MATHEMATICS

1963

SovietRxiv

Abstract

Full Text

MATHEMATICS

L. P. USOLTSEV

ON AN EXPONENTIAL RATIONAL TRIGONOMETRIC SUM OF A SPECIAL FORM

(Presented by Academician I. M. Vinogradov on 24 I 1963)

The present paper is a continuation of the work of A. G. Postnikov ([1]). In ([1]) the following was proved.

Theorem. Let $g \geqslant 2$ be a natural number. Let p be a prime number; $h = h(p)$ some integer-valued function; $h \to \infty$ as $p \to \infty$; $h \leqslant \log p/2 \log g$. Let $\lambda > 0$ be a constant. Denote by $N_p(\lambda)$ the number of integers a, $0 \leqslant a \leqslant p-1$, for which

$$\left|\sum_{x=0}^{h-1} \exp\left[2\pi i \frac{ag^x}{p}\right]\right| < \lambda\sqrt{h}.$$

Then, as $p \to \infty$,

$$\lim_{p\to\infty} \frac{1}{p} N_p(\lambda) = 1 - e^{-\lambda^2}.$$

In this theorem we have managed to remove the restriction $h \leqslant \log p/2 \log g$ in the case when the denominator has the special form $p = g^\tau - 1$, where $\tau \geqslant 2$ is arbitrary natural. The result is formulated as the following theorem:

Theorem 1. Let $g \geqslant 2$, $\tau \geqslant 2$, c, h be natural numbers such that $c\tau \to \infty$, $(c-1)\tau < h \leqslant c\tau$. Let $\lambda > 0$ be a constant. Denote by $N_{g^\tau-1}(\lambda)$ the number of integers a, $0 \leqslant a \leqslant g^\tau - 2$, for which

$$\left|\sum_{x=0}^{h-1} \exp\left[2\pi i \frac{ag^x}{g^\tau - 1}\right]\right| < \lambda\sqrt{(2c-1)h - c(c-1)\tau}.$$

Then, as $c\tau \to \infty$,

$$\lim_{c\tau\to\infty} \frac{1}{g^\tau - 1} N_{g^\tau-1}(\lambda) = 1 - e^{-\lambda^2}.$$

The proof of this theorem is carried out by the method of moments in exactly the same way as was done in ([1]); however, the moments here are expressed in terms of the number of solutions of the congruence

$$g^{x_1} + ... + g^{x_n} \equiv g^{y_1} + ... + g^{y_n} \pmod{g^\tau - 1} \tag{1}$$

in integers x_i, y_i belonging to a longer interval than in ([1]). We find this number in Theorem 2; therefore, for the proof of Theorem 1 it is only necessary to repeat the reasoning of A. G. Postnikov in ([1]), but now taking into account the assertion of Theorem 2.

Theorem 2. Let $n \geqslant 2$, $g \geqslant 2$, $\tau \geqslant 2$, c, h be natural numbers such that $c\tau \to \infty$, $(c-1)\tau < h \leqslant c\tau$. Then for the number of solutions $A_n(h)$ of congruence (1) in integers $0 \leqslant x_i, y_i \leqslant h-1$ $(i, j = 1, ..., n)$, as $c\tau \to \infty$ the asymptotic formula

$$A_n(h) = n!\,[(2c-1)h - c(c-1)\tau]^n + O(c^n h^{n-1}),$$

holds, where the constant in the O-symbol depends only on n.

For the proof of this theorem we shall need the following

Lemma. Let $g \geqslant 2$, n, c, p, N be natural numbers such that $g < p$, $(g, p) = 1$. Then the number of solutions of the congruence

$$N \equiv g^{z_1} + ... + g^{z_n} \pmod{p} \tag{2}$$

in nonnegative integers $z_1, ..., z_n$ such that $g^{z_1} + ... + g^{z_n} \leqslant$

$\leq cp$, is estimated as $O(c)$, where the constant in the symbol O depends only on n.

