ISSN 0001-4346, Mathematical Notes, 2007, Vol. 81, No. 3, pp. 338–355. © Pleiades Publishing, Ltd., 2007.
Original Russian Text © N. G. Moshchevitin, I. D. Shkredov, 2007, published in Matematicheskie Zametki, 2007, Vol. 81, No. 3, pp. 385–404.

On the Multiplicative Properties Modulo m of Numbers with Missing Digits

N. G. Moshchevitin* **and I. D. Shkredov****

Moscow State University

Received March 14, 2005; in final form, June 20, 2006

Abstract—We obtain upper bounds for character sums modulo a composite number over sets of numbers with missing digits in a number system. We derive results on the solvability of congruences of the form $x_1 \cdots x_t \equiv \lambda \pmod m$ in the numbers with missing digits and also asymptotic formulas for the number of solutions.

DOI: 10.1134/S000143460703008X

Key words: *residue modulo m, number with missing digits, character sum, finite Fourier series.*

1. INTRODUCTION

In what follows, s, k are natural numbers,

$$D = \{d_0, \dots, d_k\} \subset \mathbb{N}_0 = \mathbb{N} \cup \{0\}, \qquad 0 = d_0 < d_1 < \cdots < d_k < s, \quad 1 \le k \le s-2,$$

is a fixed set of digits in a number system with base s, and $(d_1, \dots, d_k) = 1$. In the present paper, we study the distribution of elements of sets of the form

$$K_s^D(N) = \left\{ x \in \mathbb{N}_0 : x < N,\ x = \sum_{j=0}^{h} \delta_j s^j,\ \delta_j \in D \right\} \tag{1}$$

in a multiplicative residue group modulo m. Everywhere below, we assume

$$(m, s) = 1.$$

Recently, Konyagin [1] proved that, for natural N, m, and s such that $(m, s) = 1$ and

$$N > \exp(\gamma \log m \log\log m)$$

(here γ is a constant depending on s), the elements of the set $K_s^D(N)$ are uniformly distributed modulo m. As a consequence, it was found that, under the conditions mentioned above, for any integer x there exists an $a \in K_s^D(N)$ such that $a \equiv x \pmod m$. In the same paper, Konyagin posed the following problem: Is it true that there exists a constant $\sigma(s)$ satisfying

$$N > m^{\sigma(s)} \tag{2}$$

such that the set $K_s^D(N)$ contains all the residues modulo m? Konyagin gives a positive answer to this question for "almost all" natural numbers m. In the simplest case where $\operatorname{ord}_m s \le \beta \log m$ with a constant $\beta > 0$, the positive answer was given in [2].

In this paper, we prove a number of results on the distribution of elements of the sets (1) modulo m under condition (2): we estimate the character sums modulo m on the elements of the sets (1) and prove a number of assertions on the number $T_l(N, m, \lambda)$ of solutions of congruences of the form

$$x_1 \cdots x_l \equiv \lambda \pmod m, \qquad x_j \in K_s^D(N),$$

*E-mail: moshchevitin@rambler.ru
**E-mail: ishkredov@rambler.ru

for $(\lambda, m) = 1$. In particular, for any arbitrary natural m, $l \geq 4$, and for $N \geq m^\sigma$ with sufficiently large positive σ, we shall prove the following asymptotic formula for the number of solutions of the congruence:

$$T_l(N, m, \lambda) = \frac{|K_s^D(N, m)|^l}{\varphi(m)} \cdot \bigl(1 + O\bigl(\exp(-\sqrt{\gamma \log m}\,)\bigr)\bigr), \qquad \gamma > 0, \quad m \to \infty;$$

if $l = 3$, then we shall establish the formula

$$T_3(N, m, \lambda) = \frac{|K_s^D(N, m)|^3}{\varphi(m)} \cdot \left(1 + O\left(\exp\left(-\sqrt{\frac{\gamma \log m \, \log\log\log m}{\log\log m}}\,\right)\right)\right),$$
$$\gamma > 0, \quad m \to \infty,$$

where $|K_s^D(N, m)|$ is the number of elements in the set

$$K_s^D(N, m) = \{x \in K_s^D(N) : (x, m) = 1\}.$$

In the case $l = 2$, we obtain the following estimate:

