ber theory helped him when he was working in the field of the theory of probability. The very titles of Linnik's papers (the ergodic method in number theory; the dispersion method) indicated the influence of the theory of probability upon his research in number theory. Of course, the point is not that any ready results were transferred from one field to another, but only that there was some influence of ideas from the theory of probability upon the creation of new, original methods in number theory.

Yuri V. Linnik possessed a lucky ability to attract talented disciples. He skilfully directed them to the study of problems which were both difficult and important for the development of science. As a director of studies, Yuri V. Linnik was generous in giving both ideas and advice, always having time for working discussions with his disciples and colleagues. At the same time he was exigent, awaiting with interest those results, which, in his opinion, were bound to be a success. In relations with his disciples, Yuri V. Linnik was solicitous not only as a teacher, but also as a senior colleague, trying to be helpful also in everyday life, when necessary.

Among Linnik's disciples of different periods, there were: the prematurely deceased Hungarian Academician A. Renyi, Academician of the Lithuanian SSR J. Kubilius, A. V. Malyshev, A. I. Vinogradov, B. F. Skubenko, B. M. Bredikhin, A. N. Andrianov and others — in the field of number theory, and V. V. Petrov, I. A. Ibragimov, Academician of the Lithuanian SSR V. Statulavicius, O. V. Shalayevsky and many others — in the field of the theory of probability and mathematical statistics.

The scientific merits of Yuri V. Linnik were generally recognized. In 1947 he was awarded a State Prize, in 1970 he became the Lenin Prize Winner. In 1953 he was elected a Corresponding Member, and in 1964 a Full Member of the Academy of Sciences of the USSR. In 1970 he was given the rank of Hero of Socialist Labour. Since the year of its founding, 1959, until 1965 he was the President of the Leningrad Mathematical Society. Yuri V. Linnik was elected a Fellow of the International Statistical Institute, a Foreign Member of the Swedish Academy of Sciences, and obtained the title of Doctor honoris causa of Paris University. He was a member of the editorial boards of several scientific periodicals, including "Acta Arithmetica". Linnik's "Selected Writings" are planned to be published.

Yuri V. Linnik combined the extraordinary intensity of scientific creative work with a vast scope of interests. His many-sided endowments were astonishing: he was greatly interested in belle-lettres, especially poetry and memoires, as well as in history, especially military history. He spoke seven languages fluently and wrote witty poetry in Russian, English, German and French.



ACTA ARITHMETICA
XXVII (1975)

# Yu. V. Linnik's works in number theory

by

A. V. Malyshev (Leningrad)

**1. Ergodic method in number theory.** Yu. V. Linnik's first works were related to the analytic theory of quadratic forms. He investigated there the problem of representation of numbers $m$ by positive ternary quadratic forms $f$, i.e. the problem of solution of Diophantine equation

$$f(x, y, z) = m \tag{1}$$

in integers $x, y, z$. It dealt with the conditions of solvability of the equation (1) and the number of its solutions $R(f, m)$ (or, in other words, with the number of integral points on the ellipsoid (1), the problem of distribution of these points over the surface of the ellipsoid naturally arising). Analogous problems for quadratic forms of $n \geqslant 4$ variables were successfully solved by the traditional analytic methods. Nevertheless in the case of $n = 3$, connected with the important problem of determining a crystallic lattice by its distances, those methods ceased to work, and the problem did not permit any solution in spite of the efforts of many scholars.

Having used as a tool the arithmetics of quaternions and hermitions for the purpose of investigating the problem, Linnik created an original analytic-algebraic method, which, in further development substantially expanding the sphere of its applications, was named the ergodic method in number theory. The method was described in articles [2]–[6], [62], [63], [69], [71], [76]–[79], [81], [84], [86], [88], [89], [102], [113], [148], [168], [224], partially in [46], [115], [152], and also in monograph [VII] basically summing up the whole field of investigation (several problems were treated with more detail in A.V. Malyshev's monograph *On the representations of integers by positive quadratic forms*, Steklov Mathematical Institute works, LXV, 1962).

The fundamentals of the method were given by Linnik in paper [6], outstanding in its depth and sophistication, and making a summit of his creative work. In that very complicated article he succeeded in estimating $R(f, m)$ from below (and, in particular, in finding conditions for representability of large numbers $m$ by the form $f$) in the case of forms which have odd determinants and are representable by the sum of three squares, the so-called "convenient" forms, and suggested the ways for investigating the problem for arbitrary forms.

