MEAN-VALUE THEOREM FOR THE MODULUS OF MULTIPLE TRIGONOMETRIC SUMS

G. I. Arkhipov

UDC 511

A two-dimensional analog of the Vinogradov mean-value theorem for the modulus of trigonometric sums is proven.

The Vinogradov mean-value theorem is fundamental to this well-known method of trigonometric sums (see [1, 2, 4, 6, 7]). Similarly, our theorem is fundamental to the method of multiple trigonometric sums, which is a generalization of Vinogradov's method. For simplicity, we consider the case of double sums in which the summation variables are equivalent. The case of sums of higher multiplicity differs only in technical details. The theorem to be proven can be simplified and generalized somewhat by making the proof more complicated. The mean-value theorem will be proven by the p-adic method, using the procedure developed by Karatsuba (see [3, 5, 6]). The theorem yields estimates of multiple trigonometric Weyl sums and from them, using well-known procedures (see [1, 2]), we obtain theorems for the distribution of the fractions of a polynomial of several variables and some other results.

1. Formulation of the Theorem, Notation, and Auxiliary Assertions. We consider the set of pairs of integers (m, t) with the condition $0 \leq t \leq m \leq n$, where n is natural, $n > 4$. In all there will be $((n+1)\cdot(n+2)/2)-1$ such pairs. We number these pairs $0, 1, \ldots, ((n+1)(n+2)/2)-1$ setting $l = l(m, t) = (m(m+1)/2)+t$. Obviously, if l is the number of the pair (m, t), then m is the largest integer such that $m(m+1)/2 \leq l$, and $t = l-(m(m+1)/2)$.

THEOREM. Let K be natural and τ be a nonnegative integer, $K \geqslant 2n^3 + n^2\tau$; $N = n(n+3)/2$; $\alpha_0, \ldots \alpha_N$ are real numbers; A is the (N+1)-dimensional vector, $A = (\alpha_0, \ldots, \alpha_N)$;

$$f_A(x, y) = \sum_{m=0}^{n} \sum_{t=0}^{m} \alpha_l x^{m-t} y^t.$$

We set

$$S_P(A) = \sum_{\nu=1}^{P} \sum_{\mu=1}^{P_1} \exp(2\pi i f_A(x, y));$$
$$\nu = 1/n;\ \Delta(n, \tau) = (1-\nu)^\tau.$$

The symbol Ω denotes the (N+1)-dimensional unit cube. Then for $P \geqslant (2n)^{2n/\Delta(n,\tau)}$ we have the estimate

$$J_0(n, K, P) = \int_\Omega |S_P(A)|^{2K} dA \leqslant K^{2n^2\tau} \cdot 2^{3n^3\tau} P^{1K-(n(n+1)(n+2)/3)\cdot(1-\Delta(n,\tau))}$$

Let $Q > 0$. We set

$$S_Q(A) = \sum_{1 \leq x \leq Q} \sum_{1 \leqslant y \leqslant Q} \exp(2\pi i f_A(x, y)).$$

Furthermore, let $\Lambda = (\lambda_0, \ldots, \lambda_N)$ be the (N+1)-dimensional integral vector, and let $(A\cdot, \Lambda)$ be the scalar product of the vectors A and Λ.

V. A. Steklov Mathematics Institute, Academy of Sciences of the USSR. Translated from Matematicheskie Zametki, Vol. 17, No. 1, pp. 143-153, January, 1975. Original article submitted May 17, 1974.

We set

$$J(n, K, Q, \Lambda) = \int_{\Omega} |S_Q(A)|^{2K} \exp(-2\pi i (A\cdot, \Lambda))\, dA,$$
$$J_0(n, K, Q) = J(n, K, Q, 0).$$

We consider the system of equations

$$\sum_{k=1}^{2K} (-1)^k x_k^{m-t} y_k^t = \lambda_l, \qquad l = 0, 1, \ldots, N. \tag{1}$$

