ACTA ARITHMETICA
XXVII (1975)

Yu. V. Linnik's ergodic method in number theory

by

A. V. Malyshev (Leningrad)

1. Historical outline. In articles [1]–[5] Yu. V. Linnik elaborated the foundations of an original method in analytic number theory, which later became known as the "ergodic" method. His starting point was the following problem [1]: Given the integral positive ternary quadratic form

$$f = f(x_1, x_2, x_3) = \sum_{j,k=1}^{3} a_{jk} x_j x_k \tag{1.1}$$

of determinant $d = \det(a_{jk}) \neq 0$, find the conditions on which a given integer $m > 0$ is represented by the form f, i.e. the conditions on which the Diophantine equation

$$f(x_1, x_2, x_3) = m \tag{1.2}$$

is soluble in integers x_1, x_2, x_3. This problem becomes that of proper representations — of solving equation (1.2) with the condition

$$\text{g.c.d.}\,(x_1, x_2, x_3) = 1. \tag{1.3}$$

Clearly, to find a solution of (1.2) it is necessary that the congruences

$$f(x_1, x_2, x_3) \equiv m \pmod{g} \tag{1.4}$$

are soluble for any modulus $g > 0$ (this can be reduced to the case $g = 8md$). The conditions for the solvability of (1.4) can be expressed simply by the characters of the form f and are said to be generic (simultaneously holding or not holding for all forms of the genus).

An analogous problem of representation by a positive quadratic form $f = f(x_1, \ldots, x_s)$ in $s \geqslant 4$ variables is solved rather easily (see [52]; [35], Chapters I–III) by means of the circle method of analytic number theory.

[1] It is interesting to note that this problem arose in connection with that of Delaunay [42] on the determination of a three-dimensional crystallographic lattice by its distances.

It is proved then that if the necessary generic conditions are satisfied (the solvability of congruences analogous to (1.4)), any sufficiently large number m is represented by the form f; an asymptotic formula for the number of its representations is also obtained. In the case $s = 3$ application of this method has hitherto met with unsurmountable difficulties [2]. In order to solve the problem of the representation of numbers by positive ternary quadratic forms [3] Linnik developed a new analytic-algebraic method, using to full advantage the arithmetic of quaternions (and their generalizations — hermitions) and, in particular, the profound theory of B. A. Venkov [39] of the "rotations" of vectors (pure quaternions, quaternions without real parts).

In [5] it was proved that for the so-called "idoneous" integral positive ternary quadratic forms representable in the form of the sum of three squares of integral linear forms, any sufficienly large integer m prime to d is properly represented by the form f provided m satisfies the generic conditions for the form f; whereby, for the number of proper representations $r(f, m)$, the estimate

$$r(f, m) > c\,\frac{h(-m)}{\log\log m} \tag{1.5}$$

was obtained, where $h(-m)$ is the number of classes of integral properly primitive positive binary quadratic forms of determinant m, and where $c > 0$ is a constant dependent only on d. Here it is assumed that m satisfies conditions (1.4). In [5] an approach [4] was also outlined for the more general positive ternary quadratic forms f.

The problem of representation of numbers by ternary quadratic forms has been studied in [23], [24], [21]. The derivation of asymptotic formulae, in particular of that for $r(f, m)$ in the case of an "idoneous" form f, was made possible by a number of improvements [25] to Linnik's method, whereby it was found [9], [13] that the considerations can be simplified if some theorems from the theory of Markov chains [5] are applied.

[2] It is very likely that if application of the circle method in the case $s = 3$ is possible, it needs non-trivial estimates of the averages of Kloosterman sums.

[3] Classical arithmetic of quadratic forms can solve the problem (e.g. Jones [54]) only for one-class genera, e.g. (Gauss) for the genus of the forms $x_1^2+x_2^2+x_3^2$.

[4] It is unfortunate that this approach has not yet been realized. In monograph [35] another way of applying the ergodic method to more general quadratic forms was chosen.

[5] Namely their ergodic features, from which the term "ergodic method" was derived. It should be noted that Yu. V. Linnik's ergodic method has nothing in common with the classical ergodic method (if the similar looking formulations of their results are disregarded). For some remarks on this see § 8.4.

The problem of asymptotic formula for $r(f, m)$ in the case of an "idoneous" form f becomes the question of asymptotically uniform distribution of the proper representations (x_1, x_2, x_3) of the number m by the sum of three squares

$$x_1^2+x_2^2+x_3^2 = m \tag{1.6}$$

according to their residue-classes (b_1, b_2, b_3) with respect to the given modulus g,

$$(x_1, x_2, x_3) \equiv (b_1, b_2, b_3) \pmod{g}. \tag{1.7}$$

We will demonstrate (§ 4) the idea of Linnik's ergodic method on just this simplest model example.

The problem of representing the number m by the positive quadratic form $f = f(x_1, x_2, x_3)$ can be interpreted geometrically. By $\mathfrak{M}(f, m)$ we shall denote the set of all primitive integral points (x_1, x_2, x_3) lying on the surface of the ellipsoid (1.2), and $|\mathfrak{M}(f, m)| = r(f, m)$ will denote their number. Then, together with the question of representation of the number m by the form f (i.e. of the condition $r(f, m) > 0$) and of the asymptotic formula for $r(f, m)$, the problem of the structure of the set $\mathfrak{M}(f, m)$ naturally arises, i.e. the problem of the distribution of the points from $\mathfrak{M}(f, m)$ on the surface of the ellipsoid (1.2) according to their residue-classes with respect to a given modulus.

For the case of quadratic forms of $s \geqslant 4$ variables, problems of a similar kind are solved by means of the circle method (see [35], Chapter III). Study of the distribution of primitive integer points on the surface of the three-dimensional ellipsoid (1.2) was began in [22]. One of the important results in this direction was Linnik's theorem ([8], [16]; see also [35], Chapter VI; [19], Chapter IV) on the asymptotically uniform (for $m \to \infty$) distribution of the primitive integral points of the sphere (1.6) on its surface (of course under the assumption of the proper solvability of Diophantine equation (1.6), i.e. assuming that $m \equiv 1, 2 \pmod 4$ or $\equiv 3 \pmod 8$)). These considerations were generalized ([35], Chapter VI) for "idoneous" positive ternary quadratic forms.

The problem of representing the number m by the form f and of the structure of the set $\mathfrak{M}(f, m)$ in the case of an arbitrary integral positive ternary quadratic form f of the odd relatively prime invariants $[\Omega, \Delta]$ (for the definitions of Ω and Δ see § 2) was analysed in monograph [35], Chapter V. Unfortunately, in this general case one has not yet succeeded in obtaining the asymptotic formulae, only lower and upper estimates have been obtained for $r(f, m)$ giving its true order of magnitude (for $m \to \infty$). For an exact formulation of these results see § 3; the question of their generalizations and accuracy is discussed in § 6.

In Linnik's works ([7], [10], [11], [12], [14], [15]) and in those of B. F. Skubenko ([36], [37]) (see also [19], Chapters V and VI), the ergodic method was applied to the simplest indefinite ternary quadratic forms, i.e. to the problem of the distribution of integer points on the hyperbolic surface

$$x_1x_3 - x_2^2 = m, \quad m \neq 0. \tag{1.8}$$

In these applications not all of the integer points of the surface (1.8) were considered (due to their infinite number), but only those satisfying the supplementary "reduction" condition

$$2|x_2| \leqslant x_1 \leqslant x_3 \quad \text{if} \quad m > 0; \tag{1.9}$$

$$0 \leqslant x_2 \leqslant \sqrt{|m|}, \quad \sqrt{|m|} - x_2 \leqslant |x_1| \leqslant \sqrt{|m|} + x_2 \quad \text{if} \quad m < 0. \tag{1.10}$$

It was also proved that primitive integer points are asymptotically uniformly distributed on the surface of hyperboloid (1.8) with regard to hyperbolic metric (for $m \to +\infty$ and for $m \to -\infty$). Study of the case $m < 0$ was found to be particularly complicated. There, to apply Yu. V. Linnik's ergodic method, it was necessary to obtain a very non-trivial result regarding the lengths of the cycles of integral reduced indefinite binary quadratic forms [6]. For accurate formulations of these results see § 3; the question of their generalizations for arbitrary indefinite ternary quadratic forms is discussed in § 6.

The problem of the distribution of integer points in domain (1.8), (1.9) (for $m > 0$) can be interpreted as that of the distribution of the reduced positive integral binary quadratic forms

$$x_1u^2 + 2x_2uv + x_3v^2$$

of the determinant $x_1x_3 - x_2^2 = m$, or as the problem of the "distribution" of the classes of integer ideals of the imaginary quadratic field $Q(\sqrt{-m})$. The problem of distribution of integer points in the domain (1.8), (1.10) (for $m < 0$), can also be interpreted as that of the distribution of reduced indefinite integral binary quadratic forms of determinant m, which gives some information on the "distribution" of the classes of integer ideals of a real quadratic field. Unfortunately, the relationship between the forms studied in this paper and the classes of ideals is more complicated than in the case $m > 0$.

[6] Namely (B. F. Skubenko [37], p. 726): such an absolute constant c can be found that if l_1 and l_2 are the lengths of two such cycles (for definition see e.g. [40]), then $l_1/l_2 < c\log|m|$. This theorem is of great interest in itself (apart from its connection with the ergodic method), but unfortunately it is not well known.

The question of generalizing these considerations for the classes of integer ideals of an arbitrary algebraic number field naturally arises. In § 7 we shall study the wide programme outlined by Linnik ([15], [17]; [19], Chapter VII, Chapter IX, § 1). Regrettably, only preliminary results were obtained towards the realization of this programme. Recently Linnik [20] presented a simpler variant of this method. For its ideas see § 5 of this work.

Yu. V. Linnik ([43], [44]; [21], Chapter III; [45]) found several interesting applications of the theorems on the representations of numbers by positive ternary quadratic forms to the problem on the representations of numbers by the sums of cubes. For this see § 8.1.

2. Some facts from the arithmetic of ternary quadratic forms and hermitions [7]. Let

$$f = f(x_1, x_2, x_3) = \sum_{j,k=1}^{3} a_{jk}x_jx_k, \quad a_{jk} = a_{kj} \tag{2.1}$$

be a ternary quadratic form with integer [8] coefficients a_{jk} ($j, k = 1, 2, 3$) and with the determinant $d = d(f) = \det(a_{jk}) \neq 0$. The number $t(f) = \text{g.c.d.}\,(a_{jk})$ is said to be a *divisor* of the form f, which is said to be *primitive* if $t(f) = 1$. Let f be a primitive form, then $\bar{f} = df^{-1}$ is its adjoint form. The integers $\Omega = t(F)$ and $\Delta = d/\Omega^2$ are then said to be the *invariants* of the form f. The set of forms of the given invariants $[\Omega, \Delta]$ constitutes an order; for a given order $d = \Omega^2\Delta$.

We say that the forms f and f' are *equivalent* (in the ring of integers) if one can be transformed into the other by a unimodular integral substitution. The relation of equivalence divides the forms into classes. Each form of any one class has the same invariants (and determinant). The number of classes of forms for a given determinant is finite.

We say that the forms f and f' are *semi-equivalent* if one can be transformed into the other by a unimodular rational substitution, the denominator of which is prime to any previously fixed number. The semi-equivalence of forms is tantamount to their equivalence in the field of real numbers and in the rings of residue-classes for an arbitrary modulus (or to the integer p-adic equivalence for any prime p, including $p = \infty$). The equivalent forms are semi-equivalent but the converse does not generally hold. A *genus* is the set of all forms semi-equivalent to a given form. All forms of a given genus belong to the same order so that, in

[7] For details see e.g. Jones [54] and A. V. Malyshev [35], Chapter IV.

[8] One can also consider forms f with the integer coefficients $a_{11}, a_{22}, a_{33}, 2a_{12}, 2a_{13}, 2a_{23}$. We restrict ourselves to the integer a_{jk} to avoid difficulties of a technical nature.

particular, the number of classes in a genus is finite. A genus of forms can be defined by a finite number of its invariants, i.e. by a complete system of the form's characters (see Jones [54]).

Assume we are given an arbitrary odd [9] number $g > 0$, then the form f of the invariants $[\Omega, \Delta]$ is equivalent to the form

$$f' \equiv a_1 x_1^2 + \Omega a_2 x_2^2 + \Omega\Delta a_3 x_3^2 \pmod{g}, \tag{2.2}$$

where $a_1 a_2 a_3 \equiv 1 \pmod{dg}$.

We say that the number m is *represented* by the form f if the integers x_1, x_2, x_3, for which

$$f(x_1, x_2, x_3) = m, \tag{2.3}$$

can be found; the triple (x_1, x_2, x_3) is called the *representation* of the number m by the form f. If at the same time g.c.d. $(x_1, x_2, x_3) = 1$, then we say that m is *properly* represented by the form f (and the triple (x_1, x_2, x_3) is the *proper* representation of m by f). Let $r(f, m)$ be the number of proper and $R(f, m)$ the number of all representations of number m by form f. For positive forms f the numbers $r(f, m)$ and $R(f, m)$ are finite, and for indefinite forms, in general, are infinite. In the latter case one considers the number of representations satisfying some supplementary conditions, e.g. the number of "reduced" representations, see § 3. The quantities $r(f, m)$ and $R(f, m)$ are the class invariants.