$$T_2(N, m, \lambda) \ll \frac{|K_s^D(N)|^2}{\varphi(m)} \cdot m^\varepsilon, \qquad m \to \infty;$$

moreover, for the cardinality of the "exceptional set" (i.e., the set of λ's for which the congruence $x_1 x_2 \equiv \lambda \pmod m$ is unsolvable in numbers $x_j \in K_s^D(N)$), we obtain an upper bound of the form

$$O(\varphi(m) \cdot \exp(-\sqrt{\gamma \log m}\,)), \qquad \gamma > 0.$$

It should be particularly noted that, in the case of $m = p$, a prime, instead of the first two estimates given above, the following stronger result is valid:

$$T_l(N, p, \lambda) = \frac{|K_s^D(N, p)|^l}{p - 1} \cdot \bigl(1 + O(p^{-l/2+1+l\varepsilon})\bigr), \qquad l \geq 3,$$

for a sufficiently large σ, depending on ε, and, for the exceptional set in the binary problem with $m = p$, we shall have an estimate $O(p^\varepsilon)$.

Rigorous statements of the main results will be given in Sec. 6 (character sums) and Secs. 7, 8 (the numbers of solutions of congruences); in Secs. 2–5 we are concerned with the main definitions statements, and proofs of auxiliary assertions. Note that a number of results for the case in which $m = p$ is a prime were announced in [2]; however, there there are some inaccuracies in that paper (see the remarks after Corollary 3 of Theorem 3 in Sec. 7 of the present paper), while the proofs were only outlined. Here we present the complete proofs of all theorems. In contrast to [2], where Schmidt's lemma [3] was used, the proofs in the present paper are based on Konyagin's lemma [1, Lemma 1] (whose proof is, naturally, not given here; it, in turn, uses considerations from the paper [4] of P. Erdős, C. Mauduit, and A. Sarközy).

Note that, for small values of N (such that $K_s^D(N) \gg p^{1/2+\varepsilon}$), nontrivial estimates of character sums modulo a prime p can be obtained by applying Weil's estimates just as in [5]. A number of arithmetical properties of the sets (1) were obtained in [6]. In particular, the following asymptotic formula for the number of elements in the set was proved there:

$$K_s^D(N, m) = \{x \in K_s^D(N) : (x, m) = 1\};$$

this formula is also of interest to us (see the remark to Lemma 3 from Sec. 6). Besides, note that, as shown in [7], some results on the distribution of elements of the sets (1) modulo m can be obtained by studying the number of solutions of congruences of the form

$$x_1 + \cdots + x_l \equiv y_1 + \cdots + y_l \pmod m, \qquad x_j, y_j \in K_s^D(N).$$

Assertions from [7] can be proved by using theorems of the type of Plünnecke's inequality (see [8, Chap. 7]). Some results can be obtained by using Schmidt's classical approach [3].

2. FINITE FOURIER SERIES FOR CHARACTERS MODULO A COMPOSITE NUMBER

Suppose that

$$m = \prod_{1\le j\le t} p_j^{\alpha_j}$$

is the canonical expansion of a number m in prime factors. Let $\chi(x)$ be a character modulo m. Then, by the Chinese remainder theorem,

$$\chi(x) = \prod_{1\le j\le t} \chi_j(x),$$

where χ_j is a character modulo $p_j^{\alpha_j}$. We need the expansion of the character χ in the finite Fourier series

$$\chi(x) = \sum_{y=1}^{m} c_m(\chi, y) \exp\left(2\pi i \frac{xy}{m}\right).$$

Note that if the character $\chi = \chi_0$ is principal modulo m, then its Fourier coefficients are called the *Ramanujan sums* (see [9]) and can be calculated by the formula

$$c_m(\chi_0, y) = \frac{\mu(Y)\varphi(m)}{m\varphi(Y)},$$

where $\mu(\,\cdot\,)$ and $\varphi(\,\cdot\,)$ are the Möbius and Euler functions, respectively, and $Y = m/(m, y)$.