LEMMA 1. Let Δ be an arbitrary finite set of integral collections $\|(z_1, v_1), \ldots, (z_{2K}, v_{2K})\|$, and let $\varphi(\Lambda)$ be the number of solutions of system (1) belonging to the set Δ. Then

a) $\sum_{\Delta} \exp\left(2\pi i \sum_{k=1}^{2K} (-1)^k f_A(x_k, y_k)\right) = \sum_{\Lambda} \varphi(\Lambda) \exp(2\pi i (A\cdot, \Lambda))$,

where $\sum_{\Delta}$ denotes summation over the collections belonging to Δ and $\sum_{\Lambda}$ denotes summation over all the integral vectors Λ; by virtue of the finiteness of Δ the right-hand side a) contains a finite number of nonzero terms;

b) $\varphi(M) = \int_{\Omega} \sum_{\Delta} \exp\left(2\pi i \sum_{k=1}^{2K} f_A(x_k, y_k) - 2\pi i (A\cdot, \Lambda)\right) dA$;

c) J(n, K, Q, Λ) equals the number of solutions of (1) under the condition that $1 \leq x_k, y_k \leq Q$, k = 1, 2, ..., 2K;

d) $|S_Q(A)|^{2K} = \sum_{\Lambda} J(n, K, Q, \Lambda) \exp(2\pi i (A\cdot, \Lambda))$.

The proof is similar to the proof of Lemma 1 in [6].

Moreover, we have trivially

$$|S_Q(A)| \leqslant Q^2; \quad I(n, K, Q, \Lambda) \leqslant I_0(n, K, Q) \leqslant Q^{2K_1} \cdot I_0(n, K - K_1, Q) \leqslant Q^{2K},$$

where $0 \leqslant K_1 \leqslant K$; $I(n, K, Q_1, \Lambda) \leqslant I(n, K, Q_2, \Lambda)$, if $Q_1 \leqslant Q_2$; $I(n, K, Q, \Lambda) = I(n, K, [Q], \Lambda)$, where [Q] is the integer part of Q.

Let K_1 be an arbitrary natural number. Say that the matrix $H = \|h_{l,k}\|$ having an N + 1 row and a K_1 column, corresponds to the collection of pairs of integers of unknowns $\|z_k, v_k\|$, where k = 1, 2, ..., K_1, if $h_{l,k} = z_k^{m-t} v_k^t$, where the number of the row is l = 0, 1, ..., N and the number of the column is k = 1, 2, ..., K_1. The matrix corresponding to $\|x_k, y_k\|$, k = 1, 2, ..., 2K, the collection of unknowns in (1), is represented by D and its elements by $d_{l,k}$. The symbol E denotes the 2k-dimensional vector $E = \|(-1)^k\|$, k = 1, 2, ..., 2K. Then system (1) can be written in the form of the matrix equality $D \cdot E = \Lambda$. It then follows in particular that $J_0(n, K, Q)$ expresses the number of solutions of the system $D \cdot E = 0$ under the condition that $1 \leq x_k, y_k \leq Q$, k = 1, ..., 2K.

$D(a, b) = \|d_{l,k}(a, b)\|$ denotes the matrix corresponding to the collection $\|x_k + a, y_k + b\|$, k = 1, 2, ..., K_1. Then for $K_1 = 2K$ we have D(0, 0) = D.

LEMMA 2. $D(a + a_1, b + b_1) = G(a, b) \cdot D(a_1, b_1)$, where G(a, b) is a square matrix of order N + 1, and $G(a, b) = \|g_{l,k}(a, b)\|$, where the number of the row l and the number of the column k take the values 0, 1, ..., N; if $l \leq k \leq N$, then $g_{l,k}(a, b) = 0$ and if $0 \leq k \leq l$, then $g_{l,k}(a, b) = \binom{m-t}{m_1}\binom{t}{t_1} a^{m_1} b^{t_1}$, where $0 \leq m_1 \leq m-t$, $0 \leq t_1 \leq t$, and the numbers m_1, t_1 are determined uniquely with respect to k from the relation (see the beginning of Sec. 1): $k = ((m-m_1-t_1)(m-m_1-t_1+1)/2) + t - t_1$.

Proof. We multiply the matrices G(a, b) and D(a_1, b_1) according to the usual rules.

COROLLARIES of LEMMA 2. a) The matrices D(a, b) and D(0, 0) have the same rank in $\mathbf{Z}_p$ — the field of residues of the prime modulus p.

