ON THE QUESTION OF AN ASYMPTOTIC FORMULA

MATHEMATICS

1970

SovietRxiv

Abstract

Full Text

UDC 511.9

MATHEMATICS

B. G. KOTSAREV

ON THE QUESTION OF AN ASYMPTOTIC FORMULA

FOR THE NUMBER OF SOLUTIONS OF A CONGRUENCE OF WARING TYPE

(Presented by Academician Yu. V. Linnik on 27 X 1969)

Consider the congruence

$$x_1^n + x_2^n + \dots + x_t^n \equiv d \pmod{p^s}, \tag{1}$$

where n, t, s are natural numbers, p is prime, and d is an arbitrary integer. Let $M_1, \dots, M_t,\ Q_1, \dots, Q_t$ be integers, $0 \le M_j < M_j + Q_j \le p^s,\ j = 1, \dots, t$. In the works of A. A. Karatsuba ([1,2]) an asymptotic formula was obtained for the number of solutions of congruence (1) in an incomplete system of residues

$$M_j \le x_j \le M_j + Q_j - 1, \qquad j = 1, \dots, t. \tag{2}$$

Generally speaking, it is impossible to obtain an analogous asymptotic formula for the number of solutions of congruence (1) when $t = n$ (see ([2,3])). In this connection it is of interest to study such a congruence which, in a certain sense, would differ little from congruence (1), and for the number of whose solutions an asymptotic formula could be obtained for $t = n$. In the present work we consider the congruence obtained from congruence (1) by replacing the constant number d by a variable y, with a small interval of variation q, and some generalizations of it with a possibly smaller number of variables $x_1, \dots, x_t$. A similar approach to the formulation of the problem was used by Yu. V. Linnik ([4]) in considering the binary Goldbach problem. An asymptotic formula for the number of solutions of the congruence obtained in this way already holds for $t = \min(n, s)$ and q increasing arbitrarily slowly with the growth of p, or for fixed $p \ge n + 1$ and q increasing arbitrarily slowly with the growth of s, if $t \ge n + 1$. In ([5]) it was shown that, as $s \to \infty$ and $q = s$, an analogous asymptotic formula for $t = n$, generally speaking, does not hold.

We shall henceforth consider the congruence

$$\sum_{j=1}^{\tau}\sum_{r_j=1}^{\alpha_j} a_{jr_j} x_{jr_j}^{n_j} \equiv y \pmod{p^s}, \tag{3}$$

where $a_{jr_j}, n_j, s \geq 3$ are integers, $(a_{jr_j}, p) = 1$, $3 \leq n_1 < \cdots < n_\tau < p$.

Let $t = \alpha_1 + \cdots + \alpha_\tau$, $l_j = \min(n_j, s)$; we shall call the number N, defined as follows, the harmonic index of congruence (3):

$$N = t\left(\sum_{j=1}^{\tau}\frac{\alpha_j}{l_j}\right)^{-1}.$$

For congruence (1), $N = \min(n, s)$. Denote by $T'_q(N)$ the number of solutions of congruence (3) for which inequalities (2) hold and $m \leq y \leq m+q-1$, where m and q are integers, $0 \leq m < m+q \leq p^s$.

Theorem 1. Let $t \geq N$, and let $\varepsilon > 0$ be a real number, $1 \leq q \leq p^s$,

$$p^{s(1/2+1/l_j+\varepsilon)} \leq Q_{jr_j} \leq p^s, \qquad r_j = 1, \dots, \alpha_j, \quad j = 1, \dots, \tau. \tag{4}$$

Then for the quantity $T'_q(N)$ the following expression holds:

$$T'_q(N) = qQ_1 \cdots Q_t p^{-s}\{1 + O(\gamma(q)\eta(t)\max(p^{-t/2+1},\ p^{-l_1(t/N-1)})\}.$$

where

$$\gamma(q) = \begin{cases} 1, & \text{if } q = 1, \\ q^{-1}\ln q, & \text{if } q \geqslant 2; \end{cases} \qquad \eta(t) = \begin{cases} s, & \text{if } t = N, \\ 1, & \text{if } t > N. \end{cases}$$

The constant in the symbol O depends only on $n_1, \dots, n_\tau, \alpha_1, \dots, \alpha_\tau$ and ε.

The proof of the theorem is based on the following lemmas.

