SOME REMARKS ON THE LARGE SIEVE OF YU. V. LINNIK

By

P. ERDŐS and A. RÉNYI

Mathematical Institute of the Hungarian Academy of Sciences, Budapest

(Received November 22, 1967)

§ 1. Introduction

YU. V. LINNIK has discovered (see [1]) in 1941 a very powerful new method of elementary number theory, which he called the large sieve[1]. In his original formulation the large sieve asserts that if we take any sequence S_N consisting of Z positive integers $\leqq N$, and if Y denotes the number of those primes[2] $p \leqq \sqrt{N}$ for which all the elements of the sequence S_N are contained in $\leqq p(1-\varepsilon)$ residue classes mod p, where $0<\varepsilon<1$, then one has

$$Y \leqq \frac{20\pi N}{\varepsilon^2 Z}. \tag{1.1}$$

As shown by the second named author in [3], Linnik's method is capable to prove much more, namely that if Z is not too small compared with N, then the elements of the sequence S_N not only occupy "almost all" residue classes mod p with respect to most primes $p \leqq \sqrt{N}$, but are almost uniformly distributed in the p residue classes mod p for most primes $p \leqq \sqrt{N}$. More exactly, let us denote by $Z(a, p)$ (where $a = 0, 1, \ldots, p-1$) the number of elements of the sequence S_N which are congruent to a mod p. Then one has, putting

$$\Delta^2(p) = p \sum_{a=0}^{p-1} \left(Z(a, p) - \frac{Z}{p} \right)^2. \tag{1.2}$$

the inequality[3]

[1] As regards important applications of the large sieve in number theory, see e.g. [2] [3], [4], [5], [6]; [5] and [6] contain many further references.

[2] In this paper p always denotes a prime number.

[3] Here and in what follows all the constants of the O-estimates are absolute, i.e. do not depend on N, nor on the sequence S_N nor on Q.

$$(1.3) \qquad \sum_{p \leq Q} \Delta^2(p) = O(Z^{2/3} N^{4/3} Q^{1/3})$$

for $Q \leq N^{3/5}$. Later, the second named author has found (see [7]), a new probabilistic method for proving theorems of the type of the large sieve. This method (developed further and generalized in the papers [8], [9], [10], [11], [12]) gave the result

$$(1.4) \qquad \sum_{p \leq Q} \Delta^2(p) = O\big(Z(Q^3 + N)\big)$$

for $Q \leq \sqrt{N}$. This estimate is better than (1.3) for $Q \leq N^{3/8}$, but weaker if $N^{3/8} < Q \leq \leq \sqrt{N}$.

Especially for $Q = N^{1/3}$ this result gives

$$(1.5) \qquad \sum_{p \leq N^{1/3}} \Delta^2(p) = O(NZ).$$

The estimate (1.5) is essentially best possible, because if for instance S_N is the sequence of odd numbers $\leq N$, one has $Z(0, 2) = 0$ and thus $2\left(Z(0,2) - \frac{Z}{2}\right)^2 = \frac{Z^2}{2}$ i.e. this single term is already of order NZ.

The probabilistic approach, besides leading to a very sharp estimate for $Q \leq N^{1/3}$, has thrown light on the reasons why an arbitrary sufficiently dense subsequence of the sequence $1, 2, \ldots, N$ has to be almost uniformly distributed among the residue classes mod p for most $p \leq N^{1/3}$; it became obvious that this is due to the statistical independence (more exactly: almost independence) of the distribution mod p and mod q of the numbers $n \leq N$ for any two primes $p, q \leq N^{1/3}$, $p \neq q$.

In the last two years important progress was made on the large sieve. The first essential improvement was obtained by K. F. ROTH [13]. His result was sharpened by BOMBIERI [14] who has shown that (1.5) holds also for $Q = \sqrt{N}$. More exactly Bombieri proved

$$(1.6) \qquad \sum_{p \leq Q} \Delta^2(p) = O\big(Z(Q^2 + N)\big).$$

Clearly (1.6) is superior to both (1.3) and (1.4) for the full ranges $Q \leq N^{3/5}$ resp. $Q \leq \sqrt{N}$.