Proof. According to Lemma 2, $D(a, b) = G(a, b) \cdot D(0, 0)$, $D(0, 0) = G(-a, -b)D(a, b)$; this is a confirmation of a) since the rank of the matrix product is not higher than the rank of any of the cofactors.

b) From the equality $D(a, b) \cdot E = 0$ it follows that $D(0, 0) \cdot E = 0$ and vice versa.

Proof. It is sufficient to multiply the matrix equalities of a) by the vector E on the right.

2. First Fundamental Lemma (an analog of Linnik's theorem – see [4]). T(W) denotes the number of solutions of the system of congruences in the ring of residues in mod p^n (p is a prime):

$$(W)\ \sum_{k=1}^{2n^2}(-1)^k z_k^{m-t} v_k^t \equiv \lambda_l \pmod{p^m},$$

where λ_l are fixed integers, $l = 0, 1, \ldots, N$, z_k, v_k are unknowns, $k = 1, 2, \ldots, 2n^2$, and the rows of the matrix $B = \| b_{l,k} \|$, $b_{l,k} = z_k^{m-t} v_k^t$, $l = 0, 1, \ldots, N$, $k = 1, 2, \ldots, 2n^2$, i.e., B corresponds to the collection $\| z_k, v_k \|$, are linearly independent in $\mathbf{Z}_p$. Then we have the

FIRST FUNDAMENTAL LEMMA.

$$T(W) \leqslant n^{2n^2} p^{4n^2 - n(n+1)(n+2)/3}$$

Proof. Without loss of generality we can assume that $0 \leq z_k, v_k \leq p^n - 1$ for all k, and also that $p > n$ (otherwise, the rank of B is always smaller than $N + 1$; therefore $T(W) = 0$). Furthermore, let

$$z_k = \sum_{r=1}^{n} x_{k,r} p^{r-1}, \qquad v_k = \sum_{r=1}^{n} y_{k,r} p^{r-1},$$

and $0 \leq x_{k,r}, y_{k,r} \leq p-1$ for all k and r. For $s = 1, 2, \ldots, n$ we set

$$z_{k,s} = \sum_{r=1}^{s} x_{k,r} p^{r-1}, \qquad v_{k,s} = \sum_{r=1}^{s} y_{k,r} p^{r-1}.$$

We consider the system

$$(W_s)\ \sum_{k=1}^{2n^2}(-1)^k z_{k,s}^{m-t} v_{k,s}^t \equiv \lambda_l \pmod{p^{u_{l,s}}},$$

where $j = 1, 2, \ldots, N$, $u_{l,s} = m$, if $1 \leq l \leq s(s+3)/2$, i.e., $m \leq s$; if $s(s+3)/2 < l$, i.e., $m > s$, then $u_{l,s} = s$; moreover, the rows of the matrix B_s, which corresponds to the collection $\| z_{k,s} v_{k,s} \|$, $k = 1, 2, \ldots, 2n^2$, are linearly independent in $\mathbf{Z}_p$. Let $T(W_s)$ be the number of solutions of the system W_s. Note that the systems W_n and W are equivalent (we assume that $\lambda_0 = 0$); therefore $T(W_n) = T(W)$. Furthermore, from the definitions of $z_{k,s}$, $v_{k,s}$ we have

$$z_{k,s}^{m-t} v_{k,s}^t \equiv z_{k,s-1}^{m-t} v_{k,s-1}^t + p^{s-1}((m-t) z_{k,s-1}^{m-t-1} v_{k,s-1}^t x_{k,s} + t z_{k,s-1}^{m-t} y_{k,s}) \pmod{p^s}.$$

Since $u_{l,s} \leq s$, the system W_s can be rewritten ($l = 1, \ldots, N$ the rank of $B_s = N + 1$)

$$\sum_{k=1}^{2n^2}(-1)^k z_{k,s-1}^{m-t} v_{k,s-1}^t \equiv p^{s-1} \sum_{k=1}^{2n^2}(-1)^k ((m-t) z_{k,s-1}^{m-t-1} v_{k,s-1}^t x_{k,s} + t z_{k,s-1}^{m-t} v_{k,s-1}^{t-1} y_{k,s}) + \lambda_l \pmod{p^{u_{l,s}}}. \tag{1}$$

Obviously, $u_{l,s} \equiv \min(s-1, u_{l,s})$ and for all s the matrices B_s have the same rank. Therefore, (1) implies that $z_{k,s-1}$, $v_{k,s-1}$ satisfy the system W_{s-1}.