Lemma 1. Let $f(x_1, \dots, x_t)$ be an integral rational function with integer coefficients in t variables $x_1, \dots, x_t$, $t \geqslant 1$; let T be the number of solutions of the congruence

$$f(x_1, \dots, x_t) \equiv y \pmod{p^s},$$

for which the inequalities (2) hold, $m \leqslant y \leqslant m+q-1$.

Then

$$T = qQ_1 \cdots Q_t p^{-s} +$$
$$+O\left(\gamma_0(q)p^{-s}\sum_{k=1}^{s} p^k \max_{z \not\equiv 0 \ (\bmod p)}\left|\sum_{x_1=M_1}^{M_1+Q_1-1}\cdots\sum_{x_t=M_t}^{M_t+Q_t-1}\exp\frac{2\pi i}{p^k} z f(x_1, \dots, x_t)\right|\right)$$

with an absolute constant in the symbol O, $z \in [1, p^s - 1]$; $\gamma_0(q) = 1$, if $q = 1$, $\gamma_0(q) = \ln q$, if $q \geqslant 2$.

Proof. We express the number of solutions T through a trigonometric sum (see (6), question 1, a to Chapter IV)

$$T = p^{-s} \sum_{k=0}^{s} \sum_{\substack{z=1\\(z,p)=1}}^{p^k} \sum_{x_1=M_1}^{M_1+Q_1-1} \cdots \sum_{x_t=M_t}^{M_t+Q_t-1} \sum_{y=m}^{m+q-1} \exp \frac{2\pi i}{p^k} z(f(x_1, \dots, x_t) - y).$$

Hence

$$|T - qQ_1 \cdots Q_t p^{-s}| \leqslant$$
$$\leqslant p^{-s} \sum_{k=1}^{s} R(k) \max_{z \not\equiv 0 \pmod p} \left| \sum_{x_1=M_1}^{M_1+Q_1-1} \cdots \sum_{x_t=M_t}^{M_t+Q_t-1} \exp \frac{2\pi i}{p^k} z f(x_1, \dots, x_t) \right|, \quad (5)$$

where

$$R(k) = \sum_{\substack{z=1\\(z,p)=1}}^{p^k} \left| \sum_{y=m}^{m+q-1} \exp \frac{2\pi i}{p^k}(-zy) \right| \leqslant \sum_{z=1}^{p^k-1} \frac{|\sin \pi z q/p^k|}{\sin \pi z/p^k}. \quad (6)$$

If $q = 1$, then $R(k) < p^k$. For $q \geqslant 2$, to estimate $R(k)$ we use the following result of B. I. Golubov ([7]), putting $M = p^k$.

There exists an absolute constant $c_0 > 0$ such that

$$\sum_{z=1}^{M-1} \frac{|\sin \pi z q/M|}{\sin \pi z/M} \leqslant c_0 M \ln q. \quad (7)$$

From formula (5) and inequalities (6) and (7) the assertion of the lemma follows.

Lemma 2 (Hua Loo-keng ([8])). Let a, q, P be integers, $(a, q) = 1$, $q \geqslant 1$, $P \geqslant 1$, $n \geqslant 2$.

Then for any $\varepsilon > 0$

$$\sum_{x=1}^{P} \exp \frac{2\pi i}{q} a x^n = \frac{P}{q} \sum_{x=1}^{q} \exp \frac{2\pi i}{q} a x^n + O(q^{1/2+\varepsilon}),$$

where the constant in the symbol O depends only on n and ε.

Lemma 3. Let $f(x) = a_1x + \dots + a_{nx}^n$ be a polynomial of degree $n \geqslant 2$ with integer coefficients, $p > n$ a prime, $a_n \not\equiv 0 \pmod p$, $s \geqslant 1$.

Then the estimate holds

$$\left|\sum_{x=1}^{p^s} \exp\frac{2\pi i}{p^s} f(x)\right| \leqslant \begin{cases}(n-1)p^{1/2}, & \text{if } s=1,\\ (n-1)p^{s-1}, & \text{if } 2\leqslant s\leqslant n,\\ c(n)p^{s(1-1/n)}, & \text{for any } s\geqslant 1.\end{cases}$$

The proof of the first of the inequalities written above is the subject of the papers ([9], [10]) and § 2 of A. G. Postnikov' s book ([11]). The second and third inequalities are proved, respectively, in the papers of A. A. Karatsuba ([12]) and Hua Loo-keng (([13]), *pp*.7—12). In the case when $f(x) = ax^n$, $(a, p) = 1$, Lemma 3 follows from lemmas of I. M. Vinogradov (([14]), *pp*.269—271).

