h^{2r} p^{\alpha_r}),$$

where α_r depends only on r and $\alpha_r < 1$, and where $0 \leqq \theta \leqq 1$, $0 \leqq \theta' \leqq 1$. Also

$$\sum_x (S_h(x))^{2r-1} = O(h^{2r} p^{\alpha_r}).$$

Proof. Consider first the case of the exponent $2r$. We have

$$\sum_x (S_h(x))^{2r} = \sum_{n_1=1}^{h} \cdots \sum_{n_{2r}=1}^{h} \sum_x \left(\frac{(x+n_1)\cdots(x+n_{2r})}{p}\right).$$

The sets of integers $n_1, \ldots, n_{2r}$ can be divided into two types. If the set comprises at most r distinct integers, each of which occurs an even number

of times, we say that it is of the first type. In this case, the polynomial $(x+n_1)\cdots(x+n_{2r})$ is a perfect square, and the value of the sum extended over x lies between $p-r$ and p. Hence the contribution of the sets of integers $n_1, \ldots, n_{2r}$ of the first type is

$$F(r, h)(p-\theta r),$$

where $F(r, h)$ is the number of such sets and $0 \leqq \theta \leqq 1$.

Now consider the remaining sets of integers $n_1, \ldots, n_{2r}$. For these, the polynomial $(x+n_1)\cdots(x+n_{2r})$ is not congruent (mod p) to the square of another polynomial, since it has a zero of odd multiplicity. Under these circumstances it is known [7]) that

$$\sum_x \left(\frac{(x+n_1)\cdots(x+n_{2r})}{p} \right) = O(p^{\alpha_r}),$$

where α_r depends only on r and $\alpha_r < 1$. Hence the contribution of sets of the second type is $O(h^{2r} p^{\alpha_r})$.

It remains only to estimate the number, say $F(r, h)$, of sets of integers $n_1, \ldots, n_{2r}$, with $1 \leqq n_j \leqq h$, which comprise at most r distinct integers each of which occurs an even number of times. The number of ways of choosing *exactly* r distinct integers from $1, 2, \ldots, h$ is $h(h-1)\cdots(h-r+1)$, and the number of different ways of arranging these as r pairs is $(2r-1)(2r-3)\ldots 5.3.1$. Hence

$$F(r, h) \geqq 1.3 \ldots (2r-1)\, h(h-1)\cdots(h-r+1).$$

On the other hand, the number of ways of choosing at most r distinct integers from $1, 2, \ldots, h$ is $\leqq h^r$, and, when these have been chosen, the number of different ways of arranging them in $2r$ places (each occurring an even number of times) is at most $(2r-1)(2r-3)\ldots 5.3.1$. Hence

$$F(r, h) \leqq 1.3 \ldots (2r-1) h^r.$$

Thus

$$F(r, h) = 1.3 \ldots (2r-1)(h-\theta' r)^r,$$

and the result follows.

The result for the sum with an odd exponent is now obvious, since in this case there are no sets of the first type.

Theorem 5. *Let h be any function of p satisfying*

$$h \to \infty, \quad \frac{\log h}{\log p} \to 0 \quad \text{as} \quad p \to \infty. \tag{24}$$

---

[7]) By a theorem of Davenport [*Acta Math.*, **71** (1939), 99—121; see formula (13)] the result holds with $\alpha_r = (4r+3)(4r+6)$. A much deeper theorem of A. Weil would allow one to take $\alpha_r = \frac{1}{2}$.

Let $S_h(x)$ be defined by (23) *for primes p. Let $M_p(\lambda)$ denote the number of integers x with $0 \leqq x < p$ for which*

$$S_h(x) \leqq \lambda h^{\frac{1}{2}}.$$

Then

$$\frac{1}{p} M_p(\lambda) \to \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{\lambda} e^{-\frac{1}{2}t^2} dt \quad as \quad p \to \infty$$

for each fixed λ.

