# SYSTEMS OF CONGRUENCES AND EQUATIONS OF WARING TYPE

MATHEMATICS

1965

SovietRxiv

## Abstract

## Full Text

UDC 511.9

**MATHEMATICS**

A. A. KARATSUBA

# SYSTEMS OF CONGRUENCES AND EQUATIONS OF WARING TYPE

*(Presented by Academician I. M. Vinogradov, 8 IV 1965)*

We shall use the following notation. All letters, with the exception of $\varepsilon, \varepsilon_0, \dots, \delta, \delta_0, \dots$, denote integers; $\varepsilon, \varepsilon_0, \dots, \delta, \delta_0$ are positive real quantities; $n \geq 10$; $1 \leq r \leq n$; $p$ is a prime number. The notation $A \gg B$ means that $A \geq C(n)|B|$, where $C(n)$ is a constant depending only on $n$; $C, C_1, \dots$ are absolute constants; $J_{k,n}(\lambda_1, \dots, \lambda_n)$ is the number of solutions of the system of equations

$$\begin{gathered} x_1 + \dots - y_k = \lambda_1 \\ x_1^n + \dots - y_k^n = \lambda_n, \\ 1 \leq x_i, y_i \leq P; \quad i = 1, 2, \dots, k; \end{gathered} \tag{1}$$

$I_{k,n}$ is the number of solutions of the equation

$$x_1^n + \dots + x_k^n = y_1^n + \dots + y_k^n,$$

$$1 \leq x_i, y_i \leq P; \quad i = 1, 2, \dots, k;$$

$N_{k,n}$ is the number of solutions of the system of congruences

$$\begin{gathered} x_1 + \dots - y_k = 0, \\ x_1^r + \dots - y_k^r = 0, \\ x_1^{r+1} + \dots - y_k^{r+1} \equiv 0 \pmod{q_{r+1}}, \\ x_1^n + \dots - y_k^n \equiv 0 \pmod{q_n}, \\ 1 \leq x_i, y_i \leq P; \quad i = 1, 2, \dots, k. \end{gathered} \tag{1'}$$

The mean value theorem of I. M. Vinogradov ([1]) asserts that for

$$k \geq n(n+1)/4 + n\tau$$

the inequality holds

$$J_{k,n}(0,\dots,0) = I_{k,n} \ll P^{2k-n(n+1)/2+\delta}, \tag{2}$$

where

$$\delta = \frac{1}{2}n(n+1)/(1-1/n)^{\tau}.$$

It follows from this theorem that for $k \geq n(n+1)/4 + n\tau$, for $N_{k,n}$ the estimate

$$N_{k,n} \ll P^{2k-r(r+1)/2+\delta}(q_{r+1}\dots q_n)^{-1} \tag{3}$$

holds.

For any $k$ we trivially have

$$N_{k,n} \gg P^{2k-n(n+1)/2}(q_{r+1}\dots q_n)^{-1}.$$

Thus, estimate (3) is sharp.

The problem arises of obtaining estimates of the form (3) for smaller values of $k$. Let $1 \leq r \leq n$; $P^r \ll q \leq P^r$; $q \leq q_\nu < 2q$; $\nu = r+1,\dots,n$; $Q = q^{n-r}$. In ([2]), for a certain special $q_0$ and $q_{r+1} = \dots = q_n = q_0$, the estimate

$$N_{k,n} \ll P^{2k-rn+r(r-1)/2+\varepsilon_1}, \tag{4}$$

if $k \geqslant 6rn\ln n$. In the present article it is proved that, for $k \geqslant 6rn\ln n$, the estimate (4) holds for almost all sets $(q_{r+1},\dots,q_n)$. Moreover, a lower estimate is given for the number of sets $(q_{r+1},\dots,q_n)$ for which, when $k \leqslant 6rn\ln n$, the estimate (4) cannot be obtained. In the last two theorems, estimates are obtained for $I_{k,n}$ and inequalities between the quantities $I_{k,n}$ and $I_{k,m}$, which refine the corresponding theorems of ([2]).

**Theorem 1.** Among the $Q$ sets of moduli $(q_{r+1},\dots,q_n)$ there exist $Q(1-Q^{-\varepsilon_0})$ such that, for these moduli, when $k \geqslant 6rn\ln n$, the estimate

$$N_{k,n} \ll P^{2k-rn+r(r-1)/2+\varepsilon}Q^{\varepsilon_0},$$

holds, where $\varepsilon$ is arbitrarily small and $\varepsilon_0$ is an arbitrary positive quantity, $0 < \varepsilon_0 < 1$.

