COMPOSITIO MATHEMATICA

ALFRED RÉNYI

On the large sieve of Ju V. Linnik

Compositio Mathematica, tome 8 (1951), p. 68-75

<http://www.numdam.org/item?id=CM_1951__8__68_0>

On the large sieve of Ju V. Linnik

by

Alfred Rényi

Budapest

§ 1. Ju. V. Linnik [1]) invented an ingenious method — called by him the large sieve — which enabled him to prove the following theorem:

Theorem 1. Let us choose Y arbitrary primes $p_1, p_2, \ldots p_Y$ where $p_i < \sqrt{N}$; $i = 1, 2, \ldots Y$, let further $f(p)$ denote a positive function, $f(p) < p$, and let us put

$$\tau = \min_{i=1.\,2,\ldots Y} \frac{f(p_i)}{p_i}.$$

If we delete from the sequence $1, 2, \ldots N$ every integer belonging to one of $f(p_i)$ fixed classes of residues mod p_i, $i = 1, 2, \ldots Y$, the number of integers which remain does not exceed

$$\frac{20 \cdot \pi \cdot N}{\tau^2 \cdot Y}.$$

This theorem can be stated also in the following equivalent form:

Theorem 1*b*. Let us consider an arbitrary sequence $n_1 < n_2 < n_3 < \ldots < n_Z \leqq N$ of positive integers, let us denote further

$$\tau = \min_{p<\sqrt{N}} \frac{f(p)}{p}.$$

For every prime $p < \sqrt{N}$ with the possible exception of at most

$$\frac{20\,\pi N}{\tau^2 Z}$$

exceptional primes, the integers $n_1, n_2, \ldots n_Z$ occupy at least $p - f(p)$ different residue classes mod p.

[1]) Ju. V. Linnik, The large sieve, Comptes Rendus (Doklady) de l'Academie des Sciences de l'URSS, 1941, XXX, No. 4, 292—294 pp.

This result of Linnik has been generalized by the author in a previous paper [2]). The generalized large sieve has been the main tool in the proof given by the author of the theorem that there exists a numerical constant K such that every integer N can be represented in the form $N = p + P$, where p is prime and P has at most K prime factors (multiple factors counted multiply).

The content of Theorem 1*b* may be characterized as follows. If the sequence of integers $n_1, n_2, \ldots n_Z$, $n \leqq N$ is sufficiently dense (i.e. Z/N is not too small), for almost every prime $p < \sqrt{N}$ almost every residue class mod p is represented among the numbers n_i, $i = 1, 2, \ldots Z$. The first step of generalization consists in proving that the numbers of the sequence n_i are „approximately equally" distributed among the different residue classes mod p, for almost all primes $p < \sqrt{N}$. More exactly, it can be proved [3]) that the following theorem holds:

Theorem 2. Let us consider an arbitrary sequence of integers, $n_1 < n_2 < n_3 \ldots < n_Z \leqq N$; let $f(p)$ denote a positive function, $f(p) < p$ and let us put

$$\tau = \min_{p<\sqrt{N}} \frac{f(p)}{p}. \tag{1}$$

Let $Q(p)$ denote a positive function and let us denote

$$Q = \max_{p<\sqrt{N}} Q(p). \tag{2}$$

If $Z(p, r)$ denotes the number of integers n_i which are congruent to r mod p, we have for every prime $p < \sqrt{N}$, except for at most

$$\frac{3\pi N^2 Q^3}{2Z^2\tau^{3/2}}$$

„exceptional" primes

$$\left| Z(p, r) - \frac{Z}{p} \right| < \frac{Z}{p \cdot Q(p)}$$

for every residue r mod p with the possible exception of $f(p)$ „irregular" residue classes.

---

[2]) A. Rényi, On the representation of even numbers as the sum of a prime and an almost prime number, Bulletin (Izvestia) de l'Academie des Sciences de l'URSS, Ser. math. 12, No. 1, 1948, 57—58 pp.

[3]) This is a special case of a general theorem, proved in the paper of the author, cited above, p. 61, Lemma 1.