Proof of the lemma. We divide all solutions of congruence (2) into c groups. To the k-th group $(k = 1, 2, ..., c)$ we assign those solutions $z_1, ..., z_n$ for which

$$(k-1)p < g^{z_1} + \cdots + g^{z_n} \leq kp. \tag{3}$$

Let $z_1^{(k)}, ..., z_n^{(k)}$ be some solution of congruence (2) belonging to the k-th group. Denote

$$N_k = g^{z_1^{(k)}} + \cdots + g^{z_n^{(k)}}.$$

For any other solution $\tilde{z}_1^{(k)}, ..., \tilde{z}_n^{(k)}$ of congruence (2) belonging to the k-th group, we have

$$N_k \equiv g^{\tilde{z}_1^{(k)}} + \cdots + g^{\tilde{z}_n^{(k)}} \pmod{p}. \tag{4}$$

In view of condition (3), congruence (4) is simply the equation

$$N_k = g^{\tilde{z}_1^{(k)}} + \cdots + g^{\tilde{z}_n^{(k)}}. \tag{5}$$

In the work ([2]) A. G. Postnikov proved that the number of solutions of an equation of the form (5) in nonnegative integers is estimated as $O(1)$, where the constant in the symbol O depends only on n. Thus, in each of the c groups there will be $O(1)$ solutions. Consequently, the number of solutions of congruence (2) is estimated as $O(c)$, where the constant in the symbol O depends only on n. The lemma is proved.

Proof of Theorem 2. Denote

$$g^{\tau} - 1 = p. \tag{6}$$

We divide all solutions of congruence (1) into two categories:

1) Solutions $x_1, \ldots, x_n, y_1, \ldots, y_n$ in which at least one of the relations $x_i \equiv x_j \pmod{\tau}$ or $y_i \equiv y_j \pmod{\tau}$ holds for $i \neq j$. It is possible to specify no more than $2 \cdot C_n^2 = O(1)$ different variants of such relations. Consider one of the variants, for example the case $x_1 \equiv x_2 \pmod{\tau}$. In view of the condition $0 \leq x_1, x_2 \leq h - 1 \leq c\tau - 1$, for any value of x_2 we can find no more than c values of x_1 such that $x_1 \equiv x_2 \pmod{\tau}$. Therefore, assigning to the quantities $x_1, \ldots, x_n$ all possible values (from 0 to $h-1$), we obtain no more than ch^{n-1} systems $x_1, \ldots, x_n$ for which $x_1 \equiv x_2 \pmod{\tau}$. To each such system $x_1, \ldots, x_n$, by the lemma there will correspond $O(c)$ systems $y_1, \ldots, y_n$. Thus, the number of solutions of congruence (1) belonging to the first category is estimated as $O(c^2 h^{n-1})$, where the constant in the symbol O depends only on n.

2) Solutions $x_1, \ldots, x_n, y_1, \ldots, y_n$ in which, for $i \neq j$,

$$x_i \not\equiv x_j \pmod{\tau}, \qquad y_i \not\equiv y_j \pmod{\tau}. \tag{7}$$

By $\{a_1, a_2, a_3, \ldots\}$ we shall denote the set consisting of the numbers $a_1, a_2, a_3, \ldots$. The range of variation of the quantities x_i and y_j, i.e. the set $M = \{0, 1, \ldots, h-1\}$, is the union of the following c sets:

$$M_1 = \{0, 1, \ldots, \tau-1\}, \quad M_2 = \{\tau, \ldots, 2\tau-1\}, \ldots, \quad M_{c-1} = \{(c-2)\tau, \ldots, (c-1)\tau-1\}, \quad M_c = \{(c-1)\tau, \ldots, h-1\}.$$

Each of the first $c-1$ sets M_i consists of τ numbers, while the set M_c consists of $t = h - (c-1)\tau$ numbers. Since $(c-1)\tau < h \leq c\tau$, we have $1 \leq t \leq \tau$.

Each of the first $c-1$ sets M_i is divided into two subsets $M_i^{(1)}$ and $M_i^{(2)}$, assigning to $M_i^{(1)}$ the first t numbers of the set M_i, and to $M_i^{(2)}$ the last $\tau - t$ numbers of the set M_i. Let $M^{(1)}$ be the union of the sets $M_1^{(1)}, M_2^{(1)}, \dots, M_{c-1}^{(1)}, M_c$, and $M^{(2)}$ the union of the sets $M_1^{(2)}, M_2^{(2)}, \dots, M_{c-1}^{(2)}$. The set $M^{(1)}$ will consist of ct numbers, and the set $M^{(2)}$ of $(c-1)(\tau-t)$ numbers. The numbers belonging to the set $M^{(1)}$ can be divided into t groups so that each group contains c numbers, and all the numbers,

belonging to one and the same group will be congruent to one another modulo τ. Similarly, the numbers belonging to the set $M^{(2)}$ can be divided into $\tau-t$ groups so that in each group there will be $c-1$ numbers, and all numbers belonging to one and the same group will be congruent to one another modulo τ.