We take some solution of W_{s-1}. Then it follows from (1) that for suitable μ_l we have the following relations for the unknowns:

$$\sum_{k=1}^{2n^2}(-1)^k ((m-t) z_{k,s-1}^{m-t-1} v_{k,s-1}^t x_{k,s} + t z_{k,s-1}^{m-t} v_{k,s-1}^t y_{k,s}) \equiv \mu_l \pmod{p}. \tag{2}$$

The relations (2) form a system of $N + 1 - (s(s+1)/2)$ linear congruences with respect to the unknowns $x_{k,s}$, $y_{k,s}$, $k = 1, \ldots, 2n^2$. Let T_s be the number of solutions of this system. Then $T(W_s) = T_s \cdot T(W_{s-1})$. We estimate T_s. We consider those congruences (2) for which $t = 0$. The same applies to congruences with subscripts l equal to $s(s+1)/2$, $(s+1)(s+2)/2$, $\ldots$, $n(n+1)/2$. They form a system of $n - s - 1$ linear congruences with respect to the unknowns $x_{k,s}$:

$$\sum_{k=1}^{2n^2}(-1)^2 m z_{k,\,s-1}^{m-1} x_{k,\,s} \equiv \mu_l \pmod p. \tag{3}$$

We compare the row with number $l = m(m+1)/2$ and the column with number k of the matrix of the coefficients of this system H_1 to the row with number $l_1 = m(m-1)/2$ and the column with number k in the matrix B_{s-1}. We see that the indicated rows and columns of these matrices differ in the nonzero coefficients in Z_p (since $p > n$). Therefore, the rows of H_1 are linearly independent in Z_p and it then follows that the number of solutions of (3) does not exceed $p^{2n^2-n+s+1}$.

We now take some solution of (3). Then (2) transforms into a system of $N+1-(s(s+1)/2)-n+s+1$ linear congruences with respect to the unknowns $y_{k,s}$. As above, the linear independence of the rows of the matrix of the coefficients of this system H_2 is established (in this case the row of H_2 with number $l = (m(m+1)/2)+t$ must be compared to the row of B_{s-1} with number $l_1 = (m(m-1)/2)+t-1$). We then find that the number of solutions of the latter system does not exceed $p^{2n^2-N-1+(s(s+1),2)+n-s-1}$. Consequently, $T_s \leqslant p^{4n^2-N-1+(s(s+1),2)}$, from which $T(W) = T_n \cdot T_{n-1} \cdots T_2 \cdot T(W_1)$,

$$T(W) \leqslant p^{4n^3-(n-1)(n+1)(n+2),3} \cdot T(W_1). \tag{4}$$

We estimate $T(W_1)$. It is clear that

$$T(W_1) \leqslant p^{-N} \sum_{a_1=0}^{p-1} \cdots \sum_{a_N=0}^{p-1} |S_p(A)|^{2n^2},$$

where

$$S_p(A) = \sum_{x=1}^{p} \sum_{y=1}^{p} \exp(2\pi i f_A(x, y)),$$
$$A = (0, a_1/p, a_2/p, \ldots, a_N/p).$$

From which

$$T(W_1) \leqslant p^{-N} |S_p(0)|^{2n^2} + p^{-N} \sum_{A}' |S_p(A)|^{2n^2},$$

where Σ_A' means that the summation is over all A for which $0 \leqslant a_l \leqslant p-1$, $l = 1, \ldots, N$ and $A \neq 0$. Furthermore, $|S_p(0)|^{2n^2} = p^{4n^2}$. We estimate $S_p(A)$ for $A \neq 0$. We find $f_t(x)$ for $t = 0, \ldots, n$

$$p f_A(x, y) = \sum_{t=0}^{n} f_t(x) y^t;$$

the degree of the polynomial $f_t(x)$ is not higher than $n-t$. Let m be the maximum value of t for which $f_t(x)$ is not congruent to zero in mod p identically. Using Weil's estimate (see [8],