Let $f = x_1^2 + x_2^2 + x_3^2$. Then for $r(m) = r(f, m)$ the Gauss formula [40]

$$r(m) = \begin{cases} 12h(-m) & \text{if} \quad m \equiv 1 \text{ or } 2 \pmod{4}, \\ 8h(-m) & \text{if} \quad m \equiv 3 \pmod{8} \end{cases} \tag{2.4}$$

holds, where $h(-m)$ is the number of classes of integral properly primitive positive binary quadratic forms of the determinant m (if $m \not\equiv 1, 2 \pmod{4}$, $3 \pmod{8}$, then $r(m) = 0$). By the Siegel theorem [60],

$$m^{1/2-\varepsilon} \ll h(-m) \ll m^{1/2+\varepsilon}, \tag{2.5}$$

where $\varepsilon > 0$ is an arbitrarily small quantity; the constants implicit in the symbol $\ll$ depend only on ε.

Let f be the primitive form (2.1) of the invariants $[\Omega, \Delta]$, let $d = \Omega^2\Delta \neq 0$, and $F = (1/\Omega)\bar{f}$, where $\bar{f} = df^{-1}$ is the algebraic adjoint of f (we say that F is the primitive adjoint of f); then

$$F = \sum_{k,l=1}^{3} A_{kl} x_k x_l$$

[9] An analogous (but not so simply formulated) result can be obtained for an even g.

is the primitive form of invariants $[\Delta, \Omega]$. By $\mathfrak{A}_f$ we denote the 4-dimensional algebra over the field of rational numbers with the basis $[1, i_1, i_2, i_3]$, where 1 is the unit element of $\mathfrak{A}_f$,

$$\left.\begin{aligned} i_k^2 &= -\Delta a_{kk}, \\ i_k i_{k+1} &= -\Delta a_{kk} + \sum_{l=1}^{3} A_{k+2,l} i_l, \\ i_{k+1} i_k &= -\Delta a_{kk} - \sum_{l=1}^{3} A_{k+2,l} i_l, \end{aligned}\right\} \quad k = 1, 2, 3 \pmod{3}. \tag{2.6}$$

The elements of algebra $\mathfrak{A}_f$,

$$A = a_0 + a_1 i_1 + a_2 i_2 + a_3 i_3,$$

where a_k $(k = 0, 1, 2, 3)$ are rational numbers, we shall call *hermitions* (or *generalized quaternions*) corresponding to the ternary quadratic form f. If $f = x_1^2 + x_2^2 + x_3^2$ then $\mathfrak{A}_f = \mathfrak{A}_0$ is the algebra of ordinary quaternions.

The hermition

$$\bar{A} = a_0 - a_1 i_1 - a_2 i_2 - a_3 i_3$$

is said to be *conjugate* to the hermition A. The product

$$N(A) = A\bar{A} = \bar{A}A = a_0^2 + \Delta f(a_1, a_2, a_3) \tag{2.7}$$

is called the *norm* of hermition A; $N(AB) = N(A)N(B)$. If $a_0 = 0$ then the hermition A is said to be a *vector* (or *pure hermition*). If A is a vector (and only in this case) then

$$A^2 = -N(A). \tag{2.8}$$

We shall call the hermition $A = a_0 + a_1 i_1 + a_2 i_2 + a_3 i_3$ an *integer hermition* [10] if a_0, a_1, a_2, a_3 are integers, and we shall call the integer hermition A *primitive* if g.c.d. $(a_0, a_1, a_2, a_3) = 1$. A will be called *primitive* $(\bmod\ q)$ if g.c.d. $(a_0, a_1, a_2, a_3, q) = 1$. We say that hermition B is the *right divisor* of hermition A, A/B, if AB^{-1} is an integer hermition. The same applies to the *left* divisor C, $C \diagdown A$, if $C^{-1}A$ is an integer hermition. An integer hermition E with an integer reciprocal is said to be a *unit*; E is a unit if and only if $N(E) = 1$. Hermitions A and $B = AE$, where E is a unit, are said to be *right associated*; A and $C = EA$ — *left associated*.

The following theorem on uniqueness holds true (see e.g. [35], Chapter IV).

[10] The notion of the integer hermition can be defined in a different way by extension of the ring of hermitions with integer coefficients to a maximum order. Both definitions have their own advantages, for our purposes the given definition suffices.

Proposition 1. *Let* g.c.d. $(b, 2d) = 1$, A *be a primitive* (mod b) *hermition; B_1 and B_2 be integer hermitions of the norm b. Then, if A/B_1 and A/B_2, we have*

$$B_2 = EB_1,$$

where E is a unit of the algebra $\mathfrak{A}_f$.

The theorem of decomposition ([35], Chapter IV, § 6) also holds for the algebra $\mathfrak{A}_0$ of ordinary quaternions (and generally for hermition algebras which are principal ideal domains).

Proposition 2. *If A is an integer hermition of $\mathfrak{A}_0$ and if b is a positive integer divisor of $N(A)$ prime to $2d$ (i.e. in the case of $\mathfrak{A}_0$ if b is an odd number), then a right divisor B of A, the primitive hermition of the norm b, can be found.*

We will note one from among a number of propositions on the decomposition of hermitions (see [35], Chapter IV, §§ 2–4).

Proposition 3. *Let R_1 and R_2 be integer hermitions of norm r prime to $2d$, and let the hermition R_1R_2 be primitive. Then, if the integer vector L is right divisible by R_1 and is left divisible by R_2, L is divisible by the number r.*

Let $L = x_1i_1+x_2i_2+x_3i_3$ be a primitive integer vector of the norm Δm. Then

$$L^2 = -\Delta m, \tag{2.9}$$

which is equivalent to the equality

$$f(x_1, x_2, x_3) = m. \tag{2.10}$$

Hence to investigate the set $\mathfrak{M}(f, m)$ (see § 1) means to study the set of primitive integer vectors of the norm Δm, i.e. the set of integer hermitions with the condition (2.9). This idea (in the case $f = x_1^2+x_2^2+x_3^2$) is due to B. A. Venkov [39] who developed the theory of "rotations of vectors". Venkov's theory was generalized to hermitions by Linnik in [3]–[5]. An outline of this theory will now be given (for details see [35], Chapter IV, § 5).

Let L and L' be two primitive vectors of the norm Δm. L and L' are said to be equivalent (in a rotational sense) if for an arbitrary integer g, such an integer hermition Q of the norm prime to g can be found that

$$Q^{-1}LQ = L'. \tag{2.11}$$

Proposition 4. *If*

$$L \equiv L' \ (\mathrm{mod}\ 2d), \tag{2.12}$$

then L and L' are equivalent.

Proposition 5. *Let L and L' be equivalent and let Q be an integer hermition of the norm prime to $2d$, at the same time let equality* (2.11) *hold. Then an integer hermition R and an integer l can be found, satisfying the condition*

$$l+L' = QR. \tag{2.13}$$

Let $N(Q) = q$, $N(R) = r$. Then (2.13) implies

$$qr-l^2 = \Delta m \tag{2.14}$$

and to the pair ("rotation") (L, L') there corresponds the integral positive binary quadratic form

$$(q, l, r) = qu^2+2luv+rv^2, \quad \text{g.c.d.}\ (q, 2l, r) = 1 \tag{2.15}$$

of determinant Δm. We say that the rotation (L, L') is governed by the binary form (q, l, r). The choice of Q, R and l is not unique.

Proposition 6. *By equalities of the type* (2.11) *and* (2.13), *a one-to-one correspondence is established between the set of the pairs $(L, E^{-1}L'E)$, where E runs through all units of the algebra $\mathfrak{A}_f$, and the class of integral properly primitive binary quadratic forms of determinant Δm.* (For a more detailed formulation see [35], Chapter IV, § 5.)

Condition (2.12) shows that the number of classes of vectors is bounded by a number depending only on d. Unfortunately, this is not a necessary condition. In a more detailed study of this problem for algebra $\mathfrak{A}_0$ Venkov derived a new proof of the Gauss formula (2.4): he was fixing vector L and to the primitive points (x_1, x_2, x_3) of the sphere

$$x_1^2+x_2^2+x_3^2 = m \tag{2.16}$$

made correspond rotations (L, L') where $L' = x_1i_1+x_2i_2+x_3i_3$. In order to study the set $\mathfrak{M}(f, m)$ Linnik proceeded a little differently. He fixed norm $q = N(Q)$ of hermition Q, and for increasing m with the condition

$$\left(\frac{-\Delta m}{p}\right) = 1 \quad \text{for all primes } p\,|\,q, \tag{2.17}$$

he considered chains of primitive integer vectors of norm Δm of the form

$$L, \quad L' = Q^{-1}LQ, \quad L'' = Q'^{-1}L'Q', \quad \ldots, \tag{2.18}$$

where $Q, Q', \ldots$ are integer hermitions of norm q, and found their ergodic properties (for some details on this see § 4).

Unfortunately, even under the necessary condition (2.17), integer hermitions $Q, Q', \ldots$ of norm q, generating chain (2.18) of primitive integer vectors $L, L', L'', \ldots$ of norm Δm, cannot always be found. This is possible in the case of the algebra of ordinary quaternions (in general, in the case of a hermition algebra being a principal ideal domain), since by (2.17) such integer l can be found that

$$l^2+\Delta m \equiv 0 \pmod{q}.$$

But then $l+L$ is a primitive hermition and $q \mid N(l+L)$. Hence (Proposition 2) integer hermitions Q and R satisfying the condition

$$l+L = QR, \qquad N(Q) = q$$

can be found, so that $L' = Q^{-1}LQ$ is an integer primitive vector of norm Δm.

We shall make a further two remarks regarding algebra $\mathfrak{A}_0$ of ordinary quaternions. The integer hermition $A = a_0+a_1i_1+a_2i_2+a_3i_3$ of an odd norm is called *primary* if

$$a_0+1 \equiv a_1 \equiv a_2 \equiv a_3 \pmod{2}, \qquad a_0+a_1+a_2+a_3 \equiv 1 \pmod{4}. \tag{2.19}$$

It can be verified that the product of two primary quaternions is also a primary quaternion. The following statement therefore holds ([35], Chapter IV, § 6).

PROPOSITION 7. *Among the right* [11] *associated quaternions of an odd norm, there is one and only one primary quaternion.*

PROPOSITION 8. *Let $r > 0$ be an odd number, and let $\sigma_0(r)$ be the number of primitive primary quaternions of norm r. Then*

$$\sigma_0(r) = r\sum_{p\mid r}\left(1+\frac{1}{p}\right). \tag{2.20}$$

For arbitrary hermition algebras $\mathfrak{A}_f$ only asymptotic (for $r\to\infty$) analogues of (2.20) are known. For a much more detailed account of the arithmetic of hermitions readers are referred to [35], Chapter IV.

3. Detailed formulations of fundamental results obtained with the help of Linnik's ergodic method. All results obtained hitherto by application of Linnik's number-theoretic ergodic method relate to analytic arithmetic of integral ternary quadratic forms, and are formulated in Theorems 1–4 below. For their application to the representation of numbers by the sums of cubes see § 8. Some results related to application of the ergodic method to algebraic number fields are considered in § 7.

Let $f(x_1, x_2, x_3)$ be a primitive integral quadratic form of determinant $d \neq 0$, let $m \neq 0$ be an integer and $\Lambda_{f,m}$ be a domain on the surface

$$f(x_1, x_2, x_3) = m, \tag{3.1}$$

[11] or left.

and let $g > 0$, b_1, b_2, b_3 be integers, g.c.d. $(g, b_1, b_2, b_3) = 1$. By $r_{g;b_1,b_2,b_3}(\Lambda_{f,m})$ we shall denote the number of primitive integer points (x_1, x_2, x_3) satisfying the conditions

$$(x_1, x_2, x_3) \in \Lambda_{f,m} \tag{3.2}$$

and

$$(x_1, x_2, x_3) \equiv (b_1, b_2, b_3) \pmod{g}. \tag{3.3}$$

In particular if $g = 1$, then $r_{g;b_1,b_2,b_3}(\Lambda_{f,m}) = r(\Lambda_{f,m})$ is the number of primitive integer points of the domain $\Lambda_{f,m}$. If $\Lambda_{f,m}$ coincides with the whole surface (3.1), then $r_{g;b_1,b_2,b_3}(\Lambda_{f,m}) = r_{g;b_1,b_2,b_3}(f, m)$ is the number of proper representations of number m by the form f with the supplementary condition (3.3). If in addition $g = 1$, then $r_{g;b_1,b_2,b_3}(f, m) = r(f, m)$ is the number of all primitive representations of number m by the form f.

The aim of this consideration is to study the function $r_{g;b_1,b_2,b_3}(\Lambda_{f,m})$ as $|m|$ increases. For this it is assumed that the following necessary conditions are satisfied:

(i) The congruence

$$f(b_1, b_2, b_3) \equiv m \pmod{g} \tag{3.4}$$

holds.

(ii) The congruence

$$f(x_1, x_2, x_3) \equiv m \pmod{t} \tag{3.5}$$

is primitively soluble for an arbitrary modulus $t > 0$.

For $r_{g;b_1,b_2,b_3}(\Lambda_{f,m})$ asymptotic formulae (Theorems 2–4) or estimates (Theorem 1) are obtained, under some assumptions.