Consider the divisor

$$a \mid m, \qquad a = \prod_{1\le j\le t} p_j^{\beta_j}, \quad 0 \le \beta_j \le \alpha_j.$$

For this divisor, we define the following disjoint index sets:

$$\mathscr{J}_1 = \mathscr{J}_1(m, a) = \{j \mid 1 \le j \le t,\ \beta_j > 0\}, \qquad \mathscr{J}_2 = \mathscr{J}_2(m, a) = \{j \mid 1 \le j \le t,\ \beta_j = 0\}.$$

Suppose that

$$m = m_1 m_2, \qquad m_\nu = m_\nu(a) = \prod_{j\in\mathscr{J}_\nu} p_j^{\alpha_j}, \quad (m_1, a) = a, \quad (m_2, a) = 1. \tag{3}$$

Lemma 1. *The set of all characters modulo m splits into the disjunct union of sets*

$$\bigsqcup_{a\mid m} \Xi_a$$

such that Ξ_1 consists of one principal character modulo m, and the inclusion $\chi \in \Xi_a$, $a > 1$, implies that the character χ can be expressed as

$$\chi(x) = \chi^{(1)}(x) \cdot \chi^{(2)}(x),$$

where $\chi^{(1)}$ is a nonprincipal character modulo m_1; moreover,

$$\chi^{(1)}(x) = \sum_{\substack{1\le y\le a\\ a,y)=1}} c^{(1)}(y) \exp\left(2\pi i \frac{xy}{a}\right),$$

and, for each y, $|c^{(1)}(y)| = a^{-1/2}$, while $\chi^{(2)}(x)$ is a principal character modulo m_2. The cardinality of the sets Ξ_a satisfies the following relation:

$$|\Xi_a| = \sum_{d\mid a} \mu(d)\varphi\left(\frac{a}{d}\right) = \prod_{j=1}^{t} f(p_j^{\beta_j}), \qquad f(p^\beta) = \begin{cases} 1, & \beta = 0,\\ p-2, & \beta = 1,\\ p^{\beta-2}(p-1)^2, & \beta \ge 2. \end{cases} \tag{4}$$

Remark 1. Note that if $m_1 = 1$, then we can assume that Lemma 1 holds with $\chi^{(1)}(x) = 1$ for all x.

Remark 2. Naturally, in the case $m = p$, the assertion of Lemma 1 concerning the nonprincipal character implies the equality $|c_m(\chi, y)| = p^{-1/2}$ for any y coprime to p.

Remark 3. Obviously, the following inequality holds:

$$|\Xi_a| \le a \qquad \forall\, a \mid m. \tag{5}$$

Proof of Lemma 1. For the proof, see for example, in [10, pp. 349–355, Sec. 9, Appendix] □

Note that, in the expansions $\chi = \chi^{(1)}\chi^{(2)}$, the characters $\chi^{(1)}$ from the set Ξ_a are nonprincipal *primitive* characters modulo a. If χ is a nonprincipal character modulo m, then in order to understand for which a the inclusion $\chi \in \Xi_a$ is satisfied, we must express χ as $\chi = \chi^{(1)}\chi^{(2)}$, where $\chi^{(2)}$ is a principal character modulo m_2 and $\chi^{(1)}$ is a character modulo m_1 ($m = m_1m_2$, $(m_1, m_2) = 1$) such that it is a character modulo a (here a is a divisor of the number m_1), but is not a character modulo any number less than the modulus of $a' \mid a$.

3. ON TRIGONOMETRIC SUMS

Let us consider trigonometric sums of the form

$$S_{d,w} = \sum_{\substack{1\le y\le d\\ y,d)=1}} \left| \sum_{x\in K_s^D(s^w)} \exp\left(2\pi i \frac{xy}{d}\right)\right|, \qquad S_{d,w}(\chi, b) = \sum_{\substack{1\le y\le d\\ y,d)=1}} \left| \sum_{x\in K_s^D(s^w)} \chi(x+b)\exp\left(2\pi i \frac{xy}{d}\right)\right|,$$

where χ is a character modulo m.

In what follows we assume that r is a natural number chosen from the condition

$$s^{r-1} \le m < s^r. \tag{6}$$

Our main instrument is the following lemma proved by Konyagin.