Proof of Theorem 1. By Lemma 1 we have

$$T_q'(N) = qQ_1 \dots Q_t p^{-s} + O\left(\gamma_0(q)p^{-s}\sum_{k=1}^{s} p^{kS}(k)\right), \tag{8}$$

where

$$S(k) = \prod_{j=1}^{\tau}\sum_{r_j=1}^{a_j} S_{jr_j}(k), \qquad S_{jr_j}(k) = \max_{z\not\equiv 0 \pmod p}\left|\sum_{x_{jr_j}=M_{jr_j}}^{M_{jr_j}+Q_{jr_j}-1} \exp\frac{2\pi i}{p^k} za_{jr_j}x_{jr_j}^{n_j}\right|.$$

We estimate the expression $S_{jr_j}(k)$ by Lemma 2:

$$S_{jr_j}(k) = \max_{z\not\equiv 0 \pmod p}\frac{Q_{jr_j}}{p^k}\left|\sum_{x_{jr_j}=1}^{p^k}\exp\frac{2\pi i}{p^k} za_{jr_j}x_{jr_j}^{n_j}\right| + O\left(p^{k(1/2+\varepsilon)}\right).$$

Estimating the modulus of the complete sum on the right-hand side of the last equality by Lemma 3, depending on the value of k we obtain

$$S_{jr_j}(k) \ll \begin{cases} Q_{jr_j}p^{-1/2}, & \text{if } k=1,\\ Q_{jr_j}p^{-1}, & \text{if } 2\le k\le n_j,\\ Q_{jr_j}p^{-k/n_j}, & \text{if } n_j+1\le k\le s,\end{cases}$$

in view of the fact that Q_{jr_j} satisfies inequality (4). In estimating the remainder term in formula (8), we shall split the sum over k in accordance with the estimates for $S_{jr_j}(k)$ obtained above. Depending on the value of s, we consider the following three cases.

1°. If $s \le n_1$, then

$$\sum_{k=1}^{s} p^{kS}(k) \ll Q_1 \dots Q_t \left(p^{-t/2+1} + \sum_{k=2}^{s} p^{k-t}\right) \ll Q_1 \dots Q_t \max\left(p^{-t/2+1},\, p^{-s(t/N-1)}\right). \tag{9}$$

2°. Let $n_j < s \le n_{j+1}$, where j is one of the numbers $1, \dots, \tau - 1$ ($\tau \ge 2$). Then

$$\sum_{k=1}^{s} p^{kS}(k) \ll Q_1 \dots Q_t \left(p^{-t/2+1} + \sum_{k=2}^{n_1} p^{k-t} + \right.$$

$$+ \sum_{\nu=1}^{j-1} \sum_{k=n_\nu+1}^{n_{\nu+1}} p^{k-(a_{\nu+1}+\dots+a_\tau)-k(a_1/n_1+\dots+a_\nu/n_\nu)} + \tag{10}$$

$$\left. + \sum_{k=n_j+1}^{s} p^{k-(a_{j+1}+\dots+a_\tau)-k(a_1/n_1+\dots+a_j/n_j)} \right) \ll Q_1 \dots Q_t \max\left(p^{-t/2+1},\, p^{-n_1(t/N-1)}\right).$$

3°. If $s \ge n_\tau + 1$, then

$$\sum_{k=1}^{s} p^{kS}(k) \ll Q_1 \dots Q_t \left(p^{-t/2+1} + \sum_{k=2}^{n_1} p^{k-t} + \right.$$

$$\left. + \sum_{\nu=1}^{\tau-1} \sum_{k=n_\nu+1}^{n_{\nu+1}} p^{k-(a_{\nu+1}+\dots+a_\tau)-k(a_1/n_1+\dots+a_\nu/n_\nu)} + \sum_{k=n_\tau+1}^{s} p^{-k(t/N-1)} \right) \ll$$

$$\ll \eta(t) Q_1 \dots Q_t \max\left(p^{-t/2+1},\, p^{-n_1(t/N-1)}\right), \tag{11}$$

where $\eta(t) = s$ for $t = N$. If $t > N$, then $tN^{-1} - 1 \geqslant N_0^{-1}$, where N_0 is the least common multiple of $n_1, \dots, n_t$; consequently,

$$\sum_{k=n_\tau+1}^{s} p^{-k(t/N-1)} < p^{-n_1(t/N-1)} \left(p^{t/N-1} - 1\right)^{-1} \ll p^{-n_1(t/N-1)}.$$