THEOREM 1. *Let f be an integral positive ternary quadratic form of odd coprime invariants $[\Omega, \Delta]$ and let q be a prime number, $q \nmid 2\Delta$. Let a positive integer m satisfy the condition*

$$\left(\frac{-\Delta m}{q}\right) = 1, \tag{3.6}$$

let g.c.d. $(g, 2\Omega\Delta) = 1$, *and let $\Lambda_{f,m}$ be a convex domain seen from the centre of the ellipsoid* (3.1) *in f-elliptic solid angle* [12] $\lambda > 0$. *Then such constants m_0, $c > 0$ and $c' > 0$, dependent only on f, g, λ and q, can be found, that for $m \geqslant m_0$ and satisfying the necessary conditions* (3.4) *and* (3.5) [13],

$$ch(-\Delta m) < r_{g;b_1,b_2,b_3}(\Lambda_{f,m}) < c'h(-\Delta m), \tag{3.7}$$

[12] λ is the *volume* of intersection of the ellipsoid $f(x_1, x_2, x_3) \leqslant 1$ with a cone, corresponding to $\Lambda_{f,m}$, the apex of which is in the centre of the ellipsoid.

[13] In our assertions (3.5) is equivalent to the primitive solvability of the congruence

$$f(x_1, x_2, x_3) \equiv m \pmod{8\Omega^2\Delta m}.$$

where $h(-\Delta m)$ is the number of classes of integral properly primitive positive binary quadratic forms of determinant Δm.

Corollary. *Let f be a positive form of odd coprime invariants $[\Omega, \Delta]$, and let q be a prime number, $q \nmid 2\Delta$. Then such constants m_0, $c > 0$, and $c' > 0$, dependent only on $\Omega\Delta$ and q, can be found, that for $m \geqslant m_0$ and satisfying* (3.5) *and* (3.6),

$$ch(-\Delta m) < r(f, m) < c' h(-\Delta m). \tag{3.8}$$

For a proof of Theorem 1 see [35], Chapter V, § 4 (preliminary reports being [29] and [33]). We will now make a number of remarks.

From proper representations we can pass on to all representations, and for number $R_{g;b_1,b_2,b_3}(\Lambda_{f,m})$ of all integer representations (x_1, x_2, x_3) of number m by the form f, satisfying (3.2) and (3.3), obtain (under the assumptions of Theorem 1) the inequality

$$cH(-\Delta m) < R_{g;b_1,b_2,b_3}(\Lambda_{f,m}) < c' H(-\Delta m), \tag{3.9}$$

where $H(-\Delta m)$ is the number of all classes of integral positive binary quadratic forms of determinant Δm.

Instead of assuming the convexity of $\Lambda_{f,m}$ and that $\lambda > 0$ is fixed (with the possible dependence of $\Lambda_{f,m}$ on m) one can consider arbitrary domains $\Lambda_{f,m}$ of a fixed form [14].

Besides the necessary conditions (3.4) and (3.5), we demand that m satisfies (3.6) for some fixed prime q. Generally speaking (3.6) is not a necessary condition and is related to the specific character of the ergodic method (see § 4). It should be noted however, that for all genera of the form f of the order $[\Omega, \Delta]$, with the exception of one, (3.6) is a consequence of the necessary condition (3.5) if for q we choose the prime divisor of number Ω, for which

$$\chi_q(f) = \left(\frac{f}{q}\right) = \left(\frac{-\Delta}{q}\right). \tag{3.10}$$

For the exceptional genus (and thus for $f = x_1^2 + x_2^2 + x_3^2$) condition (3.6) involves an additional limitation on $m \,(\mathrm{mod}\, q)$. Condition (3.6) can, however, be omitted if we assume the validity of the following, as yet unproved, assertion on zeros of Dirichlet L-series with real characters:

Hypothesis ($\mathfrak{H}$). *In the domain*

$$|s-1| < \frac{(\log\log m)^2 \log\log\log m}{\sqrt{\log m}} \tag{3.11}$$

[14] We say that domains Λ_{f,m_1} and Λ'_{f,m_2} have the same forms if the cones corresponding to them can be transformed into each other by f-elliptic rotation.

of the complex variable s, there are no zeros of Dirichlet L-functions

$$L(s) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s} \quad (\mathrm{Re}\, s > 1), \qquad \chi(n) = \left(\frac{-4\Omega^2 \Delta g^2 m}{n}\right). \tag{3.12}$$

See [35], Chapter V, § 5 and also [30] and [34].

Finally, we shall note that since we are using the ineffective Siegel inequality (2.5), constants implicit in (3.7), (3.8) and (3.9) cannot be effectively computed.

Theorem 2. *Let*

$$f(x_1, x_2, x_3) = \sum_{k=1}^{3} (c_{k1}x_1 + c_{k2}x_2 + c_{k3}x_3)^2, \tag{3.13}$$

where c_{kl} $(k, l = 1, 2, 3)$ are integers and $\det(c_{kl}) = d_1$ is an odd number such that $d = d(f) = d_1^2$. Let $g > 0$ be an odd number, b_1, b_2, b_3 be integers, g.c.d. $(b_1, b_2, b_3, 2) = 1$, *and $q > 2$ be a prime number. Let $m > 0$ be prime to dgq,*

$$f(b_1, b_2, b_3) \equiv m \,(\mathrm{mod}\, 8d_1 g), \tag{3.14}$$

and

$$\left(\frac{-m}{q}\right) = 1. \tag{3.15}$$

Also let $\Lambda_{f,m}$ be a convex domain with f-elliptic solid angle $\lambda > 0$. Then for $m \to \infty$ and for fixed f, g, λ and q,

$$r_{g;b_1,b_2,b_3}(\Lambda_{f,m}) \sim \frac{\lambda}{4\pi} \cdot \frac{s\big(f, m; g, (c_{kl})\big)}{dg^2 \prod\limits_{p|dq} \left(1 + \dfrac{\left(\frac{-m}{p}\right)}{p}\right)} \cdot r(m), \tag{3.16}$$

where $\mathring{r}(m)$ is the number of primitive representations of number m by the sum of three squares [15], *and $s\big(f, m; g, (c_{kl})\big)$ is the number of distinct* $(\mathrm{mod}\, d_1)$ *solutions (x_1, x_2, x_3) of*

$$f(gx_1 + b_1, gx_2 + b_2, gx_3 + b_3) \equiv m \,(\mathrm{mod}\, d_1 g),$$

for which the systems of numbers

$$\Big\{\sum_{j=1}^{3} c_{1j}(gx_j + b_j), \sum_{j=1}^{3} c_{2j}(gx_j + b_j), \sum_{j=1}^{3} c_{3j}(gx_j + b_j)\Big\}$$

are distinct $(\mathrm{mod}\, d_1 g)$.

[15] See Gauss formula (2.4).

For proof see [35], Chapter VI, and for particular cases and preliminary reports see [25], [8], [16] and [28].

The remarks made in connection with Theorem 1 apply also to this theorem.

From asymptotic formula (3.16) one can easily pass on to the asymptotic formula for $R_{g;b_1,b_2,b_3}(\Lambda_{f,m})$. Instead of assuming the convexity of domain $\Lambda_{f,m}$ one can assume that the form of $\Lambda_{f,m}$ is fixed. (3.14) implies (3.15) for all genera of the form f except one, for which (3.15) follows from Hypothesis $(\mathfrak{H})$. The constants in (3.16) are ineffective. We will formulate important particular cases of Theorem 2.

COROLLARY 1. *Let $\Omega > 1$ be an odd number and f be a primitive integral positive ternary quadratic form of invariants $[\Omega, 1]$ belonging to the genus $\mathfrak{J}_{[\Omega,1]}$*[16] *with characters $\left(\frac{-f}{p}\right) = 1$ for all primes $p \mid \Omega$. Let $m > 0$ be an integer prime to Ω, for which the congruence*

$$f(x_1, x_2, x_3) \equiv m \pmod{\Omega} \tag{3.17}$$

is soluble. Then for $m \to \infty$ and for fixed Ω,

$$r(f, m) \sim \begin{cases} 12\left\{\prod\limits_{p\mid\Omega}\left(\dfrac{2}{1+\dfrac{1}{p}}\right)\right\} h(-m) & \text{if} \quad m \equiv 1, 2 \pmod 4, \\ 8\left\{\prod\limits_{p\mid\Omega}\left(\dfrac{2}{1+\dfrac{1}{p}}\right)\right\} h(-m) & \text{if} \quad m \equiv 3 \pmod 8). \end{cases} \tag{3.18}$$

See [25], and [35], Chapter VI.

COROLLARY 2. *Let $q > 2$ be a prime number, and $m > 0$ be an integer prime to q satisfying the conditions*

$$m \equiv 1 \text{ or } 2 \pmod 4, \text{ or } \equiv 3 \pmod 8 \tag{3.19}$$

and

$$\left(\frac{-m}{q}\right) = 1. \tag{3.20}$$

Let Λ_m be a convex domain on the surface

$$x_1^2 + x_2^2 + x_3^2 = m, \tag{3.21}$$

so that the solid angle of Λ_m is equal to $\lambda > 0$. Then for $m \to \infty$ and for fixed λ and q,

$$r(\Lambda_m) \sim \frac{\lambda}{4\pi} r(m). \tag{3.22}$$

See [8], [16], [35], Chapter VI, and [19], Chapter IV.

COROLLARY 3. *Let $g > 0$ be an odd number, $m > 0$ be a number prime to g, $m \equiv 1, 2 \pmod 4$, $\equiv 3 \pmod 8$, and*

$$\left(\frac{-m}{q}\right) = 1 \tag{3.23}$$

for all primes $q \mid g$, and let b_1, b_2, b_3 be three integers such that

$$b_1^2 + b_2^2 + b_3^2 \equiv m \pmod{g}. \tag{3.24}$$

By $r_{g;b_1,b_2,b_3}(m)$ we denote the number of primitive integer points (x_1, x_2, x_3) on the sphere

$$x_1^2 + x_2^2 + x_3^2 = m, \tag{3.25}$$

satisfying the supplementary condition

$$(x_1, x_2, x_3) \equiv (b_1, b_2, b_3) \pmod{g}. \tag{3.26}$$

Then for $m \to \infty$ and for fixed g,

$$r_{g;b_1,b_2,b_3}(m) \sim \frac{1}{\varrho(m, g)} r(m), \tag{3.27}$$

where

$$\varrho(m, g) = g^2 \prod_{p\mid g}\left(1 + \frac{1}{p}\right) = \sigma_0(g^3) \tag{3.28}$$

is the number of solutions of

$$x_1^2 + x_2^2 + x_3^2 \equiv m \pmod{g}. \tag{3.29}$$

See [25], and [35], Chapter VI.

(3.27) is also valid when condition (3.23) is relaxed, namely replaced by the existence of an odd prime q satisfying (3.23).

We now turn to indefinite ternary quadratic forms. So far only the case of the simplest form

$$f = x_1x_3 - x_2^2 \tag{3.30}$$

(or form $f' = x_1^2 + x_2^2 - x_3^2$) for $g = 1$ has been considered here. Since the number of primitive integer points (x_1, x_2, x_3) of the surface

$$x_1x_3 - x_2^2 = m \tag{3.31}$$

[16] Linnik [5] called forms of the genus $\mathfrak{J}_{[\Omega,1]}$ "idoneous" (for the application of his method).

is infinite, it is assumed that $\Lambda_{f,m} \subset P_{f,m}$, where $P_{f,m}$ is the reduced domain. The number of reduced primitive integer points of (3.31) is, however, finite. The case $m > 0$ (the hyperboloid of two sheets, Theorem 3) and $m < 0$ (the hyperboloid of one sheed, Theorem 4) are considered separately.

THEOREM 3. *Let $q > 2$ be a prime, $m > 0$ be an integer prime to $2q$ and*

$$\left(\frac{-m}{q}\right) = 1, \tag{3.32}$$

let $f = x_1x_3 - x_2^2$, and $P_{f,m}$ be the reduction domain

$$2|x_2| \leqslant x_1 \leqslant x_3 \tag{3.33}$$

lying on the hyperboloid (3.31). *Let $C > 1$ be an arbitrary constant and $P'_{f,m}(C)$ be a sub-domain of $P_{f,m}$, lying in the half-space*

$$x_3 \leqslant Cx_1 \tag{3.34}$$

such that $P'_{f,m}$ is the hyperbolic quadrangle

$$x_1x_3 - x_2^2 = m, \quad 2|x_2| \leqslant x_1 \leqslant x_3 \leqslant Cx_1. \tag{3.35}$$

Let $\Lambda_{f,m}$ be a convex domain, $\Lambda_{f,m} \subset P'_{f,m}(C)$, having the hyperbolic solid angle [17] *$\lambda > 0$. Then, for $m \to +\infty$ and for fixed λ, C and q,*

$$r(\Lambda_{f,m}) \sim \frac{\lambda}{\lambda_0} h(-m), \tag{3.36}$$

where $\lambda_0 = \frac{2}{9}\pi$ is a hyperbolic solid angle of the domain $P_{f,m}$.

See [7], [10], and [19], Chapter V.

THEOREM 4. *Let $q > 2$ be a prime, $m < 0$ be an integer prime to $2q$, where $|m|$ is not a perfect square and*

$$\left(\frac{-m}{q}\right) = 1, \tag{3.37}$$

let $f = x_1x_3 - x_2^2$, and $P_{f,m}$ be the reduction domain

$$x_1x_3 - x_2^2 = m, \quad 0 \leqslant x_2 \leqslant \sqrt{|m|}, \quad \sqrt{|m|} - x_2 \leqslant |x_1| \leqslant \sqrt{|m|} + x_2. \tag{3.38}$$

Let $\Lambda_{f,m} \subset P_{f,m}$ be a convex domain with the hyperbolic solid angle $\lambda > 0$. Then, for $m \to -\infty$ and for fixed λ and q,

$$r(\Lambda_{f,m}) \sim \frac{\lambda}{\lambda_0} r(P_{f,m}), \tag{3.39}$$

where $r(P_{f,m})$ is the number of primitive integer points of the domain $P_{f,m}$, and λ_0 is the hyperbolic solid angle of the domain $P_{f,m}$.