The way was later found to obtain not only inequalities, but also asymptotic formulae (for $m\to\infty$), for the quantities mentioned above (say, $R(f,m)$). The most remarkable application of the ergodic method is the widely known Linnik's theorem [102] (see also [VII] and [71]) on the asymptotic uniformity of distribution of integral points on the sphere with increasing radius.

Let us present the idea of the proof of that wonderful theorem, thus demonstrating also the scheme of the ergodic method. It is sufficient to consider only the primitive points on the sphere $x^2+y^2+z^2 = m$, assigning to them primitive integral vectors $L = xi+yj+zk$ under condition

$$N(L) = m. \tag{2}$$

Their number, according to the theorems of Gauss and Siegel, is

$$r(m) > \varkappa_\varepsilon m^{\frac{1}{2}-\varepsilon}, \quad \text{if} \quad m \equiv 1, 2 \pmod 4, \quad \equiv 3 \pmod 8. \tag{3}$$

Now let $q$ be a fixed prime under condition

$$\left(\frac{-m}{q}\right) = 1. \tag{4}$$

Then for any natural number $s$ there exists an integer $l$ such that $l^2+m \equiv 0 \pmod{q^s}$, and thus for every primitive integral vector $L$ with the norm $m$ we have

$$l+L = BU, \quad B = Q_1\cdot\ldots\cdot Q_s, \quad N(Q_i) = q \quad (i = 1, \ldots, s), \tag{5}$$

where $Q_1, \ldots, Q_s, U$ are integral quaternions; if $Q_1, \ldots, Q_s$ are supposed to be primary, then they are defined uniquely by the vector $L$. Rotating the vector $L$ successively by means of the quaternions $Q_1, \ldots, Q_s$:

$$L' = Q_1^{-1}LQ_1, \quad L'' = Q_2^{-1}L'Q_2, \quad \ldots, \quad L^{(s)} = Q_s^{-1}L^{(s-1)}Q_s$$

and taking (5) into account, we obtain the chain $(Z_L)$ of primitive integral vectors with the norm $m$:

$$(Z_L) \quad L\to L'\to L''\to\ldots\to L^{(s)}. \tag{6}$$

Choose $s = \left[\frac{\log r(m)}{\log q}\right]$, and consider the chains $(Z_L)$ starting with all $r(m)$ vectors $L$. It turns out that all the chains, with the possible exclusion of $o(r(m))$, have the "ergodic" property, i.e. the vectors of the chain are distributed uniformly (at $m\to\infty$) over the surface of the sphere.



The proof of "ergodicity" (from which the theorem on uniform distribution of primitive integral points on the sphere follows immediately) is based on the following lower estimate of the number of different $B$'s in $r(m)$ equalities of the form (5): the number is greater than

$$\varkappa_\varepsilon \frac{r(m)}{m^\varepsilon}, \quad \varkappa_\varepsilon > 0 \tag{7}$$

for any $\varepsilon > 0$. Here we have the most important key point of the method. The estimate (7) is proved by rather complicated arguments which use essentially the vector rotations theory by B. A. Venkov. Lately, Linnik [224] has suggested a variant of his method which permits avoidance of estimate (7).

Linnik's investigations were generalized by his disciple A. V. Malyshev to the case of positive ternary quadratic forms with odd relatively prime invariants $[\Omega, \Delta]$. It is a pity that in the general case only estimates instead of asymptotic formulae were obtained.

Linnik [77]–[79] (see also [VII] and [63]) applied the ergodic method to the proof of asymptotically (for $m\to\infty$) uniform distribution (in the sense of Lobachevsky metric) of integral points in fundamental domain of parted hyperboloid

$$xz-y^2 = m, \quad |2y| \leqslant x \leqslant z, \quad m > 0 \tag{8}$$

and his disciple B. F. Skubenko extended this work to the case of unparted hyperboloid ($m < 0$).

There is no doubt that in the questions of representing numbers by ternary quadratic forms, positive as well as indefinite, the ergodic method did not exhaust its possibilities. As to the problems arising here and solvable by this method, see [VII], pp. 202–204.

The study of the distribution of integral points in domain (8) may be treated as information on the distribution of ideal classes of quadratic fields. In his report [113] (see also [VII], Chapters VII and IX) to the III All-Union Mathematical Congress Linnik suggested a vast program for transferring those results to arbitrary algebraic fields. It is a pity that there only an auxiliary result on the distribution of integral $n$th order matrices with given determinant ([148], [168], [VII], Chapter VIII; Trudy Mat. Inst. Steklov 80 (1965), pp. 129–144), was obtained.