The proof of Theorem 2 given in the paper cited above, is a straightforward generalization of the method of Linnik. However Theorem 2 makes it clear that the large sieve is essentially a statistical statement, and suggests, that it can be found a method of probability theory by which the large sieve can be proved. As a matter of fact I succeeded in founding such a method, which furnishes a new proof of the large sieve, completely different from the original method of Linnik, the result being even stronger in some respect. The purpose of the present paper is to present this new method. Instead of aiming at giving the most general form of the large sieve, which can be obtained by the new method, we shall try to give a clear exposition of the fundamental ideas of this method.

§ 2. There have been made many attempts to apply probability methods in number theory. The starting point of all such investigations is the simple remarks, that the distributions of the infinite sequence of integers in residue classes with respect to relatively prime moduli are independent in the sense of probability theory. The difficulties in making advantage of this fact may be described most simply in the language of the axiomatic theory of Kolmogoroff [4]: The set E of „elementary events" may be chosen as the set of all positive integers. The field F of „random events" (i.e. a set of subsets of E satisfying the Haudorff axioms [5])) shall be chosen as the set of finite or infinite sequences of integers $\{n_1, n_2, \ldots n_k\} = A$ for which, putting

$$A(x) = \sum_{n_k \leqq x} 1,$$

the limit

$$P(A) = \lim_{x \to \infty} \frac{A(x)}{x} \tag{3}$$

exists. The field F, together with the probability function $P(A)$ defined by (3), satisfies the first five axioms of Kolmogoroff, but the difficulty lies in the fact, that the sixth axiom, the socalled axiom of continuity, is not satisfied. As a matter of fact this axiom states that if A_n, $n = 1, 2, 3, \ldots$ is a sequence of sets

[4]) A. Kolmogoroff, Grundbegriffe der Wahrscheinlichkeitsrechnung, Ergebnisse der Mathematik und ihrer Grenzgebiete, II. 3, Berlin 1933, p. 2.

[5]) F. Hausdorff, Mengenlehre, 1927, p. 78.

belonging to the field F, each A_n being contained in the preceding set A_{n-1}, and if the product of all sets A_n is empty, then

$$\lim_{n\to\infty} P(A_n) = 0$$

If we choose for A_n the set of all integers $\geqq n$, we see that this axiom is not satisfied in our case. It may be remarked also that F is not a Borel field of sets. For instance let B_n denote the set of integers

$$\{2^{2^n},\ 2^{2^n}+1,\ 2^{2^n}+2,\ \ldots\ 2^{2^{n+1}}-1\}.$$

It is easy to see that the sum of all sets B_n does not belong to F, because if

$$B(x) = \sum_{\substack{k \leqq x \\ k \in \sum B_n}} 1$$

we have

$$\underline{\lim_{x\to\infty}}\ \frac{B(x)}{x} = \tfrac{1}{3} \text{ and } \overline{\lim_{x\to\infty}}\ \frac{B(x)}{x} = \tfrac{2}{3}.$$

These remarks show, that we have to choose an other way. As a matter of fact, all difficulties vanish if we restrict the set E to the set of integers $1, 2, \ldots N$ with a fixed N, choose F as the set of all subsets $A = \{n_1, n_2, \ldots n_k\}$ of $\{1, 2, \ldots N\}$ and put $P(A) = \frac{k}{n}$. But in this case a new difficulty arises: the distributions of the sequence $1, 2, \ldots N$ in residue classes with respect to two relatively prime integers P and Q cease to be independent in general (except if both P and Q are divisors of N); these distributions however are in some sense „almost" independent, if P and Q are small with respect to N, and our method can be characterized by saying that it is based on a systematic use of this „almost" independence. The method is also connected with the theory of „quasi-orthogonal" systems of functions [6]) but we shall present the method in a simple direct way, without using general concepts.

§ 3. Let N denote a positive integer, which shall be fixed during this §. Let A denote an other positive integer $A < N$.

[6]) R. P. Boas Jr., A general moment problem, American Journal of Math. 63, 1941, 361—370 pp. See also R. Bellman, Almost orthogonal series, Bulletin of the American Math. Soc. 50, 1944, 517—519 pp.