An important generalization of Bombieri's theorem has been obtained by H. DAVENPORT and H. HALBERSTAM [15]. To make this advance clear one has to notice that putting

$$(1.7) \qquad S(x) = \sum_{n \in S_N} e^{2\pi i n x}$$

one has

$$(1.8) \qquad \Delta^2(p) = \sum_{a=1}^{p-1} \left| S\left(\frac{a}{p}\right) \right|^2.$$

Now DAVENPORT and HALBERSTAM have proved that if $\alpha_1, \alpha_2, \ldots, \alpha_D$ are arbitrary real numbers in the interval (0, 1) such that $|\alpha_i - \alpha_j| \geqq \delta > 0$ for $i \neq j$, one has

$$(1.9) \qquad \sum_{i=1}^{D} |S(\alpha_i)|^2 = O\left(Z\left(\frac{1}{\delta} + N\right)\right).$$

Clearly, if the numbers $\frac{a}{p}$ $(a = 1, 2, \ldots, p-1;\ p \leqq Q)$ are taken as the numbers $\alpha_1, \ldots, \alpha_D$ $(D = \sum_{p \leqq Q} (p-1))$ then $\delta \geqq \frac{1}{Q^2}$ and thus (in view of (1.8)) (1.9) implies (1.6).

Note that from (1.9) one obtains even more than (1.6), namely that

$$\sum_{q \leqq Q} \sum_{\substack{a=1 \\ (a,q)=1}}^{q} \left|S\left(\frac{a}{q}\right)\right|^2 = O\left(Z\left(\frac{1}{\delta} + N\right)\right)$$

because if $(a, q) = 1$, $(a', q') = 1$ (here (a, q) denotes the greatest common divisor of a and q) one has for $q, q' \leqq Q$ and $\frac{a}{q} \neq \frac{a'}{q'}$

$$\left|\frac{a}{q} - \frac{a'}{q'}\right| \geqq \frac{1}{Q^2}.$$

Recently P. X. GALLAGHER [16] has found a very elegant and simple method for proving (1.9). More exactly, he proved

$$(1.10) \qquad \sum_{\nu=1}^{D} |S(\alpha_\nu)|^2 \leqq Z\left(\frac{1}{\delta} + \pi N\right)$$

which implies by (1.8)

$$(1.11) \qquad \sum_{p \leqq Q} \Delta^2(p) \leqq Z(Q^2 + \pi N).$$

Thus we have for $Q = \sqrt{N}$

$$(1.12) \qquad \sum_{p \leqq Q} \Delta^2(p) \leqq (\pi + 1) ZN.$$

In the paper [17] of the first named author it has been mentioned (without giving the proof in detail) that by a probabilistic argument it can be shown that (1.12) cannot hold if Q is of larger order of magnitude than $\sqrt{N \log N}$. The aim of the present paper is to prove this statement in detail, and to get some related results concerning the behaviour of $\sum_{p \leqq Q} \Delta^2(p)$, when S_N is a *random* subset of the set $\{1, 2, \ldots, N\}$.

The results obtained throw some light on certain open problems connected with the large sieve.

§ 2. Equidistribution of random sequences in arithmetic progressions

In this § let S_N denote a random subsequence of the sequence $\{1, 2, \ldots, N\}$ obtained as follows: let $\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_N$ be independent random variables, each of which takes on the values 1 and 0 with probability $\frac{1}{2}$; let S_N denote the set of those $n \leqq N$ for which $\varepsilon_n = 1$. (It is easy to see that under these suppositions each of the 2^N subsets of the set $\{1, 2, \ldots, N\}$ has the same probability to be chosen.) In this case

$$Z = \sum_{n=1}^{N} \varepsilon_n \tag{2.1}$$

$$Z(a, p) = \sum_{k=0}^{\left[\frac{N-a}{p}\right]} \varepsilon_{kp+a} \tag{2.2}$$

and consequently

$$\Delta^2(p) = p \cdot \sum_{a=0}^{p-1} \left(Z(a, p) - \frac{Z}{p}\right)^2 \tag{2.3}$$

are all random variables. One obtains easily

$$\Delta^2(p) = p \cdot \sum_{a=0}^{p-1} Z^2(a, p) - Z^2 \tag{2.4}$$

and thus, putting[4]