**2. The large sieve.** Immediately after the research work in the arithmetics of ternary quadratic forms, summed up in paper [6], Linnik published a minor note [7], which was destined to have a great future. There he founded a new method in the analytic number theory, which he named "the large sieve". The term means the operation of eliminating some residue classes with respect to given prime moduli $p_i$ from a given set of integers, the number of the classes being permitted to increase with $p_i$ (just by the latter his sieve differs from that of V. Brun). In the note [7] he elaborated a simple and elegant analytic apparatus for estimating the number of numbers, both those belonging to the set and those left after sieving.

Linnik published only one small article [11] on this method, in which the following theorem was proved: for any $\varepsilon > 0$ and arbitrary large $N$, the upper bound for number of primes $p$ contained in the interval $(N^\varepsilon, N)$ and having a minimal quadratic non-residue greater than $p^\varepsilon$, depends only on $\varepsilon$ (and does not depend on $N$).

Later Linnik's large sieve method was developed by his disciples and followers. Interesting applications of the method were made by the Hungarian academician A. Renyi (who died untimely in 1970), working under the guidance of Linnik. The important advance in, and, to a certain extent, the completion of Linnik's large sieve method was obtained in 1965 simultaneously and independently by the Italian mathematician E. Bombieri and Linnik's disciple A. I. Vinogradov (see Addendum I to the Russian translation of K. Prachar's book „Primzahlverteilung", Moscow, 1967).

From the numerous applications of the large sieve method let us select this one: let $\pi(x; D, l)$ be the quantity of prime numbers of the form $Dk+l$ not exceeding $x$; then for arbitrary constant $A > 0$ there exists a constant $c > 0$ such that

$$\sum_{D \leqslant \frac{\sqrt{x}}{\log^A x}} \max_{\substack{l (\mathrm{mod}\, D) \\ (l, D)=1}} \left|\pi(x; D, l) - \frac{\mathrm{li}\, x}{\varphi(D)}\right| = O\left(\frac{x}{\log^{cA} x}\right). \tag{9}$$

**3. The density theorems in the theory of Dirichlet $L$-functions and their applications.** Having created the large sieve method, Linnik successfully developed the theory of Dirichlet $L$-functions $L(s, \chi)$, where $\chi$ is a Dirichlet character (mod $D$), and its applications to the prime numbers theory.

It is known that many arithmetical consequences can be obtained from the extended Riemann hypothesis that all the non-trivial zeros of $L(s, \chi)$ (i.e. zeros under condition $0 \leqslant \mathrm{Re}\, s \leqslant 1$) are situated on the straight line $\mathrm{Re}\, s = \frac{1}{2}$. At the present time proof or disproof of this hypothesis seems rather unrealistic, even for the particular case of $L$-functions, namely, for Riemann zeta function $\zeta(s)$. However, as was pointed out by Hoheisel as far back as 1930, many propositions in the prime numbers theory can be derived from much weaker, but provable, statements, namely, the density theorems containing upper estimates for the number $N(\sigma, T)$ of those zeros of the $\zeta(s)$ function which are situated in the domain

$$\sigma \leqslant \mathrm{Re}\, s \leqslant 1, \quad |t| \leqslant T \tag{10}$$

where $\sigma > \frac{1}{2}$ and $T$ is sufficiently large.

Linnik has generalized the density theorems for $L$-functions and obtained from them a number of important arithmetical consequences ([16]–[18], [22]–[26], [28]–[33], [53], [55], [58], [64], [68]). The generalization was twofold. Firstly, for a great modulus $D$ he estimated the number $N(D)$ of all functions $L(s, \chi)$ with characters $\chi(\mathrm{mod}\, D)$, which have zeros in certain special domain for $s$ depending on $D$. That allowed him to prove, among other arithmetical consequences, the following remarkable theorem on the least prime number in arithmetic progression: if $l$ and $D > 1$ are two relatively prime integers, then there exists a prime $p$ of the form $Dk+l$ such that

$$p < D^c, \tag{11}$$

where $c$ is an absolute constant. The summary of those results, with the addition of modern improvements, is to be found in Chapter X of Prachar's book cited above. Secondly, Linnik considered a direct generalization of Hoheisel's result, namely, an upper estimation for the number $N(\sigma, T; \chi)$ of zeros of function $L(s, \chi)$ in domain (10) (cf. Prachar, Ch. IX). That allowed him to give a new proof of the famous Vinogradov theorem on the representability of sufficiently large odd numbers by the sum of three primes (the so-called "ternary Goldbach problem"). Later Linnik solved the so-called "almost binary Goldbach problem", showing by the same method that all even integers are representable by the sum

$$n = p_1 + p_2 + 2^{t_1} + \ldots + 2^{t_s}, \tag{12}$$

where $p_1, p_2$ are primes, $t_1, \ldots, t_s$ are positive integers, and $s \leqslant c$, where $c$ is an absolute constant.