See [36], [37], and [19], Chapter VI.

As in the above, (3.32) and (3.37) can be replaced by Hypothesis ($\mathfrak{H}$). The asymptotic value of the quantity $r_{q;b_1,b_2,b_3}(\Lambda_{f,m})$ can be obtained in the case of $f = x_1x_3 - x_2^2$ and $m \neq 0$. Detailed studies of these problems have not however been made. We shall note that from the formulae of Theorems 3 and 4 one can pass on to the corresponding formulae for all integral representations. Finally, we shall note that constants implicit in (3.36) and (3.39) are not effective.

4. The essence of Linnik's ergodic method (on the example of the proof of uniform distribution of the integer points of a sphere, for a given modulus).

We shall demonstrate the idea of Linnik's method on the simplest, one can say model example, i.e. on the proof of Corollary 3 of Theorem 2 (§ 3). This corollary will be derived from the following [25]:

THEOREM 5. *Let $m > 0$, $q > 0$, and u be integers, $m \equiv 1, 2 \pmod 4$, $\equiv 3 \pmod 8$, q be an odd number prime to m, and let*

$$u^2 + m \equiv 0 \pmod q. \tag{4.1}$$

Let Q be a primitive integer quaternion of norm q. By $r(m, Q)$ we denote the number of primitive integer vectors L of norm m, for which the quaternion $u + L$ is left divisible by Q. Then, for $m \to \infty$ and for fixed q,

$$r(m, Q) \sim \frac{1}{\sigma_0(q)} r(m), \tag{4.2}$$

where $r(m)$ is the number of all primitive vectors L of norm m, and where

$$\sigma_0(q) = q \prod_{p|q} \left(1 + \frac{1}{p}\right) \tag{4.3}$$

is the number of primitive primary quaternions of norm q.

Proof. Without loss of generality we assume quaternions Q to be primary. We choose such number l that

$$l^2 + m \equiv 0 \pmod{q^s}, \quad l \equiv u \pmod q, \tag{4.4}$$

where

$$s = [\varrho \log_q m] \tag{4.5}$$

and a constant $\varrho > 0$ will be fixed in the sequel. We shall consider all primitive integer vectors $L_1, L_2, \ldots, L_{r(m)}$ of norm m. By (4.4) and Proposition 2 of Section 2 we can write

$$l + L_j = B_j U_j, \quad N(B_j) = q^s \quad (j = 1, \ldots, r = r(m)), \tag{4.6}$$

[17] Determined by the volume of the sub-cone $x_1x_3 - x_2^2 \leqslant 1$ corresponding to $\Lambda_{f,m}$ with its apex in the origin.

where

(4.7) $$B_j = Q_{j1}\cdot Q_{j2}\cdot \ldots \cdot Q_{js},$$

in which all Q_{jk} are primary quaternions of norm q.

In each kth column of the matrix

(4.8) $$\begin{bmatrix} Q_{11} & \ldots & Q_{1s} \\ \cdot & \cdot\ \cdot\ \cdot & \cdot \\ Q_{r1} & \ldots & Q_{rs} \end{bmatrix}$$

there are exactly $r(m, Q)$ quaternions $Q_{jk} = Q$. For $k = 1$ this is implied by its definition and (4.4), (4.6) and (4.7). The case $k > 1$ can be reduced to the afore-mentioned since there is a one-to-one correspondence between equalities (4.6) and the equalities

(4.9) $$l+L_j^{(k)} = Q_{jk}V_j^{(k)} \quad (j = 1, \ldots, r)$$

where for given k,

(4.10) $$L_j^{(k)} = (Q_{j1}\cdot \ldots \cdot Q_{j,k-1})^{-1}L_j(Q_{j1}\cdot \ldots \cdot Q_{j,k-1})$$

run through distinct primitive vectors of norm m, and where

(4.11) $$V_j^{(k)} = (Q_{j,k+1}\cdot \ldots \cdot Q_{js})\,U_j(Q_{j1}\cdot \ldots \cdot Q_{j,k-1}).$$

We shall prove the asymptotic formula (4.2) *a contrario* allowing that for some $\gamma > 0$ we can find either an infinitely increasing sequence m satisfying the assumptions of the theorem, for which

(4.12) $$r(m, Q) < (1-\gamma)\frac{r(m)}{\sigma_0(q)},$$

or such sequence m, for which

(4.13) $$r(m, Q) > (1+\gamma)\frac{r(m)}{\sigma_0(q)}.$$

Without any loss of generality, since

(4.14) $$\sum_{j=1}^{\sigma_0(q)} r(m, Q_j) = r(m)$$

we can assume that m satisfies (4.12), where $\gamma > 0$ is independent of m (but possibly dependent on q).

We shall prove that from the $r = r(m)$ equalities (4.6) one can choose

(4.15) $$r' > \frac{\gamma/2}{1-\gamma/2}\,r(m)$$

equalities

(4.16) $$l+L_j = B_jU_j, \quad N(B_j) = q^s \quad (j = 1, \ldots, r')$$

(for simplification we are changing their indices) with the condition: for a given j ($j = 1, \ldots, r'$) the number $Q_{jk} = Q$ ($k = 1, \ldots, s$) is

(4.17) $$< \left(1-\frac{\gamma}{2}\right)\frac{s}{\sigma_0(q)}.$$

Indeed, if for $\big(r(m)-r'\big)$ rows of matrix (4.8) the number $Q_{jk} = Q$ ($k = 1, \ldots, s$) for a given j is

$$\geqslant \left(1-\frac{\gamma}{2}\right)\frac{s}{\sigma_0(q)},$$

then estimating the number of times that Q appears in the columns and in the rows of matrix (4.8), we arrive at the inequality

$$\left\{\left(1-\frac{\gamma}{2}\right)\frac{s}{\sigma_0(q)}\right\}\big(r(m)-r'\big) < \left\{(1-\gamma)\frac{r(m)}{\sigma_0(q)}\right\}s$$

equivalent to (4.15).

By (4.5) the overall number of distinct primitive primary quaternions B of norm q^s is equal to

(4.18) $$q^s\prod_{p|q}\left(1+\frac{1}{p}\right) \asymp m^{\varrho}.$$

We shall find the lower and upper estimates for the number w' of distinct quaternions B_j of norm q^s, appearing in (4.16).

Firstly, it is clear that

(4.19) $$w' \leqslant w;$$

here w is the number of primitive quaternions of the form

(4.20) $$B^{(j)} = Q_1^{(j)}\cdot \ldots \cdot Q_s^{(j)},$$

where $Q_k^{(j)}$ are primary quaternions of norm q, and for a given j the number of equalities

(4.21) $$Q_k^{(j)} = Q \quad (k = 1, \ldots, s)$$

satisfies (4.17). w is found to be considerably smaller than (4.18), namely

(4.22) $$w \ll m^{\varrho-\delta},$$

where $\delta = \delta(q, \gamma) > 0$. The idea of the proof of estimate (4.22) can be demonstrated on the following simplified model.

Imagine a set of all s-digit g-adic integers, their number is equal to g^s and the number of these numbers which do not contain a given digit (e.g. 0), is

$$(g-1)^s = (g^s)^{1-|\log_g(1-1/g)|}.$$

We shall also obtain a similar estimate for the number of s-digit g-adic integers, in which the digit 0 occurs "unusually" seldom, less than $(1-\gamma)s/g$ times (instead of the "usual" frequency of s/g times). In estimating w a technical difficulty arises since for the primitivity of $B^{(j)}$, the conditions

$$Q_{k+1}^{(j)} \neq \overline{Q_k^{(j)}}E \tag{4.23}$$

must be fulfilled. This difficulty can be overcome by modelling [9], [13] the primitive quaternions $B^{(j)}$ by the Markov chains

$$\{Q_1^{(j)}, Q_2^{(j)}, \ldots, Q_s^{(j)}\}$$

with the forbidden transitions (4.23), and with the remaining equally probable transitions. A second method for overcoming this difficulty is to consider not all columns of the matrix (4.8) but only those fixed at such a distance from each other that the "interaction" of $Q_k^{(j)}$ with $Q_{k'}^{(j)}$ is asymptotically negligible. For details the reader is referred to [35], Chapter VI, § 1, where a more general question is considered which makes the idea described less clearly visible. See also [19], Chapter IV, §§ 4–5.

On the other hand, if

$$0 < \varrho \leqslant 1/2, \tag{4.24}$$

then

$$w' \gg m^{\varrho-\varepsilon}, \tag{4.25}$$

where constants implicit in (4.25) depend only on q, γ and on any arbitrarily small $\varepsilon > 0$. The proof of this assertion is a focal point of Linnik's ergodic method, although in his basic work the weaker estimate

$$w' \gg m^{1/2}, \quad \varrho = \frac{1}{2}+\tau, \quad \tau = \frac{-\log\left(1-\dfrac{1}{q}\right)}{2\log q}$$

was obtained [18]. (4.25) is obtained by a slight simplification and refinement of Linnik's considerations. See [23], [21], and [35], Chapter V, § 3; [19], Chapter III, § 2.

By (4.15) and (2.4)–(2.5), (4.25) follows directly from the following proposition: For an arbitrary quaternion B the number of $B_j = B$ $(j = 1, \ldots, r')$ in equalities (4.16) is

$$\ll m^{1/2-\varrho+\varepsilon}. \tag{4.26}$$

However, proof of (4.26) has never been obtained (and it is not clear whether (4.26) generally holds). Linnik has chosen a different way and proved that (4.26) holds "on average". In fact, if the equalities of (4.16) are numbered so that

$$l+L_{jk} = B^{(j)}U_{jk} \quad (j = 1, \ldots, w';\ k = 1, \ldots, r_j), \quad \sum_{j=1}^{w'} r_j = r', \tag{4.27}$$

where $B^{(1)}, \ldots, B^{(w')}$ are distinct quaternions of norm q^s, then

$$\sum_{j=1}^{w'} r_j^2 \ll m^{1-\varrho+\varepsilon}. \tag{4.28}$$

To prove (4.28) we will note that for given j, r_j^2 pairs

$$\left.\begin{aligned} l+L_{jk'} &= B^{(j)}U_{jk'} \\ l+L'_{jk''} &= \overline{B^{(j)}}\,\overline{U_{jk''}} \end{aligned}\right\} \quad (k', k'' = 1, \ldots, r_j) \tag{4.29}$$

can be constructed, where

$$L'_{jk''} = -\overline{B^{(j)}}L_{jk''}(\overline{B^{(j)}})^{-1}$$

is an primitive integer vector of norm m. Hence (4.28) reduces to an estimate of all pairs of equalities of the type (4.29). But by application of Venkov's rotation theory (see § 2), this question reduces again to an upper estimate of the number of representations of a binary quadratic form by the sum of three squares. For details see [35], Chapter V, § 3, and [19], Chapter III, § 2 (see also [21]).

By Cauchy's inequality, (4.28), (4.15), and Siegel inequalities (2.4)–(2.5)

$$w' \geqslant \frac{(r_1+\ldots+r_{w'})^2}{r_1^2+\ldots+r_{w'}^2} \gg \frac{(m^{1/2-\varepsilon})^2}{m^{1-\varrho+\varepsilon}} = m^{\varrho-3\varepsilon},$$

and thus (4.25) is proved.

By (4.19), for sufficiently large m (4.22) and (4.25) contradict each other, which proves Theorem 5.

Corollary. *Let $Q = Q_1Q_2$ be a primitive quaternion of norm q, let m, q and u satisfy the assumptions of Theorem 5, let $r(m; Q_1, Q_2)$ be the number of primitive vectors L of norm m, for which*

$$Q_2 \diagdown (u+L), \quad (u+L)/Q_1. \tag{4.30}$$

Then for $m \to \infty$ and for fixed q,

$$r(m; Q_1, Q_2) \sim \frac{1}{\sigma_0(q)}\, r(m). \tag{4.31}$$

This is a simple consequence of Theorem 5 since there is a one-to-one correspondence between primitive vectors L of norm m with the condition $Q \diagdown (u+L)$, and primitive vectors $L' = Q_1^{-1}LQ_1$ of norm m with conditions (4.30).

[18] Pall's objections [59] of a technical character were taken into consideration in [21], pp. 243–244.

Proof of Corollary 3 to Theorem 2 (§ 3). Let $q = g^2$. By (3.23) there is an integer u such that

$$u^2+m \equiv 0 \pmod{q}. \tag{4.32}$$

By (3.24) we can, changing $(b_1, b_2, b_3) \pmod{g}$ if necessary, assume that

$$b_1^2+b_2^2+b_3^2 \equiv m \pmod{q}. \tag{4.33}$$

The quaternion $u+b_1i_1+b_2i_2+b_3i_3$ is primitive $(\mathrm{mod}\, q)$ and its norm is divisible by q. Hence, by Proposition 2 of Section 2,

$$u+b_1i_1+b_2i_2+b_3i_3 = G_2WG_1, \tag{4.34}$$

where G_1, G_2 and W are integer quaternions, $N(G_1) = N(G_2) = g$, and $G_1G_2 = Q$ is a primitive quaternion of norm q. If L is a primitive vector of norm m, $G_2\diagdown(u+L)$, $(u+L)/G_1$, then by (4.34) and Proposition 3 of Section 2,

$$L \equiv b_1i_1+b_2i_2+b_3i_3 \pmod{g}.$$

The converse is also valid. Hence (3.27) is equivalent to (4.31), and Corollary 3 of Theorem 2 is proved.

