A. A. KARATSUBA, N. M. KOROBOV

1963

SovietRxiv

Abstract

Full Text

A. A. KARATSUBA, N. M. KOROBOV

ON A MEAN-VALUE THEOREM

(Presented by Academician A. N. Kolmogorov, 12 X 1962)

Let $N_k(P) = N_k^{(P)}(0, \dots, 0)$ and $N_k^{(P)}(\lambda_1, \dots, \lambda_n)$ be the number of solutions of the system of equations

$$x_1^\nu + \cdots + x_k^\nu = y_1^\nu + \cdots + y_k^\nu + \lambda_\nu, \qquad 0 \le x, y \le P-1 \quad (\nu = 1, 2, \dots, n), \quad (1)$$

where $\lambda_1, \dots, \lambda_n$ are arbitrary fixed integers.

In the present note a new proof is given of Vinogradov' s mean-value theorem (see [1,2,5]), which makes it possible to improve the factor depending on n in the estimate for the number of solutions of the system (1). This in turn makes it possible to improve somewhat the estimates of Weyl sums obtained in [1,4]. In its main idea this work is close to [3].

Lemma. Suppose $m \ge 1$, $\mu_1, \dots, \mu_n$ are integers, $p > n$ is prime, and T is the number of solutions of the system of congruences

$$\left.\begin{aligned} x_1 + \cdots + x_n &\equiv \mu_1 \pmod p, \\ &\cdots\cdots\cdots \\ x_1^n + \cdots + x_n^n &\equiv \mu_n \pmod{p^n}, \end{aligned}\right\} \qquad 0 \le x_j \le mp^n - 1$$

$$(j = 1, 2, \dots, n),$$

where for $i \ne j$ the condition $x_i \not\equiv x_j \pmod p$ is satisfied. Then the estimate

$$T \le n!\, m^n p^{n(n-1)/2}$$

is valid.

Proof. Write the quantities x_j in the form

$$x_j = x_{j1} + p x_{j2} + \cdots + p^{n-1} x_{jn} + p^n x_{jn+1} \qquad (j = 1, 2, \dots, n),$$

where $0 \le x_{j\nu} \le p-1$ $(\nu = 1, 2, \dots, n)$ and $0 \le x_{jn+1} \le m-1$. Note that, according to the additional condition stated in the lemma, for $i \ne j$ we have

$x_{i1} \neq x_{j1}$. It is easy to see that the quantities $x_{11}, \dots, x_{n1}$ satisfy the system of congruences

$$\left.\begin{aligned} x_{11} + \cdots + x_{n1} &\equiv \mu_1 \\ \cdots\cdots\cdots & \\ x_{11}^n + \cdots + x_{n1}^n &\equiv \mu_n \end{aligned}\right\} \pmod{p}.$$

Denote by T_1 the number of solutions of this system. Obviously, $T_1 \leq n!$. Fix one such solution and pass from the original system of congruences to congruences modulo p^2. Then we obtain

$$\left.\begin{aligned} (x_{11} + px_{12})^2 + \cdots + (x_{n1} + px_{n2})^2 &\equiv \mu_2 \\ \cdots\cdots\cdots & \\ (x_{11} + px_{12})^n + \cdots + (x_{n1} + px_{n2})^n &\equiv \mu_n \end{aligned}\right\} \pmod{p^2}.$$

Hence, after obvious transformations, we obtain a system of $n-1$ linear congruences in $x_{12}, \dots, x_{n2}$:

$$\left.\begin{aligned} x_{11}x_{12} + \cdots + x_{n1}x_{n2} &\equiv \mu_2', \\ x_{11}^{n-1}x_{12} + \cdots + x_{n1}^{n-1}x_{n2} &\equiv \mu_n' \end{aligned}\right\} \pmod{p}. \tag{2}$$

Since the quantities $x_{11}, \dots, x_{n1}$ are distinct, at least $n-1$ of them are nonzero. For definiteness we shall assume that the quantities $x_{11}, \dots, x_{n-1,1}$ are nonzero. Then, obviously,

$$\begin{vmatrix} x_{11} & \dots & x_{n-1,1} \\ \cdot & \cdot & \cdot \\ x_{11}^{n-1} & \dots & x_{n-1,1}^{n-1} \end{vmatrix} = x_{11} \cdots x_{n-1,1} \prod_{1 \leq i < j \leq n-1} (x_{i1} - x_{j1}) \not\equiv 0 \pmod{p},$$

and, consequently, for any fixed value of x_{n2}, the quantities $x_{12}, \dots, x_{n-1,2}$ are determined uniquely from the system (2). Thus, denoting by T_2 the number of solutions of this system, we obtain $T_2 = p$.