Thus, for $t > N$, $\eta(t) = 1$. From formula (8) and inequalities (9), (10), and (11), with $\gamma(q) = q^{-1}\gamma_0(q)$, the theorem being proved follows.

From comparison of A. A. Karatsuba' s result (2) and Theorem 1 we obtain

Corollary. If $n \geqslant 20$, $t \geqslant cn$, where c is an absolute constant, then the asymptotic formula holds

$$\sum_{\nu=0}^{\infty} p^{-\nu t} \sum_{\substack{z=1 \\ (z,p)=1}}^{p^\nu} \left(\sum_{x=1}^{p^\nu} \exp \frac{2\pi i}{p^\nu} z x^n \right)^t \exp\left(-\frac{2\pi i}{p^\nu} z d \right) = 1 + O\left(p^{-t/2+1}\right),$$

where the constant in the O-symbol depends only on n and t.

Let $f_j(x_j) = a_{1j}x_j + \dots + a_{n_j j} x_j^{n_j}$ be a polynomial of degree $n_j \geqslant 2$ with integral coefficients, $(a_{n_j j}, p) = 1$, $j = 1, \dots, t$; $p > \max(n_1, \dots, n_t)$, $s \geqslant 2$. Denote by $T_q(N)$ the number of solutions of the congruence

$$f_1(x_1) + \dots + f_t(x_t) \equiv y \pmod{p^s}, \tag{12}$$

when $x_1, \dots, x_t$ run through a complete system of residues modulo p^s, $m \leqslant y \leqslant m + q - 1$.

Theorem 2. If $t \geqslant N$, where N is the harmonic index of congruence (12), $1 \leqslant q \leqslant p^s$, then for $T_q(N)$ one has the expression

$$T_q(N) = qp^{s(t-1)} \left\{ 1 + O\left(\gamma(q)\eta(t) \max\left(p^{-t/2+1},\, p^{-(t/N-1)\min(n_1,\dots,n_t,s)} \right) \right) \right\}.$$

The constant in the O-symbol depends only on $n_1, \dots, n_t$; the values $\gamma(q)$ and $\eta(t)$ are determined by the conditions of Theorem 1.

The author expresses his deep gratitude to K. A. Rodosskii for his constant attention to his work and valuable advice.

Voronezh State
Pedagogical Institute

Received
6 IX 1969

REFERENCES

1. A. A. Karatsuba, *Vestn. MGU*, **1**, 38 (1962).
2. A. A. Karatsuba, Doctoral dissertation, Moscow, 1965.
3. A. A. Karatsuba, *DAN*, **169**, No. 1, 9 (1966).

4. Yu. V. Linnik, *Izv. AN SSSR, ser. matem.*, **16**, 503 (1952).

5. B. I. Stechkin, *Collected papers: Investigations in number theory*, no. 3, Saratov, 1969, p. 42.

6. I. M. Vinogradov, *Fundamentals of Number Theory*, Moscow, 1965.

7. B. I. Golubev, *Sibirsk. matem. zhurn.*, **9**, No. 2, 297 (1968).

8. L. K. Hua, *Sci. Record*, **1**, No. 1, 1 (1957).

9. A. Weil, *Proc. Nat. Acad. Sci. USA*, **34**, No. 5, 204 (1948).

10. L. Carlitz, S. Uchiyama, *Duke Math. J.*, **24**, No. 1, 37 (1957).

11. A. G. Postnikov, *Tr. Matem. inst. im. V. A. Steklova AN SSSR*, **82** (1966).

12. A. A. Karatsuba, *Izv. AN SSSR, ser. matem.*, **30**, No. 1, 183 (1966).

13. Hua Lo-keng, *Tr. Matem. inst. im. V. A. Steklova AN SSSR*, **22** (1947).

14. I. M. Vinogradov, *Selected Works*, Moscow, 1952.

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