**Proof.** Arrange all $N_{k,n}$ in increasing order. We shall use the fact that $N_{k,n}$, corresponding to the set of moduli $(q_{r+1},\dots,q_n)$, is equal to

$$\sum_{\lambda_{r+1},\dots,\lambda_n} J_{k,n}(0,\dots,0,q_{r+1}\lambda_{r+1},\dots,q_k\lambda_n).$$

Summing the last $Q^{1-\varepsilon_0}$ terms of our nondecreasing sequence and applying the estimates of Theorem 3 of article ([2]), we obtain the assertion of the theorem.

**Theorem 2.** Let the set $(q_{r+1}, \dots, q_n)$ be such that

$$q_i = p^{\alpha_i} q_i', \quad 1 \leqslant \alpha_i \leqslant i, \quad (q_i', p) = 1, \quad i = r+1, \dots, n; \quad 2p < P.$$

Then for the corresponding $N_{k,n}$ the following lower estimate holds:

$$N_{k,n} \gg P^{2k-rn+r(r-1)/2} p^{-2k+\alpha_{r+1}+\dots+\alpha_n}.$$

**Proof.** Estimating from below the number of those solutions of system $(1')$ with the given $(q_{r+1}, \dots, q_n)$ which are multiples of $p$, we obtain the assertion of the theorem.

**Corollary.** Let $\alpha_{r+1} + \dots + \alpha_n > Crn \ln n$ and $p \to \infty$ as $P \to \infty$. Then, for $k \leqslant Crn \ln n$, one cannot obtain an estimate for $N_{k,n}$ of the form (4).

In ([2]) the estimate

$$I_{k,n} \ll P^{2k-r} \tag{5}$$

was obtained for $k \geqslant 6rn \ln n$.

**Theorem 3.** The estimate (5) holds for $k \geqslant c_1 r^2$, if $1 \leqslant r \leqslant \frac{1}{3}n$, and for $k \geqslant c_2 n^2 \ln n$, if $\frac{1}{3}n < r \leqslant n$.

**Proof.** The second case follows trivially from the asymptotic formula in Waring' s problem obtained by I. M. Vinogradov (see ([1]), p. 300). Consider the case $1 \leqslant r \leqslant \frac{1}{3}n$. Let $s = 2r$ and let $p$ be a prime number satisfying the inequalities

$$P^{s/(s+1)} < p < 2P^{s/(s+1)}.$$

If $\overline{N}_{k,n}$ is the number of solutions of the congruence

$$x_1^n + \dots - y_k^n \equiv 0 \pmod{p^{s+1}},$$

$$1 \leqslant x_i, y_i \leqslant p^{1+1/s}, \quad i = 1, 2, \dots, k,$$

then it is clear that

$$J_{k,n} \leqslant \overline{N}_{k,n},$$

Take $x = py + z,\ 1 \leq z \leq p,\ y \leq p^{1/s}$. After the corresponding transformations we obtain

$$N_{k,n} \ll p^{2k/s} + p^{2k-s-1} \sum_{a=1}^{p^{s+1}} \left| \sum_{y \leq p^{1/s}} \exp \frac{2\pi i a}{p^s} \left(b_1 y + \dots + b_{sp}^{s-1} y^s\right) \right|^{2k} \ll$$

$$\ll p^{2k/s} + p^{2k} N_{k,n}',$$

where $N'_{k,n}$ is the number of solutions of the congruence

$$b_1(y_1 + \cdots - y_k) + pb_2(y_1^2 + \cdots - y_k^2) + \cdots + p^{s-1}b_s(y_1^s + \cdots - y_k^s) \equiv$$

$$\equiv 0 \pmod{p^s},$$

$$(b_1, p) = \cdots = (b_s, p) = 1; \qquad 0 \le y_i; \quad y_i \le p^{1/s}, \quad i = 1, 2, \ldots, k.$$

The last congruence is equivalent to the system of equations (1) for $\lambda_1 = \ldots = \lambda_n = 0$. Applying estimate (2) and choosing $\tau$ in a suitable way, we obtain the assertion of the theorem.

**Theorem 4.** If $k = c_3 m^2 \ln m$, $2 \le m \le n$, then the inequality

$$I_{k,n} \ll I_{k,m}$$

holds.

The proof follows from Theorem 4 (see (2), Theorem 2).

Received
5 IV 1965

## CITED LITERATURE

[1] I. M. Vinogradov, *Selected Works*, Publishing House of the Academy of Sciences of the USSR, 1952. [2] A. A. Karatsuba, DAN, 165, No. 1 (1965).

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