The above proof of Theorem 5 can be given a slightly different "ergodic" interpretation. (4.6)–(4.7) lead to $r(m)$ chains of primitive integer vectors of norm m:

$$L_j^{(0)}\to L_j^{(1)}\to \ldots \to L_j^{(s)} \quad (j = 1, \ldots, r(m)), \tag{4.35}$$

where

$$L_j^{(0)} = L_j, \quad L_j^{(k)} = Q_{jk}^{-1}L_j^{(k-1)}Q_{jk} \quad (k = 1, 2, \ldots, s). \tag{4.36}$$

Note that (4.36) is an orthogonal linear transformation with a rational matrix and denominator q. It can be shown without using the theory of quaternions, that for a given odd q and $-m$ being a quadratic residue $(\mathrm{mod}\, q)$, to each integer primitive point L lying on the sphere

$$x_1^2+x_2^2+x_3^2 = m \tag{4.37}$$

there correspond two and only two rational orthogonal transformations of denominator q, of L into primitive points L' (which corresponds to the rotations $L^{(k)}\to L^{(k+1)}$ and $L^{(k)}\to L^{(k-1)}$; we shall choose the first one).

For construction of the flow (4.35)–(4.36) we assume m to be a quadratic residue $(\mathrm{mod}\, q)$. This is the crucial point of Linnik's method. It is not clear whether without this assumption ([19]) any other flow of primitive integer vectors L of norm m with the necessary "ergodic properties" can be constructed — see below Theorem 5a.

[19] Or without the slightly weaker assumption (4.48) — see below.

It can be verified that any part of flow (4.35)–(4.36),

$$L_j^{(0)}\to L_j^{(1)}\to L_j^{(2)}\to \ldots \to L_j^{(s)} \quad (j = 1, \ldots, r'') \tag{4.38}$$

with the condition

$$r'' \geqslant m^{1/2-\varepsilon}, \tag{4.39}$$

where $\varepsilon > 0$ is an arbitrarily small number (without loss of generality we have changed the indices), possesses the following "ergodic" property.

THEOREM 5a. *Let the assumptions of Theorem 5 hold and let $\mathfrak{Q}_Q$ be the set of primitive vectors L of norm m, for which*

$$Q\diagdown(u+L). \tag{4.40}$$

By $s_j(Q)$ we denote the number of indices k satisfying the condition $L_j^{(k)}\in\mathfrak{Q}_Q$ $(k = 0, 1, \ldots, s;\ j = 1, \ldots, r'')$. Then chains (indices j) of flow (4.38) divide into two categories: I. *For each of the indices j of the first category, for $m\to\infty$,*

$$s_j(Q) \sim \frac{s}{\sigma_0(q)}, \tag{4.41}$$

where the constants implicit in the symbol $\sim$ depend only on q; II. *The number of indices j of the second category is the quantity of the order $o(r'')$.*

Proof of Theorem 5a. We shall carry out this proof (like the proof of Theorem 5) *a contrario*. Having an infinite subsequence of m's for which the number of indices j of the second category is $\gg r''$, one can assume that for this subsequence for every such j,

$$s_j(Q) < (1-\gamma)\frac{s}{\sigma_0(q)} \tag{4.42}$$

for a $\gamma > 0$, depending only on q. (4.42) is analogous to (4.17). Starting from this point we shall repeat the proof of Theorem 5 and in the same way arrive at contradiction, which proves Theorem 5a.

From Theorem 5a we can pass on to the following theorem on "mixing", a reinforcement of Theorem 5.

THEOREM 5b. *Under the assumptions of Theorem 5, indices k, $1 \leqslant k \leqslant s$ for flow (4.38) divide into two categories:* I. *For each of the indices k of the first category, for $m\to\infty$,*

$$r_k(Q) \sim \frac{r''}{\sigma_0(q)}, \tag{4.43}$$

where $r_k(Q)$ is the number of $L_j^{(k)}\in\mathfrak{Q}_Q$ for given k and $j = 1, \ldots, r''$, and where constants in the asymptotic formula depend only on q; II. *The number of indices of the second category is $o(s)$.*

This theorem follows from Theorem 5a by estimating the number of entries of the quaternion Q in matrix (4.8) (like the choice of equalities (4.16) with (4.15) and (4.17)).

Corollary 3 of Theorem 2 also has a corresponding "ergodic" analogue: Let $\mathfrak{R}_{g;b_1,b_2,b_3}$ be a class of vectors L, for which

$$L \equiv b_1 i_1 + b_2 i_2 + b_3 i_3 \pmod{g}. \tag{4.44}$$

Then under the assumptions of Corollary 3, for all indices $j = 1, \ldots, r''$, with the possible exception of $o(r'')$, the number $L_j^{(k)} \in \mathfrak{R}_{g;b_1,b_2,b_3}$ is asymptotically equal for $m \to \infty$ and given g, to

$$\frac{r''}{\varrho(m, g)}, \tag{4.45}$$

where $\varrho(m, g)$ is determined by (3.28). The asymptotic equality (4.45) follows from that of (4.43) by Proposition 3 of Section 2 (see the above considerations), whence the corresponding assertion on "mixing" follows.

(4.45) can also be proved directly. For this we make correspond to each residue class of vectors $L^{(t)} \pmod{g}$ and each index $k = 1, \ldots, s$, the set $\mathfrak{S}_t^{(k)}$ of integer quaternions $S \pmod{g}$, for which

$$L^{(t)} S \equiv S(b_1 i_1 + b_2 i_2 + b_3 i_3), \qquad N(S) \equiv q^k \pmod{g}. \tag{4.46}$$

Now the three-dimensional problem of obtaining the asymptotic equality (4.45) becomes the four-dimensional problem on quaternions $B_j = Q_{j1} \cdot \ldots \cdot Q_{js}$ of norm q^s, for which

$$Q_{j1} \cdot \ldots \cdot Q_{jk} \equiv S \pmod{g}, \qquad S \in \mathfrak{S}_t^{(k)}. \tag{4.47}$$

This four-dimensional problem can be solved by the circle method. For details see [35], Chapter VI, where a slightly more general problem is considered. This second variant of the ergodic method has the great advantage that condition (3.23) can be weakened by assuming the existence of any fixed prime q (not necessarily connected with g), for which

$$\left(\frac{-m}{q}\right) = 1. \tag{4.48}$$

To Linnik's theorem on the asymptotically uniform distribution of integer points on a sphere (Corollary 2 of Theorem 2) there also corresponds an "ergodic" analogue: Under the assumptions of this corollary for all chains of flow (4.38), possibly with the exclusion of $o(r'')$ exceptional chains, the number $L_j^{(k)} \in \Lambda_m$, for given j and $k = 1, \ldots, s$, is asymptotically proportional to the solid angle of the domain Λ_m.

Here also, the three-dimensional problem reduces in the proof to a four-dimensional problem: The whole surface of a sphere divides into parts $\Gamma_1, \ldots, \Gamma_n$ with small diameters so that for spherical rotations any real vector of domain Γ_t behaves in "almost" the same way say, as its centre of gravity M_t. Let $\mathfrak{Q}_t$ be the set of real quaternions X satisfying the condition

$$X^{-1} M_t X \in \Lambda_m \qquad (t = 1, \ldots, n). \tag{4.49}$$

Note that (4.49) is analogous to (4.46) of the preceding problem. $\mathfrak{Q}_t$ is a measurable cone-shaped domain of a four-dimensional space, whereby from the theory of Haar measure, for its solid angle ω_t we derive

$$\frac{\omega_t}{2\pi^2} = \frac{\lambda}{4\pi}. \tag{4.50}$$

Again there arises the four-dimensional problem of quaternions $B_j = Q_{j1} \cdot \ldots \cdot Q_{js}$ of norm q^s, for which

$$Q_{j1} \cdot \ldots \cdot Q_{jk} \in \mathfrak{Q}_t. \tag{4.51}$$

This problem can also be solved by application of the circle method. For details see [8], [16]; [35], Chapter VI; [19], Chapter IV.

On these lines Theorems 3 and 4 and also their "ergodic" analogues can be proved. Great technical difficulties arise due to the infinite number of unit elements corresponding to hermition algebra, and in the case of $m < 0$ difficulties arise in considering the cycles of binary quadratic forms governing the hyperbolic rotations of vectors L. Here it has been found useful to represent hermitions by integral quadratic matrices of the second order. For details see [10], [37]; [19], Chapters V and VI.

5. A new variant of Linnik's ergodic method.

In [20] ([20]) Linnik outlined a modification to his method which indicates new possibilities for its application. This modification is based on the following proposition ([21]) [41].

Proposition 1. *Let be given a real number ν, satisfying inequality*

$$\tfrac{1}{4} < \nu \leqslant \tfrac{1}{2}. \tag{5.1}$$

Let $m > 6$ be a square-free integer, and A be a real number such that

$$m^{\nu} \leqslant A \leqslant A_0 = m^{1/2}. \tag{5.2}$$

[20] In this section Linnik's idea is considerably changed as paper [20] contains an inaccuracy.

[21] It is desirable to generalize a little Proposition 1 (say, to get rid of the assumption that m is square-free) and to give a detailed proof of Propositions 1 and 2.

By $h(-m, A)$ we denote the number of reduced properly primitive integral positive binary quadratic forms

$$(5.3)\qquad (a, b, c) = au^2+2buv+cv^2, \quad ac-b^2 = m, \quad 2|b| \leqslant a \leqslant c$$

with the supplementary condition

$$(5.4)\qquad a \leqslant A.$$

Then a constant $\gamma > 0$ can be found, dependent only on ν, such that for $m\to\infty$,

$$(5.5)\qquad h(-m, A) = \frac{A}{A_0} h(-m)\{1+O(m^{-\gamma})\}.$$

For proof see [41] and [46]. The elementary operation of sieving by application of (5.5) and the Siegel estimate (2.5) leads to the following proposition, which is also used in the sequel.

PROPOSITION 2. *Under the assumptions of Proposition* 1 *let $t(-m; A, \frac{1}{2}A)$ be the number of square-free integers a from the interval*

$$(5.6)\qquad \tfrac{1}{2}A < a \leqslant A$$

satisfying the conditions:

(i) $(-m)$ *is a quadratic residue* $(\operatorname{mod} a)$;

(ii) *a is not divisible by any of the primes $p \leqslant \log m$.*

Then for $m\to\infty$,

$$(5.7)\qquad t(-m; A, \tfrac{1}{2}A) \gg A^{1-\varepsilon}.$$

We are now in a position to give an outline of new proof of (4.25), for square-free integers m. We should now in fact assume that constant $\varrho > 0$ is sufficiently small (we shall choose it in the sequel). This is already sufficient for obtaining all “ergodic” theorems, theorems on “mixing”, and for the asymptotic formulae (and estimates) which are treated in §§ 3, 4 by the initial ergodic method.

Besides this, according to Linnik [19], p. 204, this variant creates possibilities for broad generalizations of the ergodic method (see § 7).

Firstly assume that

$$(5.8)\qquad 0 < \varrho < \tfrac{1}{4}.$$

Suppose that the conditions (4.4), (4.5) are satisfied and that we have

$$(5.9)\qquad r' \gg m^{1/2-\varepsilon}$$

equalities

$$(5.10)\qquad l+L_i = B_i U_i, \quad N(B_i) = q^s \quad (i = 1, \ldots, r'),$$

where $\varepsilon > 0$ is an arbitrarily small real number. Let w' be the number of distinct quaternions B_i in (5.10). We shall prove that

$$(5.11)\qquad w' \gg m^{\varrho-\varepsilon},$$

where $\varepsilon > 0$ is an arbitrarily small real number.

We shall assume the contrary: There can be found such an infinitely increasing sequence m satisfying our conditions, that

$$(5.12)\qquad w' \ll m^{\varrho-\delta},$$

where $\delta > 0$ is independent of m. Further on we shall assume that m has been taken from this sequence.

By Proposition 2 we can find square-free integers [22]

$$(5.13)\qquad a_1, \ldots, a_t$$

with the conditions:

1.

$$(5.14)\qquad \tfrac{1}{2}m^{1/2-\varrho} < a_j \leqslant m^{1/2-\varrho} \quad (j = 1, \ldots, t);$$

2.

$$(5.15)\qquad m^{1/2-\varrho-\varepsilon} \ll t \ll m^{1/2-\varrho};$$

3. If p is the prime divisor of a_j $(j = 1, \ldots, t)$, then

$$(5.16)\qquad p > \log m;$$

4. The number $(-m)$ is a quadratic residue $(\operatorname{mod} a_j)$ $(j = 1, \ldots, t)$. By (5.10) and (5.16), for arbitrary j $(j = 1, \ldots, t)$ the integer l_j can be found satisfying

$$(5.17)\qquad l_j^2+m \equiv 0 \,(\operatorname{mod} q^s a_j), \quad l_j \equiv l \,(\operatorname{mod} q).$$

However, we then obtain $t\cdot r(m)$ equalities

$$(5.18)\qquad l_j+L_i = B_i V_{ij} A_{ij} \quad (j = 1, \ldots, t;\ i = 1, \ldots, r(m)),$$

where B_i and A_{ij} are primitive primary quaternions,

$$(5.19)\qquad N(B_i) = q^s, \quad N(A_{ij}) = a_j,$$

where B_i, determining by L_i, do not depend on j and for $i = 1, \ldots, r'$ egual to B_i from (5.10).