We define the following system of functions in the interval (0, 1):

$$f_{p,k}(x) = \begin{cases} 1 \text{ if } [Nx] \equiv k \bmod p \\ 0 \text{ if } [Nx] \not\equiv k \bmod p \end{cases} \tag{4}$$

(here $[y]$ denotes the integral part of y), where p runs over all primes $\leqq A$, and k takes the values 0, 1, 2 ... $p-1$. Let us put

$$F_{p,k}(x) = \sqrt{p}.\,(f_{p,k}(x) - \frac{1}{p}) \tag{5}$$

It follows by some simple calculations, that the functions, defined by (5), satisfie the following three relations:

$$\int_0^1 F_{p,k}^2(x)dx = 1 - \frac{1}{p} + \frac{\vartheta A}{N}, \text{ where } |\vartheta| \leqq 2. \tag{6}$$

$$\text{if } p \neq p' \int_0^1 F_{p,k}(x)F'_{p'k'}(x)dx = \frac{\lambda A}{N}, \text{ where } |\lambda| \leqq 4, \tag{7}$$

$$\text{if } k \neq k' \int_0^1 F_{p,k}(x)F_{p,k'}(x)dx = -\frac{1}{p} + \frac{\mu}{N}, \text{ where } |\mu| \leqq 4. \tag{8}$$

Clearly the values of ϑ, λ and μ in (6), (7) and (8) depend on the indices p, k, p', k', but it will be not necessary to indicate this explicitly.

Now let us consider an arbitrary sequence of integers, $n_1 < n_2 < n_3 < \ldots < n_Z < N$, and let us denote by E the set of those points x of the interval (0,1) for which $[Nx] \equiv n_j$ for some $j \leqq Z$. Let $E(x)$ denote the characteristic function of the set E (i.e. $E(x) = 1$ if x belongs to E and $E(x) = 0$ if not), and let us put

$$a_{pk} = \int_0^1 E(x)F_{pk}(x)dx. \tag{9}$$

Now we have clearly

$$\int_0^1 \left(E(x) - \sum_{p<A} \sum_{k=0}^{p-1} a_{pk}F_{pk}(x)\right)^2 dx \geqq 0. \tag{10}$$

Multiplying out in (10) and using (6), (7) and (8), we obtain

$$0 \leqq \int_0^1 E^2(x)dx - \left(1 - \frac{2A}{N}\right)\left(\sum_{p<A} \sum_{k=0}^{p-1} a_{pk}^2\right) + \frac{4A}{N}\left(\sum_{p<A} \sum_{k=0}^{p-1} |a_p|\right)^2. \tag{11}$$

Now we have evidently

$$\int_0^1 E^2(x)dx = \frac{Z}{N}. \tag{12}$$

For the sake of brevity let us put

$$\omega = \sum_{p<A} \sum_{k=0}^{p-1} a_{pk}^2. \tag{13}$$

Using the inequality of Cauchy-Schwarz, we obtain

$$\left(\sum_{p<A} \sum_{k=0}^{p-1} |a_{pk}|\right)^2 \leqq A^2\omega \tag{14}$$

Thus we obtain from (11)

$$\omega \leqq \frac{Z}{N\left(1 - \frac{4A^3 + 2A}{N}\right)}. \tag{15}$$

Let us suppose now, that $A < \sqrt[3]{\frac{N}{12}}$. It follows from (15), that

$$\omega = \sum_{p<A} \sum_{k=0}^{p-1} a_{pk}^2 < \frac{2Z}{N}. \tag{16}$$

But it is easy to see, that if $Z(p, k)$ denotes the number of those integers of the sequence n_j, $j = 1, 2, \ldots Z$ which are congruent to k mod p, we have

$$a_{pk} = \frac{\sqrt{p}}{N}\left(Z(p, k) - \frac{Z}{p}\right). \tag{17}$$

Thus (16) gives

$$\sum_{p<A} p \cdot \sum_{k=0}^{p-1}\left(Z(p, k) - \frac{Z}{p}\right)^2 \leqq 2NZ. \tag{18}$$