Lemma 2 (see [1, Lemma 1]). *Suppose that $m \ge s$. Given some positive constants $\gamma_\nu = \gamma_\nu(s)$, $\nu = 1, 2$, the following estimate holds for $w \ge 2r$:*

$$\sum_{d\le m} S_{d,w} \le |K_s^D(s^w)|\left(\exp\left(\gamma_1 \cdot \frac{\log m}{\exp(\gamma_2 w/\log m)}\right) - 1\right).$$

Remark. Lemma 2 is a direct restatement of a result from [1], where the condition $m \ge s$ is required. However, it is obvious that Lemma 2 also holds for any $m \ge 2$ with a somewhat larger γ_1 and the replacement of the sign '$\le$' by '$\ll$'.

4. ESTIMATES OF AUXILIARY QUANTITIES

Let us choose a positive ε. In what follows, we assume that σ is sufficiently large, i.e., $\sigma \ge \sigma_0(s, \varepsilon)$ and $w \ge \sigma r$.

For the divisor $a \mid m$, we consider the numbers $m_\nu = m_\nu(a)$ defined by (3), set $\overline{m_2} = \max\{m_2, 3\}$, and define the quantities

$$R_w^1(m, a) = \frac{\log\log \overline{m_2}}{a^{1/2}} \sum_{2\le q\le m_2} \frac{1}{q^2} \cdot \left(\exp\left(\frac{\gamma_1 \log aq}{\exp(\gamma_2 w/\log aq)}\right) - 1\right), \tag{7}$$

$$R_w^2(m, a) = \frac{\log\log \overline{m_2}}{a^{1/2}m_2}\left(\exp\left(\frac{\gamma_1 \log am_2}{\exp(\gamma_2 w/\log am_2)}\right) - 1\right) \tag{8}$$

(note that if $a=1$, then $m_2=m$),

$$R_w^3(m,a)=\frac{\varphi(m_2)}{a^{1/2}m_2}\left(\exp\left(\frac{\gamma_1\log a}{\exp(\gamma_2 w/\log a)}\right)-1\right) \tag{9}$$

(this value is defined only for $a>1$) and

$$\Delta_w(m,a)=R_w^1(m,a)+R_w^2(m,a)+R_w^3(m,a). \tag{10}$$

For a prime $a=m=p$, $m_2=1$, and from the definition of R_w^j for $\sigma\ge\sigma_0(s,\varepsilon)$ and $w\ge\sigma r$, the following inequality holds:

$$\Delta_w(p,p)\ll p^{-1/2+\varepsilon}. \tag{11}$$

For estimates in the general case, we need the inequality

$$\exp\left(\frac{\xi}{\exp(b/\xi)}\right)-1\ll\frac{\xi}{\exp(b/\xi)}\qquad\text{for}\quad 0\le\xi\le\frac{b}{\log b} \tag{12}$$

and the relation

$$\max_{\xi:\xi\ge c}\exp\left(-\log\xi-\frac{b}{\log\xi}\right)=\begin{cases}\exp(-2\sqrt{b}\,) & \text{if } c\le\exp(\sqrt{b}\,),\\ \dfrac{1}{c\cdot\exp(b/\log c)} & \text{if } c\ge\exp(\sqrt{b}\,).\end{cases} \tag{13}$$

Let us estimate $R_w^1(m,a)$. First, for q from the corresponding domain of summation, we have $aq\le am_2\le m$ and, therefore,

$$\frac{\gamma_2 w}{\log qm_2}\ge\frac{\gamma_2 w}{\log m}\ge\frac{\gamma_2\sigma}{\log s}.$$

Thus, for a sufficiently large σ, the following inequality is satisfied:

$$\frac{\gamma_1}{\exp(\gamma_2 w/\log am_2)}\le\varepsilon$$

(we have used the definition of w from the beginning of this section and the definition of r from condition (6)). Since the series $\sum_q q^{-2+\varepsilon}$ is obviously convergent for small values of ε, the following estimate always holds:

$$R_w^1(m,a)\ll\frac{\log\log\overline{m_2}}{a^{1/2-\varepsilon}}. \tag{14}$$

Second, denoting

$$E=\exp\left(\frac{\gamma_2 w}{\log\gamma_1\gamma_2 w}\right),$$

we write

$$\sum_{2\le q\le m_2}\frac{1}{q^2}\cdot\left(\exp\left(\frac{\gamma_1\log aq}{\exp(\gamma_2 w/\log aq)}\right)-1\right)=\sum_{q\le E/a}+\sum_{q>E/a}.$$