$$\left|\sum_{k=0}^{p} \exp(2\pi i g(k)/p)\right| \leqslant (d-1)\sqrt{p},$$

where g(k) is a polynomial of degree d with integer coefficients and is not congruent to zero in mod p identically, we obtain

$$|S_p(A)| \leqslant \sum_{x,\, f_m(x) \equiv 0\,(p)} \left|\sum_{y=0}^{p-1} \exp(2\pi i f_A(x, y))\right| +$$

$$+ \sum_{x,\, f_m(x) \not\equiv 0\,(p)} \left|\sum_{y=1}^{p} \exp(2\pi i f_A(x, y))\right| \leqslant (n-m)p + p(m-1)p^{1/2} \leqslant np^{3/2}.$$

Consequently, $T(W_1) \leqslant n^{2n^2} p^{4n^2-N}$, which instead of (4) gives a confirmation of the lemma.

3. Second Fundamental Lemma (see [6] and [7]). Let p be prime, $(2/3)Q^{\nu} \leq p \leq Q^{\nu}$, $p \geq n^2$, $Q_0 = (Q/p)+1$. Then the following is true:

SECOND FUNDAMENTAL LEMMA.

$$J_0(n, K, Q) \leqslant K^{2n^2} \cdot 2^{3n^3-1} \cdot Q^{4K-4n^2+1n^3-n(n+1)(n+2),3} J_0(n, K, n^2, Q_0).$$

Proof. Let $Q_1 = Q$ if Q is an integer divisible by p, and let $Q_1 = p([Q/p] + 1)$ otherwise. Then $J_0(n, K, Q) \le J_0(n, K, Q_1)$. We estimate $J_0(n, K, Q_1)$.

Let $D_1 = \| d_{l,k} \|$, $l = 0, 1, \ldots, N$; $k = 1, 3, \ldots, 2K-1$; $D_2 = \| d_{l,k} \|$, $l = 0, 1, \ldots, N$; $k = 2, 4, \ldots, 2K$, and, as before, $d_{l,k} = x_k^{m-t} y_k^t$. Every solution of the system

$$D \cdot E = 0, \quad 1 \leqslant x_k, \; y_k \leqslant Q_1, \; k = 1, \ldots, 2K,$$

generates its matrices D_1 and D_2. If for some solution the rows of each of the matrices are linearly independent in Z_p then this solution refers to the first class; all other solutions refer to the second class. Let J_1 be the number of solutions of the first class and J_2 be the number of solutions of the second. Then $J_0(n, K, Q_1) = J_1 + J_2$. We estimate J_2. Henceforth, we assume that x_k, y_k, q_k, r_k, z_k, v_k, q, r satisfy the following conditions (k = 1, 2, ..., 2K): $x_k = q_k + pz_k$, $y_k = r_k + pv_k$, $1 \le q_k, r_k, q, r \le p$.

Furthermore, let

$$Q_2 = Q_1/p, \; S(q, r) = \sum_{z=0}^{Q_2-1} \sum_{v=0}^{Q_2-1} \exp(2\pi i f_A(q + pz, r + pv)).$$

Let J_3 be the number of such solutions of system II for which the rows of D_2 are linearly independent. Linear independence means the existence in Z_p of the (N+1)-dimensional vector $C = \| c_l \|$, $l = 0, \ldots, N$ such that $C + D_2 = 0$ in Z_p. Let $F_C(x, y) = \sum_{l=0}^{N} c_l x^{m-l} y^l$. The equality $C \cdot D_2 = 0$ means that

$$F_c(x_k, y_k) \equiv 0 \pmod{p} \text{ for } k = 2, 4, \ldots, 2K. \tag{5}$$

We take some vector $C \neq 0$ in Z_p. Let $J_4(C)$ be the number of solutions which satisfy the relations (5) for a given C. Then

$$J_4(C) = \int_\Omega \sum_1 \cdot \sum_2 dA,$$

where

$$\sum_1 = \Big(\sum_{x, y, 1 \leqslant x, y \leqslant p, F_C(x, y) \equiv 0(p)} S(x, y) \Big)^K,$$
$$\sum_2 = \Big(\sum_{x=1}^{p} \sum_{y=1}^{p} \overline{S(x, y)} \Big)^K.$$