The fundamental inequality (18) is the source of the following

Theorem 3. Let us consider an arbitrary sequence of integers, $n_1 < n_2 < n_3 < \ldots < n_Z < N$; let $f(p)$ denote a positive function, $f(p) < p$ and let us put

$$\tau = \min_{p<\sqrt[3]{\frac{N}{12}}} \frac{f(p)}{p},$$

let further $Q(p)$ denote a positive function and let us denote

$$Q = \max_{p < \sqrt[3]{\frac{N}{12}}} Q(p).$$

If $Z(p, k)$ denotes the number of integers n_j which are congruent to k mod p, we have for every prime $p < \sqrt[3]{\frac{N}{12}}$, except for at most

$$\frac{2NQ^2}{Z\tau} \tag{19}$$

„exceptional" primes

$$\left| Z(p, k) - \frac{Z}{p} \right| < \frac{Z}{p \cdot Q(p)} \tag{20}$$

for every residue k mod p, with the possible exception of $f(p)$ irregular residue classes.

Proof of *Theorem* 3. Let us suppose, that there are Y exceptional primes $p < \sqrt[3]{\frac{N}{12}}$, for which (17) is not satisfied for at least $f(p)$ residue classes. For such an exceptional prime we have

$$p \cdot \sum_{k=0}^{p-1} \left(Z(p, k) - \frac{Z}{p} \right)^2 \geqq \frac{p \cdot f(p) Z^2}{p^2 Q^2(p)} \geqq \frac{Z^2 \tau}{Q^2}.$$

Thus we obtain from (18) that

$$Y \cdot \frac{Z^2 \tau}{Q^2} \leqq 2ZN,$$

which proves Theorem 3.

Clearly Theorem 3 is of exactly the same type as Theorem 2. It is stronger in that the number of exceptional primes, given by (19) is less than the number of exceptional primes in Theorem 2. As regards the range of „sieving primes" it is weaker, but this does not make any difference in the applications. It may be mentioned, that by choosing $Q(p) \equiv 1$, we obtain a direct improvement of Linnik's theorem, namely the following

Corrolary 1. Let us consider a sequence of positive integers $n_1 < n_2 < n_3 < \ldots < n_Z < N$. Let $f(p)$ denote a positive func-

tion, $f(p) < p$, and let us put $\tau = \min_{p < \sqrt[3]{\frac{N}{12}}} \frac{f(p)}{p}$. For every prime $p < \sqrt[3]{\frac{N}{12}}$, except for at most

$$\frac{2N}{Z\tau}$$

exceptional primes, the integers n_j occupy at least $p - f(p)$ different residue classes mod p.

As an other special case let us consider the distribution of primes in arithmetic progressions. Choosing for the sequence n_j the sequence of primes $\leqq N$, we have the following

Corrolary 2. Let $\pi(N, p, k)$ denote the number of primes $\leqq N$ in the progression $px + k$, $x = 1, 2, 3, \ldots p$ prime, $(p, k)=1$. For every prime $p < \sqrt[3]{\frac{N}{12}}$, with the possible exception of $O(\sqrt[4]{N} \cdot \log N)$ exceptional primes, we have

$$\pi(N, p, k) = \frac{\pi(N)}{p-1} + O\left(\frac{N}{\log N \cdot p^{3/4}}\right) \tag{21}$$

for every residue k mod p, with the possible exception of at most $p^{3/4}$ irregular residues k.

It is well known, that the distribution of zeros of the L-functions of Dirichlet is closely connected with the distribution of primes in progressions, and every result regarding the first or the second problem has its consequences regarding the other problem. Thus it can be easily understood, that by means of theorems of the type of Corrolary 2 there can be obtained „statistical" theorems regarding the zeros of the L-functions. Such results have been given in the paper cited above [7]). Using the improved form of the large sieve as given in the present paper, these results can also be improved.

Finally it may be mentioned, that (18) can be considered as a special case of a general theorem of probability theory, which will be published elsewhere [8]).

Mathematical Institute of the University of Budapest (Hongarije).
(Received 15 February 1949).

---

[7]) See footnote [2]).

[8]) A. Rényi, Un nouveau théorème concernant les fonctions indépendantes et ses applications à la théorie des nombres, to be published in the Journal de Mathématiques, 1949.