$$\pi_r(Q) = \sum_{p \leqq Q} p^r \qquad (r = 0, 1, 2, \ldots) \tag{2.5}$$

we have

$$R(Q) = \sum_{p \leqq Q} \Delta^2(p) = \sum_{n=1}^{N} \sum_{m=1}^{N} [A_Q(n-m) - \pi_0(Q)]\varepsilon_n \varepsilon_m, \tag{2.6}$$

where

$$A_Q(k) = \sum_{\substack{p/k \\ p \leqq Q}} p \tag{2.7}$$

and thus $A_Q(-k) = A_Q(k)$ and especially

$$A_Q(0) = \pi_1(Q). \tag{2.8}$$

Let us determine first the expectation[5] of $R(Q)$. As

$$E(\varepsilon_n) = \frac{1}{2} \quad \text{and} \quad E(\varepsilon_n \varepsilon_m) = \begin{cases} \frac{1}{4} & \text{if } n \neq m \\ \frac{1}{2} & \text{if } n = m \end{cases} \tag{2.9}$$

[4] Thus $\pi_0(Q)$ denotes the number of primes $\leqq Q$.

[5] The expectation of a random variable ξ will be denoted by $E(\xi)$.

we obtain

$$E(R(Q)) = \frac{1}{4} \sum_{n=1}^{N} \sum_{m=1}^{N} (A_Q(n-m) - \pi_0(Q)) + \frac{N}{4} \pi_1(Q). \tag{2.10}$$

Now clearly

$$\sum_{n=1}^{N} \sum_{m=1}^{N} [A_Q(n-m) - \pi_0(Q)] = \sum_{p \leq Q} p \left\{ \sum_{a=0}^{p-1} \left[\left(\left[\frac{N-a}{p} \right] + 1 \right)^2 - \frac{N^2}{p^2} \right] \right\}. \tag{2.11}$$

Let us suppose that $N \equiv r \bmod p$, where $0 \leqq r < p$. Then we have

$$p \cdot \left\{ \sum_{a=0}^{p-1} \left[\left(\left[\frac{N-a}{p} \right] + 1 \right)^2 \right] \right\} = 2N + r(p-r) + p - 2r. \tag{2.12}$$

Thus it follows that

$$\sum_{n=1}^{N} \sum_{m=1}^{N} [A_Q(n-m) - \pi_0(Q)] = 2N\pi_0(Q) + O(Q^2\pi_0(Q)) \tag{2.13}$$

and thus, taking into account that $\pi_0(Q) = \frac{Q}{\log Q} + O\left(\frac{Q}{\log^2 Q}\right)$ and

$$\pi_1(Q) = \frac{Q^2}{2 \log Q} + O\left(\frac{Q^2}{\log^2 Q}\right) \tag{2.14}$$

it follows

$$E(R(Q)) = \frac{NQ\pi_0(Q)}{8} + O(Q^2\pi_0(Q)) + O\left(\frac{Q^2 N}{\log^2 Q}\right). \tag{2.15}$$

Thus the expectation of $R(Q)$ is smaller by a factor of order $\frac{1}{\log Q}$ as NQ^2. Note that *the expectation of $R(Q)$ can be interpreted as its average over all 2^N subsequences of the sequence* $\{1, 2, \ldots, N\}$. Thus the average of $R(Q)$ is of order $O(N^2)$ even for $Q = O(\sqrt{N \log N})$ while for its maximum according to (1.6) this is known only for $Q = O(\sqrt{N})$. It is an open question whether the estimate

$$R(Q) = O(N^2) \tag{2.16}$$

holds for *all* sequences S_N if $Q \sim \sqrt{N}\psi(N)$ for some function $\psi(N)$ such that $\psi(N) \to \infty$ for $N \to \infty$. Our method is not capable of giving such a result; however by evaluating the *variance* of the random variable $R(Q)$ we can show by Čebishev's inequality that the estimate (2.16) is valid at least for *most* subsequences S_N.