**4. The dispersion method in number theory.** We owe to Linnik the creation of one more mighty method in the analytic number theory, especially devised for solving additive problems of the binary type, which do not admit any use of the circle method in principle.

To this method, named the "dispersion method", articles [110], [111], [117], [125], [127], [129]–[131], [138], [140] are dedicated (they are generalized in monograph [III]) and also in the further articles [196], [199], [201], [210], [249], [253].

The main ideas of the method consist of introducing the concept of "dispersion" for the number of solutions of the binary equation, of deducing the basic inequality for the dispersion with the aid of a method like that of Vinogradov for estimating double sums, and, lastly, of applying a certain analogue of Chebyshev inequality. Let us describe a scheme of the dispersion method in the simplest case (for details see [III], pp. 5–28). Let $\{\varphi\}$ be a certain sequence of positive integers, with probable repetitions, let $D'$ run through a certain subset of the interval $(D) = [D_1, D_1+D_2]$ without repetitions, and let $\nu$ run through a certain subset of the interval $(\nu) = [\nu_0, \nu_0+\nu_0']$ independently of $D'$. We are interested in the number $r(n)$ of solutions of the binary type equation

$$n = \varphi + D'\nu. \tag{13}$$

If $U(m)$ is the number of solutions of equation $\varphi = m$, then

$$r(n) = \sum_{D'\epsilon(D)} \sum_{\nu\epsilon(\nu)} U(n-D'\nu). \tag{14}$$

Let us suppose that by some heuristic reasoning we can find some plausible asymptotic formula $A(n, D)$ for the number of solutions of the equation

$$n = \varphi + D\nu \tag{15}$$

with an arbitrary fixed $D$. Then the "dispersion" of solutions of equation (13), assuming the asymptotic formula $A(n, D)$ for equation (15), is equal to

$$V' = \sum_{D'\epsilon(D)} \Big(\sum_{\nu\epsilon(\nu)} U(n-D'\nu) - A(n, D')\Big)^2. \tag{16}$$

But it is evident that

$$V' \leqslant V = \sum_{D_1 \leqslant D \leqslant D_1+D_2} \Big(\sum_{\nu\epsilon(\nu)} U(n-D\nu) - A(n, D)\Big)^2, \tag{17}$$

and we have to know reasonably well — and this is crucial for the application of the method — the upper estimate for $V$ (and thereby for $V'$).

If $V'$ is sufficiently small, then we can turn to the $r(n)$ by classical Chebyshev arguments:

$$r(n) = \sum_{D'\epsilon(D)} \sum_{\nu\epsilon(\nu)} U(n-D'\nu) \approx \sum_{D'\epsilon(D)} A(n, D'). \tag{18}$$

The power of the dispersion method was demonstrated by Linnik when he solved ([117], [131], [140]) the classical Hardy–Littlewood problem of representing every sufficiently large number as the sum of a prime and two squares. He also obtained in [127] and [129] (see also [VII], Ch. VII) an asymptotic formula for the number of solutions of equation

$$n = p + x^2 + y^2, \tag{19}$$

where $p$ is a prime and $x, y$ are integers.

The dispersion method also permitted solution of another old problem, the so-called "Titchmarsh divisors problem", which consists of



finding an asymptotic formula (for $N \to \infty$) for the sum of a divisor function over "displaced" primes:

$$\sum_{p \leqslant N} \tau(p+l).$$

It is interesting to note that the formula were obtained later with the large sieve method (see Addendum I to Prachar's book cited above).

Linnik and his disciple B. M. Bredikhin also studied many other additive problems using the dispersion method (see, in particular Bredikhin's review in Russian Mathematical Surveys 20:2 (1965), pp. 89-130). Since then the dispersion method has been connected with ergodic ideas, which substantially expanded its possibilities and, in particular, led to an asymptotic formula in the generalized Hardy–Littlewood equation:

$$n = p + \varphi(x, y) \tag{20}$$

where $\varphi$ is an integral quadratic form.