Next, considering congruences modulo p^3, we obtain a system of $n-2$ linear congruences with respect to $x_{13}, \dots, x_{n3}$; the number of solutions of such a system is $T_3 = p^2$. Similarly we obtain $T_4 = p^3, \dots, T_n = p^{n-1}$ and $T_{n+1} = m^n$. Hence, since $T \leq T_1 \cdots T_{n+1}$, the assertion of the lemma follows:

$$T \leq n!\, p^{1+2+\cdots+n-1} m^n = n!\, m^n p^{n(n-1)/2}.$$

Now let $n \geq 2$, $P \geq (2n)^{2n(1+1/(n-1))^\tau}$, $0 < \theta \leq 1$, and $P_0 = P$. Define, for $\nu = 1, 2, \dots, \tau$, the integers P_ν and primes p_ν by means of the relations

$$\frac{1}{1+\theta}P_{\nu-1}^{1/n} \le p_\nu \le P_{\nu-1}^{1/n}, \qquad P_\nu = [P_{\nu-1}p_\nu^{-1}] + 1. \tag{3}$$

It is easy to show that under these conditions the estimates

$$n^2 < p_\nu, \qquad P_{\nu-1} < p_\nu P_\nu, \qquad P_\nu < (1+2\theta)^n P^{(1-1/n)^\nu}. \tag{4}$$

also hold. We also note that the quantity θ is chosen so that in each of the intervals (3) there is a prime number.

Theorem 1. If $\tau \ge 1$, $k \ge n^2 + n\tau$, then the estimate

$$N_k(P) < (3k^{2n})^\tau (1+2\theta)^{2k(n+\tau)} P^{2k-n(n+1)/2+n(n+1)/2(1-1/n)^\tau}.$$

holds.

Proof. By definition, $P = P_0 \le p_1 P_1$, and, consequently, $N_k(P) \le N_k(p_1 P_1)$, where $N_k(p_1 P_1)$ is the number of solutions of the system of equations (1) with $\lambda_1 = \cdots = \lambda_n = 0$:

$$(x_1+p_1z_1)^\nu+\cdots+(x_k+p_1z_k)^\nu = (y_1+p_1t_1)^\nu+\cdots+(y_k+p_1t_k)^\nu \qquad (\nu = 1, 2, \dots, n), \tag{5}$$

$$0 \le x_j,\ y_j \le p_1 - 1, \qquad 0 \le z_j,\ t_j \le P_1 - 1.$$

We shall assign the system $x_1, \dots, x_k$ to the first class if in it one can find n distinct quantities x_j. All the remaining systems $x_1, \dots, x_k$ will be assigned to the second class. Obviously,

$$N_k(p_1P_1) = N_k^{(1)} + N_k^{(2)},$$

where $N_k^{(1)}$ is the number of solutions of the system (5) for which $x_1, \dots, x_k$ and $y_1, \dots, y_k$ belong to the first class, while $N_k^{(2)}$ is the number of solutions of the system (5) for which $x_1, \dots, x_k$ or $y_1, \dots, y_k$ belong to the second class.

Introduce, for systems with distinct $x_1, \dots, x_n$ and arbitrary $x_{n+1}, \dots, x_k$, the notation $(x_1, \dots, x_n)x_{n+1}, \dots, x_k$. We shall call permutations of these systems such systems in which the distinct x_j stand no longer in the first n places, but in arbitrary places.

It is easy to see that every system of the first class occurs among the permutations of systems of the form $(x_1, \dots, x_n)x_{n+1}, \dots, x_k$. Consequently, the quantity $N_k^{(1)}$ does not exceed the number of solutions of the system (5) with variables of the form

$$(x_1, \dots, x_n)x_{n+1}, \dots, x_k, \quad (y_1, \dots, y_n)y_{n+1}, \dots, y_k,$$

multiplied by $(C_k^n)^2$.