To evaluate the variance[6] of $R(Q)$ note that though the random variables $\varepsilon_n\varepsilon_m$ are not independent, they are pairwise uncorrelated and thus the variance

[6] The variance of a random variable ξ will be denoted by $D^2(\xi)$.

of the sum on the right hand side of (2.6) is equal to the sum of the variances of the single terms. As $D^2(\varepsilon_n\varepsilon_m) = \frac{3}{16}$ if $n \neq m$ and $D^2(\varepsilon_n^2) = \frac{4}{16}$.

$$D^2(R(Q)) = \frac{3}{16}\sum_{n=1}^{N}\sum_{m=1}^{N}(A_Q(n-m)-\pi_0(Q))^2 + \frac{N}{16}(\pi_1(Q)-\pi_0(Q))^2. \tag{2.17}$$

Now clearly

$$\sum_{n=1}^{N}\sum_{m=1}^{N} A_Q^2(n-m) \leqq N^2[\pi_0^2(Q)+\pi_1(Q)-\pi_0(Q)] + 2N\pi_1^2(Q)+\pi_2^2(Q). \tag{2.18}$$

As further from (2.11) we have

$$\sum_{n=1}^{N}\sum_{m=1}^{N} A_Q(n-m) \geqq N^2\pi_0(Q) - 2N\pi_0(Q) + \pi_1(Q)$$

it follows

$$D^2(R(Q)) \leqq \frac{3}{16}N^2(\pi_1(Q)-\pi_0(Q)) + \tag{2.19}$$

$$+\frac{3N}{8}\left(\pi_1^2(Q)+2\pi_0^2(Q)+\frac{(\pi_1(Q)-\pi_0(Q))^2}{6}\right)+\frac{3}{16}\pi_2^2(Q)-\frac{3}{8}\pi_1(Q)\pi_0(Q).$$

In view of (2.14), it follows

$$D^2(R(Q)) = O\left(\frac{N^2Q^2}{\log Q}\right) + Q\left(\frac{NQ^4}{\log^2 Q}\right) \tag{2.20}$$

i.e.

$$\frac{D(R(Q))}{E(R(Q))} = O\left(\frac{\sqrt{\log Q}}{Q}\right) + O\left(\frac{1}{\sqrt{N}}\right). \tag{2.21}$$

It follows from Čebishev's inequality that for $\lambda > 1$ with probability $\geqq 1-\frac{1}{\lambda^2}$ $R(Q)$ is contained in an interval

$$[E(R(Q)) - \lambda D(R(Q)),\ E(R(Q)) + \lambda D(R(Q))].$$

Choosing for λ the value $\lambda = \min\left(\frac{Q}{(\log Q)^{3/2}}, \frac{\sqrt{N}}{\log Q}\right)$ it follows that for all but $\frac{2^N}{\lambda^2}$ possible exceptions for all other sequences, i.e. for the large majority of all sequences, $R(Q)$ is of order $\frac{NQ^2}{8\log Q} + O\left(\frac{NQ^2}{\log^2 Q}\right)$.

Thus we have proved the following

THEOREM 1. *Let us consider all 2^N subsequences S_N of the sequence $\{1, 2, \ldots \ldots, N\}$. We have for all these subsequences with the possible exception of $\frac{2^N}{\lambda^2}$ such sequences*

$$R(Q) = \frac{NQ^2}{8 \log Q} + O\left(\frac{NQ^2}{\log^2 Q}\right) \tag{2.22}$$

where $Q \geqq N^{1/3}$ and

$$\lambda = \min\left(\frac{Q}{(\log Q)^{3/2}}, \frac{\sqrt{N}}{\log Q}\right). \tag{2.23}$$

Thus, if $Q \leqq \sqrt{N \log N}$, (2.22) holds except for at most $\frac{2^N \log^3 Q}{Q^2}$ sequences, while for $Q > \sqrt{N \log N}$ (2.22) holds, except for at most $\frac{2^N \log^2 N}{N}$ sequences.

COROLLARY. If $Q = \sqrt{AN \log N}$ $(A > 1)$ then $R(Q) \sim \frac{AN^2}{8}$ except for at most $\frac{2^N \log^2 N}{N}$ sequences.

Let us now consider the quantity

$$\operatorname*{Max}_{p \leqq Q}\left[\operatorname*{Max}_{0 \leqq a \leqq p-1}\left|Z(a, p) - \frac{Z}{p}\right|\right].$$

It is easy to show [using the central limit theorem and the fact that for any given p the quantities $Z(a, p)$ $(a = 0, 1, \ldots, p-1)$ are independent], that

$$P\left(\operatorname*{Max}_{0 \leqq a \leqq p-1}\left|Z(a,p) - \frac{Z}{p}\right| > \sqrt{\frac{N \log pQ}{2p}}\right) = O\left(\frac{1}{Q}\right) \tag{2.24}$$

and thus except for at most $O\left(\frac{2^N}{\log Q}\right)$ exceptional sequences we have

$$\left|Z(a,p) - \frac{Z}{p}\right| \leqq \sqrt{\frac{N \log pQ}{2p}}$$

for *all* a and p $(0 \leqq a \leqq p-1,\ p \leqq Q)$.