From (5.18) we obtain equalities

$$(5.20)\qquad l_j+L_{ij} = A_{ij} B_i V_{ij} \quad (i = 1, \ldots, r';\ j = 1, \ldots, t),$$

[22] Added in proof. See: Н. В. Плоскурин, Записки научн. семинаров ЛОМИ 50 (1975), pp. 169–178.

where

$$L_{ij} = A_{ij} L_i A_{ij}^{-1} \tag{5.21}$$

is an integer primitive vector of norm m. We have

$$A_{ij} B_i = \tilde{B}_{ij} \tilde{A}_{ij}, \quad N(\tilde{B}_{ij}) = q^s, \quad N(\tilde{A}_{ij}) = a_j \qquad (i = 1, \ldots, r';\ j = 1, \ldots, t), \tag{5.22}$$

where $\tilde{B}_{ij}$ and $\tilde{A}_{ij}$ are primitive primary quaternions (uniquely determined by (5.22) in virtue of Propositions 1 and 7 of Section 2).

Let

$$B^{(1)}, \ldots, B^{(g)} \tag{5.23}$$

be the set of all primitive primary quaternions of norm q^s so that

$$g = q^s \prod_{p|q} \left(1 + \frac{1}{p}\right) \tag{5.24}$$

(see Proposition 8 of § 2).

For given j and k, the number h_{jk} of distinct quaternions $\tilde{A}_{ij}$ in (5.22) satisfying the supplementary condition

$$\tilde{B}_{ij} = B^{(k)} \tag{5.25}$$

for the given $B^{(k)}$, is estimated as

$$h_{jk} \ll m^{1/2-\varrho-\gamma}, \tag{5.26}$$

where $\gamma > 0$ is a constant dependent on δ but not on m. In fact the number of primitive primary quaternions A of norm a_j, for which $B^{(k)}A$ is right divisible by the given quaternion $B^{(l)}$ of norm $q^s \asymp m^\varrho$, is

$$\ll \frac{a_j}{m^\varrho} \ll m^{1/2-2\varrho+\varepsilon}, \tag{5.27}$$

for sufficiently small $\varrho > 0$ (see [35], Chapter IV, § 3). The number w' of distinct B_i in (5.22) (i.e. in (5.10)) is however estimated by (5.12).

Let r_k be the number of equalities

$$l + L_i = B_i U_i \quad (i = 1, \ldots, r = r(m)) \tag{5.28}$$

with the condition

$$B_i = B^{(k)}, \tag{5.29}$$

and let $r_k^{(j)}$ be the number of equalities (5.22) with condition (5.25) for given j ($k = 1, \ldots, g$; $j = 1, \ldots, t$). Then

$$\sum_{k=1}^{g} r_k = r \tag{5.30}$$

and

$$r_k^{(j)} \leqslant r_k, \quad \sum_{k=1}^{g} r_k^{(j)} = r' \quad (j = 1, \ldots, t;\ k = 1, \ldots, g). \tag{5.31}$$

We shall prove that there exists such k ($1 \leqslant k \leqslant g$), that the number of indices j, for which

$$r_k^{(j)} \geqslant r_k m^{-\gamma/4} \tag{5.32}$$

and

$$r_k \geqslant m^{1/2-\varrho-\gamma/8}, \tag{5.33}$$

will be

$$\geqslant t m^{-\gamma/4}. \tag{5.34}$$

In fact in the opposite case, for every k either

$$r_k < m^{1/2-\varrho-\gamma/8}, \tag{5.35}$$

or the number j with condition (5.32) is

$$< t m^{-\gamma/4}. \tag{5.36}$$

Therefore, by (5.31), (5.35), (5.36), (5.24), (4.4), (5.30) and (5.15),

$$\sum_{k=1}^{g} \sum_{j=1}^{t} r_k^{(j)} \leqslant g m^{1/2-\varrho-\gamma/8} + (t m^{-\gamma/4}) \sum_{k=1}^{g} r_k + t \sum_{k=1}^{g} (r_k m^{-\gamma/4}) \tag{5.37}$$
$$\ll m^{1/2-\gamma/8} + m^{-\gamma/4} tr \ll m^{1-\varrho-\gamma/4+\varepsilon}.$$

On the other hand, by (5.15), (5.31) and (5.9),

$$\sum_{k=1}^{g} \sum_{j=1}^{t} r_k^{(j)} = tr' \gg m^{1-\varrho-\varepsilon}. \tag{5.38}$$

Since for large m estimates (5.37) and (5.38) contradict each other, we can choose index $k = k_0$ with condition (5.33), whereby the number of indices j with condition (5.32) has the lower estimate (5.34).

We fix such k and for a given j we will find the lower estimate for the number of pairs of equalities

$$\begin{aligned} l_j + L_{ij} &= \tilde{B}_{ij} \tilde{A}_{ij} V_{ij}, \\ l_j + L_{i'j} &= \tilde{B}_{i'j} \tilde{A}_{i'j} V_{i'j} \end{aligned} \tag{5.39}$$

with the conditions

$$\tilde{B}_{ij} = \tilde{B}_{i'j} = B^{(k)} \tag{5.40}$$

and

$$\tilde{A}_{ij} = \tilde{A}_{i'j} \tag{5.41}$$

(including the trivial pairs $i = i'$). Let $r_k^{(j,v)}$ be the number of equalities (5.20)–(5.22)–(5.25) for given j, k and

$$\tilde{A}_{ij} = \tilde{A}^{(v)} \tag{5.42}$$

$(v = 1, \ldots, h_{jk})$. Then

$$\sum_{v=1}^{h_{jk}} r_k^{(j,v)} = r_k^{(j)},$$

and on applying the Cauchy inequality, from (5.26) it follows that for given j the number of pairs of equalities of the type (5.39)–(5.40)–(5.41) is equal to

$$\sum_{v=1}^{h_{jk}} (r_k^{(j,v)})^2 \geqslant \frac{1}{h_{jk}} (r_k^{(j)})^2 \gg m^{-1/2+\varrho+\gamma} (r_k^{(j)})^2. \tag{5.43}$$

However, for this k and due to (5.33), (5.32), (5.34) and (5.15), the number of pairs of equalities (5.39)–(5.40)–(5.41) is

$$\gg \sum_{j=1}^{t} m^{-1/2+\varrho+\gamma} (r_k^{(j)})^2 \geqslant t m^{-\gamma/4} m^{-1/2+\varrho+\gamma} (r_k m^{-\gamma/4})^2 \gg m^{\gamma/4-\varepsilon} r_k^2. \tag{5.44}$$

Estimate (5.44) also holds for the number of non-trivial pairs of (5.39)–(5.40)–(5.41) (for our k), since by (5.15) the number of trivial pairs is

$$\ll t r_k \ll m^{1/2-\varrho} r_k,$$

and since by (5.33)

$$m^{\gamma/4-\varepsilon} r_k^2 \gg m^{1/2-\varrho+\gamma/8} r_k.$$

On the other hand, the number of all pairs of vectors (L, L') with conditions (5.28)–(5.29) is

$$\ll r_k^2. \tag{5.45}$$

By estimations (5.44) and (5.45) we obtain that

$$\gg m^{\gamma/8} \tag{5.46}$$

pairs of equalities (5.39)–(5.40)–(5.41) can be found, for which

$$L_{ij} = L_0, \quad L_{i'j} = L_0', \tag{5.47}$$

where (L_0, L_0') is a fixed pair of distinct vectors satisfying (5.28)–(5.29) for given k. From (5.39) with conditions (5.40) and (5.41) we find that $N(L_0 - L_0')$ is divisible by $\gg m^{\gamma/8}$ distinct numbers of the set (5.13).

But this is impossible since

$$0 \neq N(L_0 - L_0') \ll m,$$

and since the least common multiple of the described divisors from (5.13) is

$$\gg m^2.$$

In fact, since the prime factors of numbers from (5.13) satisfy (5.16), if the least common multiple were $< m^2$ the number of all prime factors of all our divisors would be

$$\leqslant \frac{\log m^2}{\log\log m} = 2 \frac{\log m}{\log\log m}.$$

From these factors, no more than

$$2^{2 \frac{\log m}{\log\log m}}$$

distinct square-free integers can be found, which contradicts the estimate $\gg m^{\gamma/8}$ for the number of divisors. This contradiction proves estimate (5.11).

The final considerations can be simplified and made more accurate if instead of Proposition 2 we prove the existence (under the assumptions of Proposition 1) of $\gg A^{1-\varepsilon}$ primes (or almost-primes) a with conditions

$$\tfrac{1}{2}A < a \leqslant A, \quad \left(\frac{-m}{p}\right) = 1, \quad p \mid a.$$

6. On some unsolved problems from the theory of ternary quadratic forms. "As usual the unsolved problems from a given field of studies are more numerous, and also much more difficult, than those that have been solved" (Y. V. Linnik [19], Chapter XI). Unsolved problems related to Linnik's ergodic method are discussed in report [17] and in monographs [35] (Conclusion) and [19], Chapter XI.

In Sections 6–8 we shall formulate some of these unsolved problems and consider possible means for their solution by application of Linnik's ergodic method. This section is devoted to ternary quadratic forms.

6.1. The representation of numbers by indefinite ternary quadratic forms. In Theorems 3, 4 of § 3, due to Linnik [7], [10] $(m > 0)$ and Skubenko [36], [37] $(m < 0)$, the indefinite ternary quadratic form

$$f_0 = x_1 x_3 - x_2^2 \tag{6.1}$$

was considered. Of course there now arises the problem of generalizing the results of Linnik and Skubenko to integral indefinite ternary quadratic forms more general than (6.1). It is assumed that $d(f) = \det f \neq 0$ (since otherwise the problem becomes "binary"). Without loss of generality we can assume that in the representation of f as the sum of three squares of real linear forms, one square will be positive and two negative. Then, as for f_0,

$$f(x_1, x_2, x_3) = m \tag{6.2}$$

is for $m > 0$ a hyperboloid of two sheets and for $m < 0$ a hyperboloid of one sheet.

It appears that the considerations of Linnik and Skubenko can be generalized if we develop in the appropriate way (see [35], Chapter IV), the arithmetic of indefinite hermitions of $\mathfrak{A}_f$, and in particular if the theorem on decomposition (Proposition 2, § 2) and the theory of the rotations of vectors (see § 2) are established. In the case $f = f_0$ this has been done by Linnik and Skubenko who found representations of integer hermitions of the algebra $\mathfrak{A}_{f_0}$ by integer rational quadratic matrices of the second order. The representation of $\mathfrak{A}_f$ by second order matrices ([23]) does not generally appear to serve any purpose. One should therefore carry out studies directly with hermitions from $\mathfrak{A}_f$.

The decomposition theorem (generalized to some extent ([24])) follows from the Eichler theorem [53] that all ideals of a simple central algebra over the field of rational numbers which is not a definite hermition algebra, are principal.

The great technical difficulties arise from the existence of an infinite number of units. It would be interesting to by-pass these difficulties by generalizing the concept of the primary quaternion to indefinite hermitions. If this is not possible studies should be limited to hermitions belonging to the fundamental domain of a group of automorphisms of the form f, and in all operations with them it should be ensured that vectors do not depart from the reduction domain (for the case $f = f_0$ this has been done in papers [10] and [37]; see also [19], Chapters V and VI).

For realizing Linnik's ergodic method in the case $m < 0$, Skubenko's theorem on cycles [37] (for a formulation see the footnote ([6]) of this paper) and its generalization to automorphisms of the form f are necessary. It should be noted that Skubenko's theorem on cycles is interesting in itself. It would be worthwhile to find for it a direct proof, which does not use the theory of rotations of hermitions (or integral matrices of the second order).

It would be interesting to study the relationship between the decomposition of hermitions from $\mathfrak{A}_f$ and the property of the form f (one class per genus) given by Meyer's theorem [58], and papers [56] and [57] in which it is made more precise. In this connection, the question of the existence of a Euclidean algorithm for rings of integer hermitions in $\mathfrak{A}_f$ is also of interest.

Finally the case $m = 0$, i.e. the question of integer points on the cone

$$f(x_1, x_2, x_3) = 0, \tag{6.3}$$

should be considered. This problem is generally simpler than that of integer points on the hyperboloid ($m \neq 0$) since integer points of the cone (6.3) permit rational parametrization. Particular cases of this problem are considered in [49], [38] and others. As far as we know the general case has not been fully studied.

6.2. The representation of numbers by positive ternary quadratic forms. Here two problems naturally arise:

a. to extend the results of [35], Chapter V (Theorems 1–5) to as general as possible integral positive ternary quadratic forms f, i.e. if possible without assuming that invariants $[\Omega, \Delta]$ are odd and coprime; not forgetting however, that for some forms f results of the type of Theorems 1–5 [35], Chapter V do not hold; see the counter-examples of Jones and Pall [55]);

b. to prove asymptotic formulae in all these cases (or in as many cases as possible).

We believe that the most natural way of applying the ergodic method is as follows. Let us consider the set of hermition algebras

$$\{\mathfrak{A}_{f_1}, \ldots, \mathfrak{A}_{f_g}\}, \quad f_1 = f,$$

where $f_1, \ldots, f_g$ are representants of all classes of forms of the genus f (one can say, the "genus" of integral order of a hermition algebra over a field of rational numbers). In each of these algebras we single out the primitive integer vectors of norm Δm. In doing so we consider proper representations of the number m by the genus f. For the number of such representations, formulae representing this number by $h(-\Delta m)$ are known (see e.g. Jones [54]). For a thus constructed genus of primitive vectors of norm Δm one can try to construct the flow of vectors and prove its "ergodicity", and then to obtain asymptotic formulae.