Arguing in the same way as in the derivation of estimate (14), we see that

$$\sum_{q>E/a}\le\sum_{q>E/a}q^{-2+\varepsilon}a^{\varepsilon}=O\left(\frac{a}{E^{1-\varepsilon}}\right).$$

If we now have

$$a\le E^{1/3}=\exp\left(\frac{\gamma_2 w}{3\,\log\gamma_1\gamma_2 w}\right),$$

then, for a sufficiently large σ (sufficiently small ε), we obtain

$$R_w^1(m,a) \ll \frac{\log\log \overline{m_2}}{a^{1/2}}\biggl(\sum_{2\le q\le E/a}\frac{1}{q^2}\cdot\biggl(\exp\biggl(\frac{\gamma_1\log aq}{\exp(\gamma_2 w/\log aq)}\biggr)-1\biggr)+O(E^{-1/3})\biggr);$$

moreover, we can apply inequality (12) (where we set $\xi=\gamma_1\log aq$ and $b=\gamma_1\gamma_2 w$) to each summand of the sum over q. For a given positive Q, we have the following estimate:

$$\begin{aligned}R_w^1(m,a) &\ll \frac{\log\log \overline{m_2}}{a^{1/2}}\biggl(\sum_{q\le m_2}\frac{1}{q^2}\cdot\frac{\log aq}{\exp(\gamma_2 w/\log aq)}+O(E^{-1/3})\biggr)\\ &\ll \frac{\log m\,\log\log \overline{m_2}}{a^{1/2}}\biggl(\frac{1}{\exp(\gamma_2 w/\log aQ)}\cdot\sum_{q\le Q}\frac{1}{q^2}+\sum_{q>Q}\frac{1}{q^2}+O(E^{-1/3})\biggr)\\ &\ll \frac{\log m\,\log\log \overline{m_2}}{a^{1/2}}\biggl(\frac{1}{\exp(\gamma_2 w/\log aQ)}+\frac{1}{Q}+O(E^{-1/3})\biggr).\end{aligned}$$

Optimally, the value of Q can be chosen from the condition

$$\exp\biggl(\frac{\gamma_2 w}{\log aQ}\biggr)=Q, \tag{15}$$

i.e., $\log Q=(\sqrt{\log^2 a+4\gamma_2 w}-\log a)/2$. Then we obtain

$$R_w^1(m,a)\ll\frac{\log m\,\log\log \overline{m_2}}{a^{1/2}}\biggl(\frac{1}{\exp((\sqrt{\log^2 a+4\gamma_2 w}-\log a)/2)}+O(E^{-1/3})\biggr).$$

In the case $a\le E^{1/3}$ under study, consider two more possibilities. First, if $a\le\exp(\sqrt{\gamma_2 w/2}\,)$, then

$$\frac{1}{2}(\sqrt{\log^2 a+4\gamma_2 w}-\log a)\ge\sqrt{\frac{\gamma_2 w}{2}},$$

$$R_w^1(m,a)\ll\frac{\log m\,\log\log \overline{m_2}}{a^{1/2}}\biggl(\frac{1}{\exp(\sqrt{\gamma_2 w/2}\,)}+O(E^{-1/3})\biggr)\ll\frac{\log m\,\log\log \overline{m_2}}{a^{1/2}\exp(\sqrt{\gamma_2 w/2}\,)}.$$

(Here we can discard terms $O(E^{-1/3})$, which obviously follows from the definition of E.)