But then, using the notation

$$S(x) = \sum_{z=0}^{p_1-1} e^{2\pi i f(x+p_1 z)}, \qquad f(x) = \alpha_1 x + \dots + \alpha_n x^n,$$

we obtain

$$N_k^{(1)} \le (C_k^n)^2 \int_0^1 \dots \int_0^1 \left| \sum_{\substack{(x_1,\dots,x_n) \\ x_{n+1},\dots,x_k}} S(x_1) \cdots S(x_k) \right|^2 d\alpha_1 \cdots d\alpha_n \le$$

$$\le (C_k^n)^2 p_1^{2k-2n-1} \int_0^1 \dots \int_0^1 \left| \sum_{(x_1,\dots,x_n)} S(x_1) \cdots S(x_n) \right|^2 \sum_{x=0}^{p_1-1} |S(x)|^{2k-2n} \, d\alpha_1 \cdots d\alpha_n.$$

The integral appearing on the right-hand side of this inequality is, obviously, equal to the number of solutions of the system

$$(x_1 + p_1 z_1)^\nu + \dots - (y_n + p_1 t_n)^\nu = (x + p_1 z_{n+1})^\nu + \dots - (x + p_1 t_k)^\nu$$

$$(\nu = 1, 2, \dots, n),$$

or, equivalently, to the number of solutions of the system

$$(x_1 - x + p_1 z_1)^\nu + \dots - (y_n - x + p_1 t_n)^\nu = p_1^\nu (z_{n+1}^\nu + \dots - t_k^\nu) \tag{6}$$

$$(\nu = 1, 2, \dots, n),$$

where $0 \le x, x_j, y_j \le p_1 - 1$, $0 \le z_j, t_j \le P_1 - 1$, and for $i \ne j$ the condition $x_i \ne x_j$ is satisfied. Under the same conditions for the range of variation of the unknowns, let us also consider the system of equations

$$(x_1 - x + p_1 z_1)^\nu + \dots - (y_n - x + p_1 t_n)^\nu = \lambda_\nu p_1^\nu \qquad (\nu = 1, 2, \dots, n), \tag{7}$$

where $\lambda_1, \dots, \lambda_n$ are arbitrary fixed integers, and the system of congruences

$$(x_1 - x + p_1 z_1)^\nu + \cdots - (y_n - x + p_1 t_n)^\nu \equiv 0 \pmod{p_1^\nu} \qquad (\nu = 1, 2, \ldots, n). \quad (8)$$

Denoting respectively by N'_k, $N'_n(\lambda_1 p_1, \ldots, \lambda_n p_1^n)$, and T' the numbers of solutions of the systems (6), (7), and (8), we obtain

$$N'_k = \sum_{\lambda_1, \ldots, \lambda_n} N'_n(\lambda_1 p_1, \ldots, \lambda_n p_1^n)\, N_{k-n}^{(P_1)}(\lambda_1, \ldots, \lambda_n) \leq$$

$$\leq N_{k-n}(P_1) \sum_{\lambda_1, \ldots, \lambda_n} N'_n(\lambda_1 p_1, \ldots, \lambda_n p_1^n) = T' N_{k-n}(P_1) \, *.$$

Finally, choosing in the lemma $m = [P_1 p_1^{-n+1}] + 1$, we obtain

$$T' \leq p_1 (p_1 P_1)^n n! ([P_1 p_1^{-n+1}] + 1)^n p_1^{n(n-1)/2} \leq n! 2^n P_1^{2n} p_1^{-n(n+1)/2 + 2n + 1},$$

$$N_k^{(1)} \leq (C_k^n)^2 p_1^{2k-2n-1} N'_k \leq 2k^{2n} P_1^{2n} p_1^{2k - n(n+1)/2} N_{k-n}(P_1). \qquad (9)$$

Let us now estimate the quantity $N_k^{(2)}$. Obviously,

$$N_k^{(2)} = \int_0^1 \cdots \int_0^1 \left[\sum_{x_1, \ldots, y_k} S(x_1) \cdots S(y_k) \right] d\alpha_1 \cdots d\alpha_n,$$

* The sum $\sum_{\lambda_1, \ldots, \lambda_n}$ is extended over the region $|\lambda_1| \leq k P_1, \ldots, |\lambda_n| \leq k P_1^n$.