By constructing and studying the flow we put ourselves in need of a generalization of Venkov's theory [39] of rotations of integer vectors (see also § 2) for genera of primitive vectors of the hermition algebra $\mathfrak{A}_f$. Thereby, to the pair of vectors (L, L') corresponds an ideal of algebra $\mathfrak{A}_f$ (containing L), "governing" the rotation from L to L'.

We also need generalizations of the theorems on hermitions of a large norm (see [35], Chapter IV, § 3), for ideals. One can consider these gen-

[23] Although representation by quadratic second order matrices with integer algebraic elements is apparently possible.

[24] The difference between definitions of integer hermitions in our paper and those of Eichler should be noted.

eralizations as the quantitative analogue of the theorem on rational transformations of one form of a genus into another (see [35], Chapter V, Remark 7), which is in itself of interest.

However, in studies of the posed problem one can more directly follow the considerations of monograph [35]. It appears that it is possible to generalize Remark 7, [35], Chapter V (refining Smith's theorem on rational transformations of forms of a genus) for some cases of not coprime or even invariants $[\Omega, \Delta]$ (here it is necessary to bear in mind the aforementioned counter-examples of Pall–Jones [55]). Once for the genus of some form f a proposition of the type of Remark 7, [35], Chapter V is proved, for the forms of this genus we can derive Theorem 1, [35], Chapter V, and hence all the remaining results of Chapter V, [35].

In this way one can also try to obtain asymptotic formulae. Here, for applying the method Remark 7, [35], Chapter V, should be made more precise by obtaining asymptotic formulae for the number of rational transformations of one given form of a genus into another with a given increasing denominator. This problem is cognate to that on the representation of large numbers by quaternary quadratic forms (see Hermite's formulae for the automorphs of ternary quadratic forms), and to solve it one can attempt to apply the asymptotic formulae of [35], Chapter III.

6.3. On the condition $\left(\frac{-\Delta m}{q}\right) = 1$. This condition is necessary for the construction of a flow of vectors, and is an essential feature of Linnik's ergodic method.

For all genera of ternary quadratic forms, with the exception of genera with characters

$$\left(\frac{-\Delta m}{q}\right) = -1 \tag{6.4}$$

for all odd primes $q|\Omega$ (q prime to Δ), this condition is a consequence of the necessary "generic" (p-adic) conditions for representing m by the form f.

For the remaining "exceptional" genera (among them the genus of the form $f = x_1^2+x_2^2+x_3^2$) this condition appears to be unnecessary, depending only on the method applied for proof. One can be freed of this condition by assuming the validity of some Hypothesis ($\mathfrak{H}$) on zeros of L-functions with real characters, lying in the neighbourhood of $s = 1$ (see [35], Chapter V, § 5; Chapter VI, § 2). It would be interesting to weaken this hypothesis and ideally, to completely get rid of it.

6.4. The remainder terms of asymptotic formulae. In all the asymptotic formulae obtained hitherto with the help of the number theoretic-ergodic method, the remainder terms have not been estimated. The problem of estimating these terms naturally arises. According to Linnik [19], Chapter XI, by the ergodic method one can obtain estimates for the remainder term of the order

$$O\left(\frac{1}{\log^{\gamma} m}\right), \tag{6.5}$$

where $\gamma > 0$ is a constant.

According to monographs [35] and [19] it appears that by straightforward application of Linnik's method, estimate (6.5) can be obtained, but under a certain assumption about the lower estimate for $h(-\Delta m)$ which is better than the Siegel estimate (2.5). Such an estimate can be derived from some still unproved hypotheses of ($\mathfrak{H}$) type on zeros of Dirichlet L-functions, mentioned in 6.3. An unconditional estimate of the type (6.5) can be obtained for the remainder terms, based upon the variant of the ergodic method presented in Section 5 of this paper.

6.5. On ternary forms with integer algebraic coefficients. It is of great interest to generalize these considerations (including the arithmetic of hermitions) for the representation of integer algebraic numbers by ternary quadratic forms with integer algebraic coefficients.

6.6. On the arithmetic of hermitions. In all these considerations an important role is played by the arithmetic of hermitions. The study of the arithmetic of hermitions (generalized quaternions) is in itself interesting. It is particularly interesting to consider the conditions on which a Euclidean algorithm can exist in the algebra $\mathfrak{A}_f$, and also the relationship between the property of the form f "one class per genus" (Meyer type theorems [58], [56], [57]) and the assumption that all ideals of the algebra $\mathfrak{A}_f$ are principal.

6.7. On the possibility of replacing the apparatus of the arithmetic of hermitions by considering rational transformations of ternary quadratic forms. Let f be an integral primitive ternary quadratic form of determinant $d \neq 0$, and let (x_1, x_2, x_3) be a proper representation of m by form f. If p is an odd prime number with the condition

$$\left(\frac{-\Delta m}{p}\right) = 1, \tag{6.6}$$

it can be shown that the rational substitution S of denominator p and determinant ± 1 can be found for which

$$fS \text{ is an integral form} \tag{6.7}$$

and

$$\begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} S^{-1} \text{ is a primitive integer vector} \tag{6.8}$$

(if however (6.6) is not satisfied, such a substitution S does not exist). By choosing S from among substitutions SU, where U is a unimodular substitution, we will be able to obtain the uniqueness of S.

Therefore we can construct a flow of primitive representations of number m, satisfying (6.6), by forms of the genus f. Proofs of "ergodic" theorems and their corollaries (theorems on "mixing" and asymptotic formulae) for this flow without using the apparatus of the arithmetic of hermitions, are of great interest.

7. Linnik's programme for studies of the ergodic properties of algebraic fields. As previously stated, problem of the distribution of integer points in domains (3.31), (3.33) (for $m > 0$) and (3.31), (3.38) (for $m < 0$) can be considered as the question of the distribution of ideal classes of imaginary and real quadratic fields. Thereby ergodic properties of second order matrices L, satisfying the condition

$$L^2 = -m, \tag{7.1}$$

were analysed. In his report [17] to the 3rd All-Union Mathematical Congress in 1956 (see also [15], and [19], Chapter VII and Chapter IX, § 1) Linnik designated a wide programme for the extension of these results onto nth order matrices and arbitrary algebraic number fields. That is the study of asymptotic properties of a sequence of algebraic fields depending on the parameter D (for quadratic fields this is the discriminant m), and the application of obtained results to systems of Diophantine equations with a small number of unknown quantities (indeed, of a special type).

Let $a_1(D), \ldots, a_n(D)$ be integral functions of the parameter $D \to \infty$. To the algebraic number field

$$K_D = Q(\theta_D), \tag{7.2}$$

where

$$\theta_D^n + a_1(D)\theta_D^{n-1} + \ldots + a_n(D) = 0, \tag{7.3}$$

there corresponds a set of integral quadratic nth order matrices $L = L_D$, satisfying condition

$$L^n + a_1(D)L^{n-1} + \ldots + a_n(D)E = 0. \tag{7.4}$$

(The matrix L is an analogue of a vector of hermition algebra.)

The set of quadratic real nth order matrices satisfying condition (7.4) forms a variety of dimension (generally speaking) $n^2 - n$. We are interested in the problem of the distribution of integer matrices L on this variety, and particularly in the problem of the uniform distribution of these matrices in this variety (in the sense of the corresponding invariant measure).

In accordance with the principles of the method considered for proving the uniformity of the distribution, a "flow" of integer matrices L, satisfying (7.4), should be constructed and the "ergodicity" of this flow should be proved. A flow of integer matrices L can be constructed with the help of the following Linnik's theorem, given without proof in [15], [17], and [19], Chapter VII.

PROPOSITION 1. *Let L and Q be integer matrices whenever the determinant of matrix Q is square-free. For the matrix*

$$L' = Q^{-1}LQ \tag{7.5}$$

to be an integer matrix it is necessary and sufficient that there exists an integer l for which

$$lE + L = QU, \tag{7.6}$$

where U and E are integer and unit matrices respectively.

The uniqueness of transition

$$L \to L' = Q^{-1}LQ \tag{7.7}$$

can be achieved by singling out the reduction domain [25] on (7.4) (with real L).

To prove the ergodicity of the flow it is necessary to develop a theory of rotations of matrices L, generalizing Venkov's theory of rotations of vectors (see § 2 above). Some assertions of such a future theory have been given without proofs by Linnik (see [19], Chapter VII, § 3, and also [15] and [17]). It seems, according to Linnik, that there the variant of the ergodic method described in Section 5 will be particularly useful.

The integral matrix L satisfying (7.4), gives an integral solution of a special system of n Diophantine equations of n^2 unknown quantities (see [19], Chapter VII, § 1). Ergodic theorems would lead to asymptotic formulae for the number of solutions of such a system. Note that due to the small number of variables, ordinary analytic methods cannot be applied here.

[25] The construction of the reduction domain is a difficult problem which has not been fully solved, even for particular cases of (7.4).

Ergodic and asymptotic theorems for integer matrices L satisf (7.4) and lying in the reduction domain, can be considered as some formation on the asymptotic (for $D\to\infty$) distribution of ideals of field K_D. Although here, the relationship between matrices L and ic of the field K_D (excluding the case of the imaginary quadratic fiel $= -D$, $D > 0$) is so far not quite clear. Linnik proposed the applica of the Châtelet–Schur theorem for the construction of a flow of id of the field K_D representing them by the system of nth order qu ratic matrices

$$[\Omega_1, \ldots, \Omega_n].$$

For some details see [19], Chapter VII, § 2 (and also [15] and [17]).

These conditions can of course also be generalized (see [19], Cha IX, § 1) for the case when elements of the matrix L are integers o algebraic number field. This permits us firstly to include in the gen scheme the considerations based upon the arithmetic of hermitions $\mathfrak{A}_f$ an arbitrary form f (in particular the consideration of the distribu of integer points on ellipsoids), and secondly to take into considera new types of systems of Diophantine equations for rational integ

Unfortunately, with the exception of the special auxiliary the ergodic method) considerations of distribution of quadratic inte matrices on a discriminant surface (see [47], [48], and [19], Chapter V [50] and [51]), for $n > 2$ no complete results have been obtained. I natural to begin this consideration with the simplest case of the Kum field

$$L^n = \pm D, \tag{7.8}$$

where D is free of nth powers and $D\to\infty$, in particular, with case $n = 3$. Here we at once meet with analogues of cycles and have first to obtain for them an assertion corresponding to Skuben cycle theorem [37].

8. Final remarks

8.1. On the representation of numbers by the sums of cubes, on related problems. By applying the algebraic identity

$$u^3+v^3 = \frac{H^3}{4}+3H\left(u-\frac{H}{2}\right)^2, \quad \text{where} \quad H = u+v, \tag{8.1}$$

Linnik [43] and [44] (see also [21], Chapter III) derived from the theo on the representation of numbers by positive ternary quadratic fo (contained in Theorem 1 § 3), the following interesting arithmetical position.

THEOREM 6. *Every sufficiently large integer is the sum of seven cubes of non-negative integers.*

Watson [61], by using Linnik's idea (and in particular the identity (8.1)), gave a simplified variant of the proof of this theorem, in which the well-known Gauss theorem on the representation of numbers by the sum of three squares only was applied.

In article [21] Linnik had already considered the question of the representation of special types of large integers by the sum of six cubes of non-negative integers. By the same method Linnik [45] and Watson [62] studied questions on the representation of large numbers m in the form

$$m = x_1^2+x_2^2+y_1^3+y_2^3+y_3^3 \tag{8.2}$$

or

$$m = x_1^2+y_1^3+y_2^3+y_3^3+y_4^3+y_5^3, \tag{8.3}$$

where $x_1, x_2, y_1, \ldots, y_5$ are non-negative integers. Related problems have been studied in [45].

These considerations can be generalized in several directions. The most interesting (and difficult) problem within the framework of the Linnik conception given in Section 8.2 is to prove the representability of all large integers by the sum of six cubes of non-negative integers.

8.2. The ergodicity of the modular invariant. Let $m > 0$. To the integer point (x_1, x_2, x_3) of the hyperboloid

$$x_2^2 - x_1x_3 = m \tag{8.4}$$

there corresponds the positive binary quadratic form

$$(x_1, x_2, x_3) = x_1u^2+2x_2uv+x_3v^2 \tag{8.5}$$

of determinant $m = x_2^2-x_1x_3$, and to form (8.5) there corresponds the point

$$\omega = \frac{-x_2+\sqrt{-m}}{2x_1} \tag{8.6}$$

of the half-plane $H = \{s \mid \operatorname{Im} s > 0\}$ of the complex plane $s = \sigma+it$. And to the reduced forms

$$(x_1, x_2, x_3), \quad 2|x_2| \leqslant x_1 \leqslant x_3 \tag{8.7}$$

there correspond points of the fundamental domain

$$\Delta_0 = \{-\tfrac{1}{2} \leqslant \sigma \leqslant \tfrac{1}{2},\ \sigma^2+t^2 \geqslant 1\} \tag{8.8}$$

of the whole modular group Γ of transformations of the half-plane H.

We shall consider the modular figure

$$M = \{\gamma \Delta_0 |\ \gamma \in \Gamma\}. \tag{8.9}$$

To the sequence

$$L,\ L_1 = Q_1^{-1} L Q_1,\ L_2 = Q_2^{-1} L_1 Q_2, \ldots \tag{8.10}$$

of integer points of hyperboloid (8.4), if L_i and Q_i are suitably ch (in their classes), there corresponds (see [19], Chapter V, § 19) ei the sequence of points

$$\omega,\ \omega/p,\ \omega/p^2, \ldots \tag{8.11}$$

of the half-plane H, or the sequence of points

$$\{\omega\},\ \{\omega/p\},\ \{\omega/p^2\}, \ldots \tag{8.12}$$

of the fundamental domain Δ_0 respectively. Here $\{\omega\}$ is a point l in Δ_0 and equivalent to point ω with respect to the group Γ.