Second, if $a\ge\exp(\sqrt{\gamma_2 w/2}\,)$, then

$$\log aQ=\log a+\log Q=\frac{\sqrt{\log^2 a+4\gamma_2 w}+\log a}{2}.$$

Since Q satisfies (15), we have

$$R_w^1(m,a)\ll\frac{\log m\,\log\log \overline{m_2}}{a^{1/2}}\biggl(\frac{1}{\exp(\gamma_2 w/\log aQ)}+O(E^{-1/3})\biggr)\ll\frac{\log m\,\log\log \overline{m_2}}{a^{1/2}\exp(\gamma_2 w/(2\,\log a))}.$$

(Here we can discard terms $O(E^{-1/3})$, which follows from the inequality

$$\exp\biggl(\frac{\gamma_2 w}{\log aQ}\biggr)\le\exp\biggl(\frac{\gamma_2 w}{\log a}\biggr)\le\exp(\sqrt{\gamma w}\,)$$

with some positive γ.)

Let us write the resulting inequalities for $R_w^1(m,a)$ in the convenient form

$$R_w^1(m,a)\ll\begin{cases}\dfrac{\log\log \overline{m_2}}{a^{1/2-\varepsilon}} & \text{if } a\ge\exp\biggl(\dfrac{\gamma_2 w}{3\,\log\gamma_1\gamma_2 w}\biggr),\\ \dfrac{\log m\,\log\log \overline{m_2}}{a^{1/2}\exp(\gamma_2 w/(2\,\log a))} & \text{if } \exp\biggl(\sqrt{\dfrac{\gamma_2 w}{2}}\biggr)\le a\le\exp\biggl(\dfrac{\gamma_2 w}{3\,\log\gamma_1\gamma_2 w}\biggr),\\ \dfrac{\log m\,\log\log \overline{m_2}}{a^{1/2}\exp(\sqrt{\gamma_2 w/2}\,)} & \text{if } a\le\exp\biggl(\sqrt{\dfrac{\gamma_2 w}{2}}\biggr).\end{cases} \tag{16}$$

Now we estimate $R_w^2(m,a)$. First, we again have $am_2 \le m$, and hence

$$\frac{\gamma_2 w}{\log am_2} \ge \frac{\gamma_2 w}{\log m} \ge \frac{\gamma_2 \sigma}{\log s}.$$

Therefore, for a sufficiently large σ, we again have

$$\frac{\gamma_1}{\exp(\gamma_2 w/\log am_2)} \le \frac{\varepsilon}{2},$$

and the following estimate always holds:

$$R_w^2(m,a) \ll \frac{\log\log \overline{m_2}}{a^{1/2}m_2}\cdot (am_2)^{\varepsilon/2} \ll \frac{1}{a^{1/2-\varepsilon}m_2^{1-\varepsilon}}.$$

If

$$am_2 \le \exp\biggl(\frac{\gamma_2 w}{\log \gamma_1\gamma_2 w}\biggr),$$

then we can apply inequality (12) and obtain the estimate

$$\begin{aligned} R_w^2(m,a) &\ll \frac{\log\log \overline{m_2}}{a^{1/2}m_2}\cdot \frac{\log am_2}{\exp(\gamma_2 w/\log am_2)} \\ &\ll a^{1/2}\log m\,\log\log \overline{m_2}\cdot \max_{\xi:\xi\ge a}\exp\biggl(-\log\xi - \frac{\gamma_2 w}{\log \xi}\biggr) \end{aligned}$$

(here we have used again the inequality $am_2 \le m$ and taken $\xi = am_2$ and $b = \gamma_2 w$). In this case, we additionally consider two subcases, depending on where the maximum in formula (13) is attained. If, besides this inequality, we also have $a \ge \exp(\sqrt{\gamma_2 w}\,)$, then

$$R_w^2(m,a) \ll \frac{\log m\,\log\log \overline{m_2}}{a^{1/2}\exp(\gamma_2 w/\log a)}.$$

But if $a \le \exp(\sqrt{\gamma_2 w}\,)$, then

$$R_w^2(m,a) \ll \frac{a^{1/2}\log m\,\log\log \overline{m_2}}{\exp(2\cdot \gamma_2 w/\log a)} \le \frac{\log m\,\log\log \overline{m_2}}{\exp(\frac{3}{2}\cdot \sqrt{\gamma_2 w}\,)}.$$