where the quantities $x_1, \ldots, y_k$ vary in such a way that at least one of the systems $x_1, \ldots, x_k;\ y_1, \ldots, y_k$ belongs to the second class. Noting that the number of systems of the second class does not exceed $n^k p_1^{n-1}$, we obtain

$$\sum_{x_1, \ldots, y_k} S(x_1) \cdots \overline{S(y_k)} \ll n^k p_1^{k+n-1} \sum_{x=0}^{p_1 - 1} |S(x)|^{2k} \ll n^k P_1^{2n} p_1^{k+n-1} \sum_{x=0}^{p_1 - 1} |S(x)|^{2k-2n},$$

$$N_k^{(2)} \ll n^k P_1^{2n} p_1^{k+n-1} \int_0^1 \cdots \int_0^1 \sum_{x=0}^{p_1 - 1} |S(x)|^{2k-2n} \, d\alpha_1 \cdots d\alpha_n = n^k P_1^{2n} p_1^{k+n} N_{k-n}(P_1).$$

Since $n < p_1^{1/2}$ and $k \geq n^2 + n$, we have $n^k p_1^{k+n} \ll n^{2n} p_1^{2k-n(n+1)/2}$, and consequently

$$N_k^{(2)} \ll n^{2n} P_1^{2n} p_1^{2k-n(n+1)/2} N_{k-n}(P_1).$$

Hence, by virtue of (9), it follows that

$$N_k(P) \ll N_k^{(1)} + N_k^{(2)} \ll 3k^{2n} P_1^{2n} p_1^{2k-n(n+1)/2} N_{k-n}(P_1).$$

Applying this inequality τ times, we obtain

$$N_k(P) \ll (3k^{2n})^\tau (P_1 \cdots P_\tau)^{2n} (p_1 \cdots p_\tau)^{2k-n(n+1)/2} (p_2 p_3^2 \cdots p_\tau^{\tau-1})^{-2n} N_{k-n\tau}(P_\tau). \tag{10}$$

Using the estimates (4), it is not hard to verify that

$$P_1 \cdots P_\tau \ll p_2 p_3^2 \cdots p_\tau^{\tau-1} P_\tau^\tau, \qquad p_1 \cdots p_\tau \ll (1+2\theta)^\tau P^{1-(1-1/n)^\tau}.$$

Substituting these estimates into (10) and using the trivial estimate for $N_{k-n\tau}(P_\tau)$, we obtain the assertion of the theorem:

$$N_k(P) \ll (3k^{2n})^\tau P_\tau^{2k} (p_1 \cdots p_\tau)^{2k-n(n+1)/2} \ll$$

$$\ll (3k^{2n})^\tau (1+2\theta)^{2k(n+\tau)} P^{2k-n(n+1)/2+n(n+1)/2(1-1/n)^\tau}.$$

It follows from Bertrand' s postulate that in Theorem 1 one may choose $\theta = 1$. Using deeper facts from elementary number theory, one can arrange that the quantity θ decreases as n increases. In particular, choosing, for $n \geq 11$, $\theta = 1/3 \ln 2n$ and estimating $N_{k-n\tau}(P_\tau)$ more precisely, we obtain the following assertion:

Theorem 2. There exist absolute constants α and C such that, for $n \geq 11$, $1 \leq \tau \leq 2n \ln(n+1) + 1$, $k \geq 2n^2 + n\tau$, $P \geq n^{\alpha n(1+1/(n-1))^\tau}$, the estimate

$$N_k(P) \leq C P^{2k-n(n+1)/2+n(n+1)/2(1-1/n)^\tau *}$$

is valid.

Received
12 X 1962

References

[1] I. M. Vinogradov, *Izv. Acad. Sci. USSR, Ser. Math.*, **15**, 109 (1951).
[2] I. M. Vinogradov, *Izv. Acad. Sci. USSR, Ser. Math.*, **22**, 161 (1958).
[3] A. A. Karatsuba, *Vestn. Moscow Univ.*, **4**, 28 (1962).
[4] N. M. Korobov, *DAN*, **123**, No. 1, 28 (1958).
[5] Hua Loo-keng, *Quart. J. Math.*, **20**, 48 (1949).

* It can be shown that for $\alpha = 86$ one obtains $C \leq 1$.

Note: Figure translations are in progress. See original paper for figures.