One can consider (8.12) as a sequence of "generalized fracti parts" with respect to the modular figure M (similar to ordinary f tional parts of complex numbers with respect to a quadratic lattice the fundamental domain $0 \leqslant \sigma \leqslant 1$, $0 \leqslant t \leqslant 1$), (8.12) being fracti parts in Lobatchewsky geometry. Ergodic theorems for integer po of hyperboloid (8.4) (see § 3) become a question on the distributio such "fractional parts". However according to Linnik, ordinary metl for studying fractional parts are not applicable here due to known p liarities in the behaviour of a modular figure in the neighbourhoo a real axis.

Linnik ([15], [17], and [19], Chapter V, § 19) proposed one r interpretation of ergodic theorems for imaginary quadratic fields in te of the modular invariant $I(\omega)$.

It is not clear whether such "modular" interpretations can sim considerations of ergodic properties, although this subject merits r detailed study and generalizations for other fields, in particular the quadratic field. It is also not clear whether in the general case there any connections with automorphic functions.

There is also the problem to give an interpretation similar to (8 for integer points of the general hyperboloid of two sheets

$$f(x_1, x_2, x_3) = m,$$

where f is an indefinite integral quadratic form (see § 6.1).

8.3. "The elementary-ergodic method". For applications of the n ber theoretic dispersion method Linnik needed some considerations with an "ergodic" character. It should be noted however, that he

a different technique in his considerations. For some details see [19], Chapter IX, § 3. Later on, B. M. Bredihin, P. P. Vekhov, Y. P. Golubeva, T. T. Tonkov and others were working in the same direction.

8.4. On the method. When we speak about Linnik's ergodic method in number theory we have in mind a really precise and specific method of the analytic number theory, which we have tried to describe to some extent in this paper. Unfortunately, it has nothing in common with methods of the classical ergodic theory [26], although the results are analogous to those of the ergodic theory. We would like to hope that it is possible to build a unique theory of which the classical ergodic method and the "discrete" Linnik ergodic method are particular cases. The main difficulty here lies in the construction of a working analogue for invariant measure.

References [27]

[1] Ю. В. Линник, *Несколько новых теорем о представлении больших чисел отдельными положительными тернарными квадратичными формами*, Докл. АН СССР 24 (1939), pp. 211–212.

[2] — *О представлении больших чисел положительными тернарными квадратичными формами*, Докл. АН СССР 25 (1939), p. 578.

[3] — *Одна общая теорема о представлении чисел отдельными тернарными квадратичными формами*, Изв. АН СССР, сер. матем. 3 (1939), pp. 87–108.

[4] — *On certain results relating to positive ternary quadratic forms*, Матем. сб. 5 (47) (1939), pp. 453–471.

[5] — *О представлении больших чисел положительными тернарными квадратичными формами*, Изв. АН СССР, сер. матем. 4 (1940), pp. 363–402.

[6] — *Кватернионы и числа Кэли; некоторые приложения арифметики кватернионов*, Успехи матем. наук 4 (1949), № 5 (33), pp. 49–98.

[7] — *Некоторые приложения геометрии Лобачевского к теории бинарных квадратичных форм*, Докл. АН СССР 93 (1953), pp. 973–974.

[8] — *Асимптотическое распределение целых точек на сфере*, Докл. АН СССР 96 (1954), pp. 909–912.

[9] — *Применение теории цепей Маркова в арифметике кватернионов*, Успехи матем. наук 9 (1954), № 4 (62), pp. 203–210.

[10] — *Асимптотическое распределение приведенных бинарных квадратичных форм в связи с геометрией Лобачевского, I—II—III*, Вестник Ленинград. ун-та 1955, № 2, pp. 3–23; № 5, pp. 3–32; № 8, pp. 15–27.

[11] — *Нові арифметичні застосування геометрії Лобачевського*, Доповіді АН Укр. РСР 1955, № 2, pp. 112–114.

[26] It should be noted that in his publications Linnik always refrained from calling this method "ergodic".

[27] [1]–[37] is the complete collection of works directly devoted (fully or partly) to Linnik's ergodic method. Articles [43], [44] and [45] contain applications of the ergodic method. [47], [48], [50], [51] and [41], [46] contain results (of interest in themselves) which have been used by the ergodic method. A number of Linnik's articles are translated in English (see: this Journal, pp. 11–35).

[12] Ю. В. Линник, *An application of the theory of matrices and of Lobaischevskia geometry to the theory of Dirichlet's real characters*, J. Indian Math. Soc. 20 (1956 pp. 37–45.

[13] — *Цепи Маркова в аналитической арифметике кватернионов и матри* Вестник Ленинград. ун-та 1956, № 13, pp. 63–68.

[14] — *Асимптотическая геометрия гауссовых родов; аналог эргодической теоремı* Докл. АН СССР 108 (1956), pp. 1018–1021.

[15] — *Еще об аналогах эргодических теорем для мнимого квадратичного пол* Докл. АН СССР 109 (1956), pp. 694–696.

[16] — *Асимптотико-геометрические и эргодические свойства множества цель точек на сфере*, Матем. сб. 43 (85) (1957), pp. 257–276.

[17] — *Некоторые применения неэвклидовых геометрий к теории характер Дирихле; аналоги эргодических теорем*, Труды 3-го Всесоюзн. матем. съезд т. 3, Москва 1958, pp. 21–29.

[18] — *Пять лекций о некоторых вопросах теории чисел и теории вероятност (Лекция 3. Целые точки на сфере и цепи Маркова. Аналоги эргодически теорем для целочисленных матриц)*, Труды Матем. ин-та АН Венгрии (1959), pp. 238–244.

[19] — *Эргодические свойства алгебраических полей*, Ленинград 1967, 208 p

[20] — *Application of the method of D. Burgess to the investigation of integer poin on large spheres*, Symposia Math. 5v. 4, London–New York 1970, pp. 99–112.

[21] Ю. В. Линник и А. В. Малышев, *Приложения арифметики кватернион к теории тернарных квадратичных форм и к разложению чисел на куб* Успехи матем. наук 8 (1953), № 5 (57), pp. 3–71; 10 (1955), № 1 (63), p 243–244 (исправление).

[22] — — *О целых точках на сфере*, Докл. АН СССР 89 (1953), pp. 209–21

[23] А. В. Малышев, *О представлении больших чисел положительными те нарными квадратичными формами*, Докл. АН СССР 87 (1952), pp. 175–17

[24] — *О представлении чисел положительными тернарными квадратичны формами*, Докл. АН СССР 89 (1953), pp. 405–406.

[25] — *Асимптотический закон для представления чисел некоторыми полож тельными тернарными квадратичными формами*, Докл. АН СССР 93 (195 pp. 771–774.

[26] — *О целых точках на эллипсоидах*, Успехи матем. наук 9 (1954), № 3 (6 pp. 253–255.

[27] — *О целых точках на эллипсоидах*, Вестник Ленинград. ун-та 1956, № 1 pp. 18–34.

[28] — *Асимптотическое распределение целых точек на некоторых эллипсоида* Изв. АН СССР, сер. матем., 21 (1957), pp. 457–500.

[29] — *О представлении больших чисел положительными тернарными квадр тичными формами нечетных взаимно простых инвариантов*, Докл. АН СС 118 (1958), pp. 1078–1080.

[30] — *О связи теории распределения нулей L-рядов с арифметикой тернарн квадратичных форм*, Докл. АН СССР 122 (1958), pp. 343–345.

[31] — *К теории тернарных квадратичных форм. I. Об арифметике эрмитион* Вестник Ленинград. ун-та 1959, № 7, pp. 55–71.

[32] — *К теории тернарных квадратичных форм. II. Об одной теореме Линник* Вестник Ленинград. ун-та 1959, № 13, pp. 63–70.

[33] — *К теории тернарных квадратичных форм. III. О представлении больш чисел положительными формами нечетных взаимно простых инвариант* Вестник Ленинград. ун-та 1960, № 1, pp. 70–84.

[34] А. В. Малышев, *К теории тернарных квадратичных форм. IV. О связи с гипотезой Римана*, Вестник Ленинград. ун-та 1960, № 7, pp. 14–27.

[35] — *О представлении целых чисел положительными квадратичными формами* (Труды МИАН, т. 65), Москва–Ленинград 1962, 212 pp.

[36] Б. Ф. Скубенко, *Асимптотическое распределение и эргодические свойства целых точек на однополостном гиперболоиде*, Докл. АН СССР 135 (1960), pp. 794–795.

[37] — *Асимптотическое распределение целых точек на однополостном гиперболоиде и эргодические теоремы*, Изв. АН СССР, сер. матем., 26 (1962), pp. 721–752.

[38] Г. Бабаев, *Распределение целых точек на алгебраических поверхностях*, Душанбе, 1966, 279 pp.

[39] Б. А. Венков, *Об арифметике кватернионов. I–V*, Изв. Российск. АН 1922, pp. 205–220, 221–246; Изв. АН СССР, отд. физ.-матем. наук, 1929, pp. 489–504, 535–562, 607–622.

[40] — *Элементарная теория чисел*, Москва–Ленинград 1937, 219 pp.

[41] А. И. Виноградов, Ю. В. Линник, *Гиперэллиптические кривые и наименьший простой квадратичный вычет*, Докл. АН СССР 168 (1966), pp. 259–261.

[42] Б. Н. Делоне, *Геометрия положительных квадратичных форм. I–II*, Успехи матем. наук, вып. III (1937), pp. 16–62; вып. IV (1938), pp. 102–164.

[43] Ю. В. Линник, *О разложении больших чисел на семь кубов*, Докл. АН СССР 35 (1942), p. 179.

[44] — *On the representation of large numbers as sums of seven cubes*, Матем. сб. 12 (54) (1943), pp. 218–224.

[45] — *Additive problems involving squares, cubes and almost primes*, Acta Arith. 21 (1972), pp. 413–422.

[46] — *Sur une application du théorème d'André Weil à la théorie des caractères de Dirichlet*, Seminaire Delange-Pisot-Poitou. Théorie des nombres, 8-e année, 1966/67 (1968), 6–01 – 6–07.

[47] Ю. В. Линник, Б. Ф. Скубенко, *К асимптотике целочисленных матриц третьего порядка*, Докл. АН СССР 146 (1962), pp. 1007–1008.

[48] — — *Асимптотическое распределение целочисленных матриц третьего порядка*, Вестник Ленинград. ун-та 1964, № 13, pp. 25–36.

[49] В. П. Мякишев, *Распределение примитивных целых точек на некоторых конусах*, Докл. АН СССР 143 (1962), pp. 785–786.

[50] Б. Ф. Скубенко, *К асимптотике целочисленных матриц n-го порядка и об интегральном инварианте группы унимодулярных матриц*, Докл. АН СССР 153 (1963), pp. 290–291.

[51] — *К распределению целочисленных матриц и вычислению объема фундаментальной области унимодулярной группы матриц*, Труды МИАН 80 (1965), pp. 129–144.

[52] В. А. Тартаковский, *Die Gesamtheit der Zahlen, die durch eine positive quadratische Form* $F(x_1, x_2, \dots, x_s)$ ($s \geqslant 4$) *darstellbar sind. I–II*, Изв. АН СССР, отд. физ.-мат. наук, 1929, pp. 111–122, 165–196.

[53] M. Eichler, *Über die Idealklassenzahl hyperkomplexer Systeme*, Math. Zeitschr. 43 (1938), pp. 481–494.

[54] B. W. Jones, *The arithmetic theory of quadratic forms*, Baltimore 1950, X+197 pp.

[55] B. W. Jones and G. Pall, *Regular and semi-regular positive ternary quadratic forms*, Acta Math. 70 (1939), pp. 165–191.

[56] B. W. Jones and G. L. Watson, *On indefinite ternary quadratic forms*, Ca J. Math. 8 (1956), pp. 592–608.

[57] M. Kneser, *Klassenzahlen indefiniter quadratischer Formen in drei oder Veränderlichen*, Archiv der Math. 7 (1956), pp. 323–332.

[58] A. Meyer, *Ueber indefinite ternäre quadratische Formen*, J. Reine An Math. 113 (1894), pp. 186–206; 114 (1895), pp. 233–254; 115 (1895), pp. 150– 116 (1896), pp. 307–325.

[59] G. Pall, *Quaternions and sums of three squares*, Amer. J. Math. 64 (1 pp. 503–513.

[60] C. L. Siegel, *Über die Klassenzahl quadratischer Zahlkörper*, Acta Arit (1935), pp. 83–86.

[61] G. L. Watson, *A proof of the seven cube theorem*, J. London Math. So (1951), pp. 153–156.

[62] — *On sums of a square and five cubes*, J. London Math. Soc. (2), 5 (1 pp. 215–218.

Received on 28. 2. 1974

Les volumes VI et suivants sont à obtenir chez	Volumes from IV on are available at	Die Bände IV und folgende sind zu beziehen durch	Томы IV и следующие можно получить через

Ars Polona-Ruch, Krakowskie Przedmieście 7, 00-068 Warszawa

Les volumes I–III sont à obtenir chez	Volumes I–III are available at	Die Bände I–III sind zu beziehen durch	Томы I–III можно получить через

Johnson Reprint Corporation, 111 Fifth Ave., New York, N. Y.