Since $C \neq 0$ in Z_p the number of solutions of the congruence $F_C(x, y) \equiv 0(p)$ does not exceed np. Therefore, using the Hölder inequality, we obtain

$$J_4(C) \leqslant n^{K-1} p^{3K-1} \sum_{q=1}^{p} \sum_{r=1}^{p} \int_\Omega |S(q, r)|^{2K} dA.$$

Using Corollary (b) of Lemma 2, we find that

$$\int_\Omega |S(q, r)|^{2K} dA = J_0(n, K, Q_2),$$

from which, summing over all $C \neq 0$ in Z_p we obtain

$$J_3 \leqslant n^{K-1} p^{N+3K+2} \; Q_2^{4n^2} \cdot J_0(n, K - n^2, Q_2),$$

and since analysis of the case of the linear dependence of the rows of D_1 is exactly the same, then $J_2 \le 2J_3$

$$J_2 \leqslant n^K p^{N+3K+2} \; Q^{4n^2} \cdot J_0(n, K - n^2, Q_2). \tag{6}$$

We estimate J_1. The collection $\| a_k, b_k \|$, k = 1, 2, ..., K_1, $K_1 > N$ is called proper if the rows of the matrix corresponding to the collection $\| a_k, b_k \|$, k = 1, 2, ..., N+1 are linearly independent in Z_p. The collection $\| a_k, b_k \|$, k = 1, 2, ..., $2K_1$ is called singular if each of the two collections $\| a_k, b_k \|$, k = 1, 3, 5, ..., $2K_1-1$ and $\| a_k, b_k \|$, k = 2, 4, ..., $2K_1$ are proper. The solution of a system of equations (congruences) which is a singular collection will also be called singular. Obviously

$$J_1 \leqslant (C_{K+1}^{N+1})^2 \cdot J_5,$$

where

$$J_5 = \int_\Omega S_1 \cdot S_2 \, dA, \; S_2 = \left| \sum_{q=1}^{p} \sum_{r=1}^{p} S(q, r) \right|^{2K-2n^2},$$

$$S_1 = \sum_{\substack{1 \leqslant q_k, r_k \leqslant p \\ k=1, 2, \ldots, n^2}}' \prod_{k=1}^{n^2} |S(q_k, r_k)|^2,$$

and the symbol Σ' means that averaging is only over proper collections. Using Hölder's inequality, we obtain $J_5 \leqslant p^{4K-4n^2-2} \cdot J_6$, where

$$J_6 = \int_\Omega S_1 \sum_{l=1}^{p} \sum_{r=1}^{p} |S(q, r)|^{2K-2n^2} dA.$$

Using Corollary (b) of Lemma 2, we find that J_6 is the number of singular solutions of the system ($l = 0, 1, \ldots, N$):

$$\sum_{k=1}^{2n^2} (-1)^k (x_k - q)^{m-t} (y_k - r)^t + \sum_{k=2n^2+1}^{2K} (-1)^k p^m z_k^{m-t} v_k^t = 0.$$

From which we conclude that

$$J_6 = \Sigma_\Lambda J_7(\Lambda) \cdot J(n, K - n^2, Q_2, \Lambda),$$

where Σ_Λ denotes averaging over all the integral (N + 1)-dimensional vectors, and $J_7(\Lambda)$ is the number of singular solutions of the system of equations (for fixed Λ and the unknowns q, r, x_k, y_k):

$$\sum_{k=1}^{2n^2} (-1)^k (x_k - q)^{m-t} (y_k - r)^t = \lambda_l p^m, \qquad l = 0, 1, \ldots, N.$$

Since $J(n, K-n^2, Q_2, \Lambda) \leq J_0(n, K-n^2, Q_2)$, then

$$J_6 \leqslant J_0(n, K - n^2, Q_2) \cdot \Sigma_\Lambda \cdot J_7(\Lambda).$$

But the value of $J_7(\Lambda)$ equals the number of singular solutions of the system of congruences ($l = 0, 1, \ldots, N$):

$$\sum_{k=1}^{2n^2} (-1)^k (x_k - q)^{m-t} (y_k - r)^t \equiv 0 \pmod{p^m}. \tag{7}$$