On the other hand, using again the independence of the random variables $Z(a, p)$ $(a = 0, 1, \ldots, p-1)$ and the central limit theorem it follows that for all except for at most $O\left(\frac{2^N}{N}\right)$ sequences S^N, one has, for all p such that $C \log N < p < \frac{N}{\sqrt{\log N}}$

$$\Delta^2(p) = \frac{Np}{4}\left(1 + O\left(\frac{1}{\sqrt{\log N}}\right)\right)$$

if C is a sufficiently large positive number.

§ 3. The values of a random trigonometrical polynomial at well spaced points

In this § we shall consider the sum

$$T(\alpha, S) = \sum_{\nu=1}^{D} |S(\alpha_\nu)|^2 \tag{3.1}$$

where $\alpha_1, \alpha_2, \ldots, \alpha_D$ are real numbers "well spaced" in the sense of Davenport and Halberstam, satisfying

$$0 < \alpha_1 < \alpha_2 < \ldots < \alpha_D < 1 \quad \text{and}$$

$$\alpha_{\nu+1} - \alpha_\nu \geqq \delta > 0 \quad \text{for } \nu = 1, 2, \ldots, D-1 \tag{3.2}$$

and $S(\alpha)$ is the random trigonometric polynomial

$$S(\alpha) = \sum_{n=1}^{N} \varepsilon_n e^{2\pi i n \alpha} \tag{3.3}$$

where $\varepsilon_1, \ldots, \varepsilon_N$ are independent random variables, each taking on the values 1 and 0 with probability $\frac{1}{2}$.

We first evaluate the expectation of $T(\alpha, S)$. We have clearly

$$T(\alpha, S) = \sum_{n=1}^{N} \sum_{m=1}^{N} \varepsilon_n \varepsilon_m \sum_{\nu=1}^{D} e^{2\pi i (n-m)\alpha_\nu} \tag{3.4}$$

and thus

$$E(T(\alpha, S)) = \frac{1}{2} \sum_{\nu=1}^{D} \left(\frac{N}{2} + \sum_{l=1}^{N-1} (N-l) \cos 2\pi l \alpha_\nu \right) + \frac{ND}{4}. \tag{3.5}$$

Now it is well known that

$$\frac{N}{2} + \sum_{l=1}^{N-1} (N-l) \cos 2\pi l \alpha_\nu = \frac{\sin^2 N\pi\alpha_\nu}{2 \sin^2 \pi\alpha_\nu}. \tag{3.6}$$

As a matter of fact the formula (3.6) is well known as a formula for Fejér's kernel of the arithmetic means of Fourier series.

It follows from (3.5) and (3.6) that

$$E(T(\alpha, S)) = \frac{1}{4} \sum_{\nu=1}^{D} \frac{\sin^2 N\pi\alpha_\nu}{\sin^2 \pi\alpha_\nu} + \frac{ND}{4}. \tag{3.7}$$

Let us now consider the special case when $\alpha_Q^* = (\alpha_1^*, \ldots, \alpha_D^*)$ is the set of all numbers $\frac{a}{q}$ with $(a, q) = 1$, $1 \leqq a \leqq q$, $1 < q \leqq Q \leqq N$. It is easy to see that

$$\sum_{q \leqq Q} \sum_{\substack{a=1 \\ (a,q)=1}}^{q} \frac{\sin^2 N\pi \frac{a}{q}}{\sin^2 \pi \frac{a}{q}} = O(Q^3) \tag{3.8}$$

thus, denoting by $\varphi(q)$ the number of numbers $a < q$ relatively prime to q, we have

$$E(T(\alpha_Q^*, S)) = \frac{N}{4}\sum_{q=1}^{Q}\varphi(q) + O(Q^3). \tag{3.9}$$

