

SYSTEMS OF CONGRUENCES AND EQUATIONS OF WARING TYPE

A. A. Karatsuba

1965

SovietRxiv

View the original and related papers at <https://sovietsrxiv.org/items/ru-196501.59875>

Source: Math-Net.Ru and CyberLeninka. Machine translation. Verify with the original.

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

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

$I_{k,n}$ 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

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

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

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

the inequality holds

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

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

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

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

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

if $k \geq 6rn \ln n$. In the present article it is proved that, for $k \geq 6rn \ln n$, 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 $k \leq 6rn \ln n$, 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 $k \geq 6rn \ln n$, the estimate

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

holds, where ε is arbitrarily small and ε_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

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

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

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

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 $p \rightarrow \infty$ as $P \rightarrow \infty$. Then, for $k \leq Crn \ln n$, one cannot obtain an estimate for $N_{k,n}$ of the form (4).

In ⁽²⁾ the estimate

$$I_{k,n} \ll P^{2k-r} \quad (5)$$

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

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

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 $1 \leq r \leq \frac{1}{3}n$. 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

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

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

then it is clear that

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

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

$$\begin{aligned} N_{k,n} &\ll p^{2k/s} + p^{2k-s-1} \sum_{a=1}^{p^{s+1}} \left| \sum_{y \leq p^{1/s}} \exp \frac{2\pi i a}{p^s} (b_1 y + \dots + b_s p^{s-1} y^s) \right|^{2k} \\ &\ll p^{2k/s} + p^{2k} N'_{k,n}, \end{aligned}$$

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

$$\begin{aligned} b_1(y_1 + \dots - y_k) + pb_2(y_1^2 + \dots - y_k^2) + \dots + p^{s-1}b_s(y_1^s + \dots - y_k^s) \equiv \\ \equiv 0 \pmod{p^s}, \end{aligned}$$

$$(b_1, p) = \dots = (b_s, p) = 1; \quad 0 \leq y_i; \quad y_i \leq p^{1/s}, \quad i = 1, 2, \dots, k.$$

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

Theorem 4. If $k = c_3 m^2 \ln m$, $2 \leq m \leq n$, 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.

Source: Math-Net.Ru and CyberLeninka. Machine translation. Verify with the original.