Thus, to summarize, we write the resulting estimates in the convenient form

$$R_w^2(m,a) \ll \begin{cases} a^{-1/2+\varepsilon}m_2^{-1+\varepsilon} & \text{if } am_2 \ge \exp\biggl(\dfrac{\gamma_2 w}{\log \gamma_1\gamma_2 w}\biggr), \\ \dfrac{1}{a^{1/2}\exp(\gamma_2 w/\log a)} & \text{if } am_2 \le \exp\biggl(\dfrac{\gamma_2 w}{\log \gamma_1\gamma_2 w}\biggr),\ a \ge \exp(\sqrt{\gamma_2 w}\,), \\ \exp\biggl(-\dfrac{3}{2}\cdot\sqrt{\gamma_2 w}\biggr) & \text{if } am_2 \le \exp\biggl(\dfrac{\gamma_2 w}{\log \gamma_1\gamma_2 w}\biggr),\ a \le \exp(\sqrt{\gamma_2 w}\,). \end{cases} \tag{17}$$

Now let us estimate $R_w^3(m,a)$, which is easier as compared to the two previous quantities, because the argument of its exponential does not contain m_2. Just as above, for a sufficiently large σ and any a, the following estimate holds:

$$R_w^3(m,a) \ll a^{-1/2+\varepsilon},$$

while, for $a \le \exp(\gamma_2 w/\log\gamma_1\gamma_2 w)$, from inequality (12) we obtain

$$R_w^3(m,a) \ll \frac{\log a}{a^{1/2}}\cdot\frac{1}{\exp(\gamma_2 w/\log a)}.$$

Let us combine these two inequalities:

$$R_w^3(m,a) \ll \begin{cases} a^{-1/2+\varepsilon} & \text{if } a \ge \exp\biggl(\dfrac{\gamma_2 w}{\log \gamma_1\gamma_2 w}\biggr), \\ \dfrac{\log a}{a^{1/2}}\cdot\dfrac{1}{\exp(\gamma_2 w/\log a)} & \text{if } a \le \exp\biggl(\dfrac{\gamma_2 w}{\log \gamma_1\gamma_2 w}\biggr). \end{cases} \tag{18}$$

We can easily see from (16)–(18) that, in the case under consideration, the following inequality always holds for $a > 1$:

$$\Delta_w(m,a) \ll \exp(-\sqrt{\gamma w}\,), \qquad \gamma > 0. \tag{19}$$

A more detailed analysis of formulas (16)–(18) shows that, for $\Delta_w(m,a)$, the same estimates hold as for $R_w^1(m,a)$:

$$\Delta_w(m,a) \ll \begin{cases} \dfrac{\log\log \overline{m_2}}{a^{1/2-\varepsilon}} & \text{if } a \ge \exp\left(\dfrac{\gamma_2 w}{3\,\log\gamma_1\gamma_2 w}\right), \\ \dfrac{\log m\,\log\log \overline{m_2}}{a^{1/2}\exp(\gamma_2 w/(2\,\log a))} & \text{if } \exp\left(\sqrt{\dfrac{\gamma_2 w}{2}}\right) \le a \le \exp\left(\dfrac{\gamma_2 w}{3\,\log\gamma_1\gamma_2 w}\right), \\ \dfrac{\log m\,\log\log \overline{m_2}}{a^{1/2}\exp(\sqrt{\gamma_2 w/2}\,)} & \text{if } a \le \exp\left(\sqrt{\dfrac{\gamma_2 w}{2}}\right). \end{cases} \tag{20}$$

Now, for a natural number l, we consider the quantity

$$\Delta_w^l(m) = \sum_{a|m,\,a>1} |\Xi_a| \left(\Delta_w(m,a) + \frac{1}{m}\right)^l \le \sum_{a|m,\,a>1} a \cdot \left(\Delta_w(m,a) + \frac{1}{m}\right)^l \tag{21}$$

(we have already taken (5) into account) and try to obtain an upper bound for it by using the inequalities for $\Delta_w(m,a)$.

In the easiest case of a prime $m = p$, we immediately obtain the estimate

$$\Delta_w^l(p) \ll p^{-l/2+1+l\varepsilon} \tag{22}$$

for a sufficiently large $\sigma \ge \sigma_1(s,\varepsilon)$.