As however

$$\sum_{q=1}^{Q}\varphi(q) = \frac{3Q^2}{\pi^2} + O(Q\log Q) \tag{3.10}$$

it follows that

$$E(T(\alpha_Q^*, S)) = \frac{3Q^2N}{4\pi^2} + O(NQ\log Q) + O(Q^3). \tag{3.11}$$

It follows that for $Q = o(N)$ there exists for each $\varepsilon > 0$ a sequence S_N for which

$$T(\alpha_Q^*, S_N) > \frac{3Q^2N(1-\varepsilon)}{4\pi^2}. \tag{3.12}$$

Thus the estimate

$$\sum_{q\leqq Q}\sum_{\substack{a=1\\(a,q)=1}}^{q}\left|S\left(\frac{a}{q}\right)\right|^2 = O(N^2) \tag{3.13}$$

which according to the theorem of Davenport and Halberstam is valid for $Q \leqq \sqrt{N}$ cannot be valid if Q is of larger order of magnitude than $\sqrt{N}$. By evaluating the variance of $T(\alpha, S)$ one can prove even more, namely that $T(\alpha_Q^*, S_N) \sim \sim \frac{3Q^2N}{4\pi^2}$ for all except $o(2^N)$ sequences S_N, if $\frac{1}{Q} = o(1)$ and $\frac{Q}{N} = o(1)$. In particular one can prove that

$$D\left(\sum_{q\leqq\sqrt{N}}\sum_{\substack{a=1\\(a,q)=1}}^{q-1}\left|S\left(\frac{a}{q}\right)\right|^2\right) = O(N^{3/2}) \tag{3.14}$$

which implies that except for at most $O\left(\frac{2^N\log N}{N}\right)$ exceptional sequences

$$\sum_{q\leqq\sqrt{N}}\sum_{\substack{a=1\\(a,q)=1}}^{q-1}\left|S\left(\frac{a}{q}\right)\right|^2 \sim \frac{3N^2}{4\pi^2}. \tag{3.15}$$

Let us summarize now our results: Theorem 1 shows that the estimate

$$R(Q) = O(N^2) \tag{3.16}$$

cannot hold if Q is of larger order of magnitude than $\sqrt{N\log N}$. It remains an open question whether (3.16) holds if $\sqrt{N} \leqq Q \leqq \sqrt{N\log N}$. However, (3.11) shows that even if (3.16) is true for the range $\sqrt{N} \leqq Q \leqq \sqrt{N\log N}$ it cannot be proved by the methods used up to now, as all these methods gave estimates for $R(Q)$ through estimating $T(\alpha_Q^*, S)$.

§ 4. Some open problems

Let S_N denote a subsequence of the sequence $\{1, 2, \ldots, N\}$ which contains at least cN elements $(0<c<1)$. Let $Y(\alpha, \varepsilon)$ where $0<\varepsilon<1$ and $1/2 \leqq \alpha < 1$ denote the number of those primes $p \leqq N^\alpha$ for which at least $p\varepsilon$ residue classes mod p do not contain any element of S_N. It follows already from Linnik's result (1.1) that $Y\left(\frac{1}{2}, \varepsilon\right)$ is bounded, namely that

$$Y\left(\frac{1}{2}, \varepsilon\right) \leqq \frac{20\pi}{c\varepsilon^2}. \tag{4.1}$$

From (1.12) one obtains the slightly better estimate

$$Y\left(\frac{1}{2}, \varepsilon\right) \leqq \frac{\pi+1}{\varepsilon c}. \tag{4.2}$$

As regards $Y(\alpha, \varepsilon)$ with $1/2<\alpha<1$ we get from (1.11) the estimate

$$Y(\alpha, \varepsilon) \leqq \frac{N^{2\alpha-1}}{\varepsilon c} + \frac{\pi}{\varepsilon c}. \tag{4.3}$$

It seems probable that (4.3) is far from being best possible; it is an open problem whether $Y(\alpha, \varepsilon)$ is bounded for every α with $\frac{1}{2}<\alpha<1$, or not. Of course, $Y(1, \varepsilon)$ is not bounded: as a matter of fact if S_N is the sequence of numbers $\leqq Nc \left(0<c<\frac{1}{2}\right)$ and $0<\varepsilon<\frac{1}{2}$ then for all primes p with $\frac{cN}{1-\varepsilon}<p<N$ at least $p\varepsilon$ residue classes mod p do not contain any element of S_N, and thus

$$Y(1, \varepsilon) \geqq \frac{N}{\log N}\left(1-\frac{c}{1-\varepsilon}\right)+O\left(\frac{N}{\log^2 N}\right).$$