Proof. We observe first that in view of the conditions imposed on h in (24), it follows from Lemma 3 that

$$\frac{1}{p} \sum_{x=0}^{p-1} (h^{-\frac{1}{2}} S_h(x))^r \to \mu_r \quad \text{as} \quad p \to \infty \tag{25}$$

for each fixed positive integer r, where

$$\mu_r = \begin{cases} 1.3 \ldots (2r-1) & \text{if } r \text{ is even,} \\ 0 & \text{if } r \text{ is odd.} \end{cases}$$

Let $N_p(s)$ denote the number of integers x with $0 \leqq x < p$ for which $S_h(x) \leqq s$. Then $N_p(s)$ is a non-decreasing function of s which is constant except for discontinuities at certain integral values of s. Also $N_p(s) = 0$ if $s < -h$ and $N_p(s) = p$ if $s \geqq h$. Obviously

$$M_p(\lambda) = N_p(\lambda h^{\frac{1}{2}}).$$

Collecting together the values of x in (25) for which $S_h(x) = s$, we obtain

$$\frac{1}{p} \sum_{s=-h}^{h} (h^{-\frac{1}{2}} s)^r \{N_p(s) - N_p(s-1)\} \to \mu_r. \tag{26}$$

Define $\Phi_p(t)$ by

$$\Phi_p(t) = \frac{1}{p} N_p(t h^{\frac{1}{2}}) = \frac{1}{p} M_p(t). \tag{27}$$

Then, by the definition of the STIELTJES integral, the left hand side of (26) is

$$\int_{-\infty}^{\infty} t^r \, d\Phi_p(t).$$

Putting

$$\Phi(t) = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{t} e^{-\frac{1}{2}u^2} du,$$

we have

$$\int_{-\infty}^{\infty} t^r d\Phi(t) = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{\infty} t^r e^{-\frac{1}{2}t^2} dt = \mu_r.$$

Hence

$$\int_{-\infty}^{\infty} t^r d\Phi_p(t) \to \int_{-\infty}^{\infty} t^r d\Phi(t) \quad \text{as} \quad p \to \infty, \tag{28}$$

for any fixed positive integer r. The assertion of the theorem is equivalent, by (27), to the assertion that

$$\Phi_p(\lambda) \to \Phi(\lambda) \quad \text{as} \quad p \to \infty \tag{29}$$

for each real number λ.

The fact that (28) implies (29), when $\Phi_p(t)$ is the special function defined above, is well known in the mathematical theory of probability. We outline one method of proof. If (29) is false for a particular λ, we can suppose without loss of generality that there exists $\delta > 0$ such that

$$\Phi_p(\lambda) \geqq \Phi(\lambda) + \delta \tag{30}$$

for infinitely many p. There exists [8]) a subsequence, say q, of these p such that $\Phi_q(t)$ converges to a non-decreasing function $\Phi^*(t)$ at every point of continuity of this function, and

$$\int_{-\infty}^{\infty} t^r d\Phi^*(t) = \lim_{q \to \infty} \int_{-\infty}^{\infty} t^r d\Phi_q(t) = \int_{-\infty}^{\infty} t^r d\Phi(t).$$

Also $\Phi^*(t) \to 0$ as $t \to -\infty$ and $\Phi^*(t) \to 1$ as $t \to +\infty$. It now follows from the well known uniqueness of this special moment problem that $\Phi^*(t) = \Phi(t)$ for all t. This contradicts (30), and the contradiction establishes the desired result.

An interesting problem is that of the order of magnitude of the maximum number of consecutive quadratic residues, or of consecutive quadratic non-residues, to a large prime modulus p. Denoting these maximum numbers by H_+ and H_-, it follows from Lemma 1 that

$$H_+ = O(p^{\frac{1}{2}}), \qquad H_- = O(p^{\frac{1}{2}}). \tag{31}$$

For if the numbers $x+1, x+2, \ldots, x+H$ all have the same character, then the sum

$$\sum_{n=1}^{h} \left(\frac{x+n}{p}\right),$$

[8]) See the two theorems of Helly in the introduction to J. A. Shohat and J. D. Tamarkin, *The problem of moments* (Math. Surveys No. 1, New York 1943).

where $h = \left[\frac{1}{2}H\right]$, has the value h or $-h$ for at least h consecutive values of x, and the lemma implies $h^3 \leqq ph - h^2$, whence the result. We have not been able to improve on the estimates (31).

As regards results in the opposite direction, it can be shown [9]) that there are infinitely many primes p for which

$$H_+ > c_9 (\log p)^{\frac{1}{2}},$$

and similarly with H_-, where c_9 is a positive constant. By using the result of A. WEIL it is possible to improve this lower bound to $c_9 \log p$.

(Received August 4, 1952.)

Note added January 1953. We observe that the identity of Lemma 1 is given in VINOGRADOV's Osnovy teorii čisel, p. 109.

[9]) See § 9 of the paper referred to in [7]).