We take arbitrary q, r. Each of the other unknowns in (7) takes any preassigned value in mod p^n not more than $(Q_1/p^n) + 1$ times. For the singular solution, the rows of B, which was considered in the first fundamental lemma, are linearly independent in $\mathbf{Z}_p$ since by virtue of Corollary (a) of Lemma 2, the matrices corresponding to the collections $\| x_k, y_k \|$ and $\| x_k - q, y_k - r \|$, k = 1, 2, ..., $2n^2$ have the same rank in $\mathbf{Z}_p$. Therefore, we use the first fundamental lemma to obtain

$$J_6 \leqslant p^2 ((Q_1/p^n) + 1)^{4n^2} \cdot T(W) \cdot J_0(n, K - n^2, Q_2),$$

and $T(W) \leqslant n^{2n^2} p^{4n^3 - n(n+1)(n+2)/3}$. Recalling the conditions applied to n and p and (6), we then prove the second fundamental lemma by means of trivial transformations.

4. Proof of the Theorem. When $\tau = 0$, the theorem is trivial. Let the theorem be valid for $\tau = m$ and let its conditions be satisfied for $\tau = m + 1$. Since in this case

$$P \geqslant (2n)^{2n^2 \Delta(n, m+1)} \geqslant (2n)^{2n}, \quad \text{то} \quad P^\nu > (2n)^2 > 64,$$

therefore there exists a prime p such that $(2/3)\, P^\nu \leq p \leq P^\nu$, $p \geq n^2$ and $kJ_0(n, K, P)$ can be applied to the second fundamental lemma. Consequently,

$$J_0(n, K, P) \leqslant K^{2n^2} 2^{3n^3-1} p^{4K-4n^2+4n^3-n(n+1)(n+2)/3} J_0(n, K - n^2, P_0),$$

where $P_0 = [P/p] + 1$. Furthermore, $P_0 > P^{1-\nu} > (2n)^{2n^2 \Delta(n, m)}$, $K - n^2 \geqslant 2n^3 + mn^2$. Therefore the theorem is applicable to $J_0(n, K-n^2, P_0)$ and $\tau = m$. Then

$$J_0(n, K, P) \leqslant K^{2n^2(m+1)} 2^{3n^2m} 2^{3n^2-1} (1 + (p/P))^{4K} p^{4K-4n^2-(n(n+1)(n+2)/3)+b} p^{4n^2-b},$$

where $b = (n(n+1)(n+2)/3)\Delta(n, m)$,

$$J_0(n, K, P) \leqslant K^{2n^2(m+1)} \cdot 2^{3n^2(m+1)} \cdot P^{4K-(n(n+1)(n+2)/3)(1-\Delta(n, m+1))}, \tag{8}$$

since $(1 + (p/P))^{4k} < 2$ or otherwise the theorem is trivial. Inequality (8) implies that the theorem is true for $\tau = m + 1$ and therefore it is true for all natural τ. The proof is concluded.

The author expresses his gratitude fo Prof. A. A. Karatsuba for guidance and Prof. S. B. Stechkin for careful consideration of the paper and useful advice.

LITERATURE CITED

1. I. M. Vinogradov, Method of Trigonometric Sums in Number Theory [in Russian], Moscow (1971).
2. I. M. Vinogradov, Selected Works [in Russian], Moscow (1952).
3. A. A. Karatsuba, "Waring problem for a congruence in a modulus equal to the degree of a prime number," Vestn. Mosk. Univ. Ser. Mat., 1, 28 (1962).
4. Yu. V. Linnik, "New estimates of Weyl sums," Dokl. Akad. Nauk SSSR, 34, 201 (1942).
5. A. A. Karatsuba, "Mean-value theorem and complete trigonometric sums," Izv. Akad. Nauk SSSR, Ser. Mat., 30, 183 (1966).
6. A. A. Karatsuba, "Mean value of the modulus of a trigonometric sum," Izv. Akad. Nauk SSSR, Ser. Mat., 37, 1203 (1973).
7. K. Chandrasekharan, Arithmetical Functions, Springer, Berlin (1970).
8. A. Weyl, "On some exponential sums," Proc. Natl. Acad. Sci. USA, 34, 204 (1948).