By $\tilde{a}$ we shall denote the least nonnegative residue of the integer a modulo τ. Take an arbitrary fixed system $x_1, \dots, x_n$ satisfying condition (7), and consider the number $N = g^{x_1} + \dots + g^{x_n}$. Since, by condition (6), $g^\tau = p + 1$, we have

$$N \equiv g^{\tilde{x}_1} + \dots + g^{\tilde{x}_n} \pmod{p},$$

and $\tilde{x}_i \neq \tilde{x}_j$ for $i \neq j$. Further,

$$1 \leq g^{\tilde{x}_1} + \dots + g^{\tilde{x}_n} \leq g^{\tau-1} + g^{\tau-2} + \dots + g^{\tau-n} < g^\tau = p + 1,$$

i.e.

$$1 \leq g^{\tilde{x}_1} + \dots + g^{\tilde{x}_n} \leq p. \tag{8}$$

Let, among the numbers $x_1, \dots, x_n$ that we have taken, the numbers $x_1, \dots, x_m \in M^{(1)}$, and the numbers $x_{m+1}, \dots, x_n \in M^{(2)}$, where $0 \leq m \leq n$ (if $m = 0$, then all the numbers are taken from $M^{(2)}$, and if $m = n$, then all the numbers are taken from $M^{(1)}$). Consider the congruence

$$N \equiv g^{y_1} + \dots + g^{y_n} \pmod{p} \tag{9}$$

in integers $0 \leq y_i \leq h-1$, satisfying condition (7). Congruence (9) is equivalent to the following:

$$g^{\tilde{x}_1} + \dots + g^{\tilde{x}_n} \equiv g^{y_1} + \dots + g^{y_n} \pmod{p}. \tag{10}$$

By condition (8) and the fact that $g^\tau = p + 1$, the solutions of congruence (10), and consequently also of congruence (9), will be, up to a permutation of the elements, only those systems $y_1, \dots, y_n$ for which $y_i \equiv x_i \pmod{\tau}$ $(i = 1, \dots, n)$. Since $x_1, \dots, x_m \in M^{(1)}$, $x_{m+1}, \dots, x_n \in M^{(2)}$, each of the quantities $y_1, \dots, y_m$ can assume c values from M (more precisely, from $M^{(1)}$), and each of the quantities $y_{m+1}, \dots, y_n$ can assume $c-1$ values from M (more precisely, from $M^{(2)}$). Consequently, the number of solutions of congruence (9) is equal to $n!c^m(c-1)^{n-m}$. Further, the number of distinct systems $x_1, \dots, x_n$ satisfying condition (7), and in which m numbers are taken from $M^{(1)}$, and $n-m$ numbers from $M^{(2)}$, is equal to

$$C_n^m(ct)(ct-1)\cdots(ct-m+1)[(c-1)(\tau-t)][(c-1)(\tau-t)-1]\cdots$$

$$\cdots[(c-1)(\tau-t)-(n-m)+1]=C_n^m(ct)^m[(c-1)(\tau-t)]^{n-m}$$
$$+O(c^{n-1}\tau^{n-1})=C_n^m(ct)^m[(c-1)(\tau-t)]^{n-m}+O(h^{n-1}).$$

Therefore the number of solutions of congruence (1) belonging to the second category is equal to

$$\sum_{m=0}^{n} n!c^m(c-1)^{n-m}\left\{C_n^m(ct)^m[(c-1)(\tau-t)]^{n-m}+O(h^{n-1})\right\}=$$

$$=n![c^2t+(c-1)^2(\tau-t)]^n+O(c^{nh^{n-1}})=n![(2c-1)h-c(c-1)\tau]^n+$$
$$+O(c^{nh^{n-1}}),$$

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

Adding the numbers of solutions of congruence (1) belonging to both categories, we obtain the assertion of the theorem, since, evidently, as $c\tau\to\infty$, in view of $n\geq 2$ we have

$$c^{nh^{n-1}}/[(2c-1)h-c(c-1)\tau]^n=O(1/c\tau).$$

The theorem is proved.

Omsk Machine-Building Institute

Received
16 I 1963

CITED LITERATURE

1. A. G. Postnikov, DAN, **133**, 1289 (1960).

2. A. G. Postnikow, *Festschrift anlässlich des 250 Geburtstages Leonhard Eulers*, Berlin, 1959, S. 281.

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