Up to his last days Linnik (in cooperation with Bredikhin) was developing the dispersion method, and not all his results in this field have yet been published.

**5. Other investigations in number theory.** A great number of Linnik's articles on number theory (some of them very deep ones) are difficult to classify among the discussed domains. Let us dwell briefly upon the most interesting of them.

In his paper [20] (see also [69], Ch. IV) Linnik obtained an unexpected application of his investigations [6], when he proved (using an algebraic identity invented by himself) that every sufficiently large integer is the sum of seven non-negative cubes. Recently [243] he considered, by analogous arguments, the equation

$$n = \xi^2 + \eta^2 + x^3 + y^3 + z^3, \tag{21}$$

where $\xi, \eta, x, y, z$ are non-negative integers.

In paper [197] the following interesting result regarding the distribution of ideal classes in imaginary quadratic fields was obtained. Let $\varrho$ be a constant, $\frac{1}{4} < \varrho \leqslant \frac{1}{2}$, and let $m_1$ be a number under condition $m^\varrho \leqslant m_1 \leqslant m^{1/2}$. If $h(-m, m_1)$ denotes the number of reduced positive integral binary quadratic forms $ax^2+2bxy+cy^2$ with square-free determinant $m$, for which

$$a \leqslant m_1 \tag{22}$$

then for $m \to \infty$ we have

$$\log h(-m, m_1) \sim \log m_1$$

(in fact, a much more precise result was obtained).

In articles [8], [9], [14], [19] Linnik studied the estimates of Weyl trigonometric sums with Vinogradov's method, and, in particular, obtained a very useful $p$-adic variant of the method.

Finally, we must appreciate the elementary proof of Waring's theorem [21] (see also [IV], Ch. 2), included in Khintchine's well-known book ("Three pearls in number theory", Moscow, 1948). Generally, Linnik had more than usual interest in purely arithmetical proofs of arithmetical statements (see [49], [180] and monograph [IV]). Lately he suggested (within the framework of a dispersion method branch) an idea for proving the Goldbach–Vinogradov theorem on the sum of three primes, which was, in a definite sense, elementary (see [253]).

Yu.V.Linnik's works on probability theory are widely known. A brief survey of the most important of these works is to be found in Uspehi Mat. Nauk 28:2 (1973), pp. 204–209.



ACTA ARITHMETICA
XXVII (1975)

# Bibliography of scientific works of Yu. V. Linnik*

## A. Papers

1. *Обобщение теоремы Frobenius'а установление связи ее с теоремой Hurwitz'а о композиции квадратичных форм* (*Generalization of Frobenius theorem and its connection with Hurwitz's theorem on composition of quadratic forms*), Изв. АН СССР, сер. матем. 2 (1938), pp. 41–52 (English summary).

2. *Несколько новых теорем о представлении больших чисел отдельными положительными тернарными квадратичными формами*, Докл. АН СССР 24 (1939), pp. 211–212. English transl.: *Some new theorems on representation of large numbers by separate positive ternary quadratic forms*, C.R. Acad. Sci. L'URSS 24 (1939), pp. 211–212.

3. *О представлении больших чисел положительными тернарными квадратичными формами*, Докл. АН СССР 25 (1939), p. 578. English transl.: *On the representation of large numbers by positive ternary quadratic forms*, C.R. Acad. Sci. L'URSS 25 (1939), pp. 575–576.

4. *Одна общая теорема о представлении чисел отдельными тернарными квадратичными формами* (*A general theorem on representation of numbers by some ternary quadratic forms*), Изв. АН СССР, сер. матем. 3 (1939), pp. 87–108 (English summary).

5. *On certain results relating to positive ternary quadratic forms*, Матем. сб. 5 (47) (1939), pp. 453–471 (Russian summary).

6. *О представлении больших чисел положительными тернарными квадратичными формами* (*On the representation of large numbers by positive ternary quadratic forms*), Изв. АН СССР, сер. матем. 4 (1940), pp. 363–402 (German summary).

7. „*Большое решето*", Докл. АН СССР 30 (1941), pp. 290–292. English transl.: "*The large sieve*", C.R. Acad. Sci. L'URSS 30 (1941), pp. 292–294.

8. *Новые оценки сумм Weyl'я по методу И. М. Виноградова*, Докл.

* Compiled by T. G. Fursa and A. V. Malyshev.