Another related problem is the following: if $0<\varepsilon<1$ let S_N be a subsequence of the sequence $\{1, 2, \ldots, N\}$ such that for every p with $A_\varepsilon<p<N^\alpha$ where $A_\varepsilon>0$, $0<\alpha<1$ there are at least εp residue classes mod p which do not contain any element of S_N. What is the maximum $M_N(\varepsilon, \alpha)$ of the number of terms of such a sequence S_N? It is easy to show that for each ε with $0<\varepsilon<1/2$ $M_N(\varepsilon, 1) \geqq [\sqrt{N}]$. As a matter of fact let S_N denote the sequence of squares $\leqq N$. Clearly if b is a quadratic non-residue mod p, then there is no element of the sequence $1^2, 2^2, \ldots, k^2, \ldots$ which is congruent to b mod p; thus for each p the number of empty residue classes is at least $\frac{p-1}{2}$ if $p \geqq 3$.

References

[1] YU. V. LINNIK, The large sieve, *Comptes Rendus (Doklady) de l'Académie des Sci. de l'URSS*, **30** (1941), 292 – 294.
[2] YU. V. LINNIK, Remark on the least quadratic non-residue, *Comptes Rendus (Doklady) de l'Académie des Sci. de l'URSS*, **36** (1942), 131.
[3] A. RÉNYI, On the representation of an even number as the sum of a prime and of an almost prime, *Isvestiya Akad. Nauk SSSR*, Ser. Math., **12** (1948), 57 – 78 (in Russian), (see also *American Math. Soc.*, Translation Series 2., **19** (1962), 299 – 321).
[4] P. T. BATEMAN – S. CHOWLA – P. ERDŐS, Remarks on the size of $L(1, \chi)$ *Publ. Math.*, **1**(1950), 165 – 182.
[5] M. B. BARBAN, The large sieve and its applications in number theory, *Uspechi Mat. Nauk*, **21** (1966), 51 – 102, (in Russian).
[6] H. HALBERSTAM – K. F. ROTH, *Sequences*, Vol. I. (Oxford, Clarendon Press, 1966). Ch. IV. § 10. The larges sieves of Linnik and Rényi (pp. 224 – 237).
[7] A. RÉNYI, On the large sieve of Yu. V. Linnik, *Compositio Math.*, **8** (1950), 68 – 75.
[8] A. RÉNYI, Un nouveau théorème concernant les fonctions indépendantes et ses applications à la théorie des nombres, *Journal Math. Pure et Appl.*, **28** (1949), 137 – 149.
[9] A. RÉNYI, Sur un théorème général de probabilité, *Annales de l'Institut Fourier*, **1** (1950), 43 – 52.
[10] A. RÉNYI, On a general theorem in probability theory and its application in the theory of numbers, *Zprávy o společnem 3. sjezdu matematikařu československých a 7. sjezdu matematikařu polskich*, Praha 1950. 167 – 174.
[11] A. RÉNYI, On the probabilistic generalization of the large sieve of Linnik, *MTA Mat. Kut. Int. Közl.*, **3** (1958), 199 – 206.
[12] A. RÉNYI, New version of the probabilistic generalization of the large sieve, *Acta Math. Acad. Sci. Hung.*, **10** (1959), 217 – 226.
[13] K. F. ROTH, On the large sieve of Linnik and Rényi, *Mathematika*, **12** (1965), 1 – 9.
[14] E. BOMBIERI, On the large sieve, *Mathematika*, **12** (1965), 201 – 225.
[15] H. DAVENPORT – H. HALBERSTAM, The values of a trigonometrical polynomial at well spaced points, *Mathematika*, **13** (1966), 91 – 96.
[16] P. X. GALLAGHER, The large sieve, *Mathematika*, **14** (1967), 14 – 20.
[17] P. ERDŐS, Remarks on number theory V., *Mat. Lapok*, **17** (1966), 135 – 155. (In Hungarian).