Besides, note that if the minimal divisor a_0, not equal to 1, of the number m turns out to be greater than $\exp(\gamma_2 w/\log\gamma_1\gamma_2 w)$, then (since the number of divisors of m is at most $\exp(\log m/\log\log m)$) for a sufficiently large $\sigma \ge \sigma_2(s,\varepsilon)$ and $w \ge \sigma r$, we obtain

$$\Delta_w^l(p) \ll a_0^{-l/2+1+(l+1)\varepsilon}. \tag{23}$$

Let us dwell on the case of an arbitrary m for $l \ge 2$. First, note that

$$\Delta_w^l(m) \le 2^l \sum_{a|m,\,a>1} a \cdot \max\left((\Delta_w(m,a))^l, \frac{1}{m^l}\right) \le 2^l \sum_{a|m,\,a>1} a \cdot \left((\Delta_w(m,a))^l + \frac{1}{m^l}\right).$$

Thus,

$$\Delta_w^l(m) \ll \overline{\Delta}_w^l(m) + \sum_{a|m,\,a>1} \frac{a}{m^l}, \qquad \text{where} \quad \overline{\Delta}_w^l(m) = \sum_{a|m,\,a>1} a \cdot (\Delta_w(m,a))^l.$$

Since, for $l \ge 3$,

$$\sum_{a|m,\,a>1} \frac{a}{m^l} \le \frac{1}{m}$$

and, for $l = 2$,

$$\sum_{a|m,\,a>1} \frac{a}{m^2} \le 1,$$

our problem can be reduced to the derivation of an upper bound for $\overline{\Delta}_w^l(m)$.

We split the sum in the definition of $\overline{\Delta}_w^l(m)$ into three parts:

$$\overline{\Delta}_w^l(m) = \sum_{a|m,\,a>1} a \cdot (\Delta_w(m,a))^l = \Sigma^1 + \Sigma^2 + \Sigma^3, \qquad \Sigma^1 = \sum_{a > \exp(\gamma_2 w/(3\,\log\gamma_1\gamma_2 w))},$$

$$\Sigma^2 = \sum_{\exp(\sqrt{\gamma_2 w/2})<a\le\exp(\gamma_2 w/(3\,\log\gamma_1\gamma_2 w))}, \qquad \Sigma^3 = \sum_{a\le\exp(\sqrt{\gamma_2 w/2})}.$$

First, let us estimate the sums Σ^1 and Σ^3. For $l\ge 3$, $l\varepsilon+1\le l/2$, we have

$$\Sigma^1 \ll (\log\log m)^l\cdot\exp\biggl(\Bigl(-\frac{l}{2}+1+l\varepsilon\Bigr)\cdot\frac{\gamma_2 w}{3\,\log\gamma_1\gamma_2 w}\biggr)\cdot\sum_{a|m}1\ll\exp\biggl(-\frac{\gamma w}{\log w}\biggr)$$

with some positive constant γ for a sufficiently large $\sigma>\sigma_3(s,l)$ (here we used the first estimate from (20) and the inequality $\sum_{a|m}1\ll\exp(\log m/\log\log m)$). Also, for $l\ge 2$, we have

$$\Sigma^3\ll(\log m\,\log\log m)^l\cdot\exp\biggl(-l\cdot\sqrt{\frac{\gamma_2 w}{2}}\biggr)\cdot\sum_{a\le\exp(\sqrt{\gamma_2 w/2})}1\ll\exp(-\sqrt{\gamma w}\,)$$

with some positive constant γ (here we used the third estimate from (20)).

The most difficult task is to obtain an estimate of the sum Σ^2. Here we must use the inequality

$$\sum_{a|m}\frac{1}{a^\rho}\le\exp\biggl(\gamma(\rho)\frac{(\log m)^{1-\rho}}{\log\log m}\biggr)\ll\exp\biggl(\gamma(\rho)\frac{r^{1-\rho}}{\log r}\biggr),\tag{24}$$

which holds for each $\rho\in(0,1)$ with some positive constant $\gamma(\rho)$ uniformly bounded for ρ bounded away from zero and unity. The estimates of this sum with $\rho=0,1$, which were used by us earlier, can be found, for example, in [9]. Estimate (24) given above seems to be a known one, but the authors could not find the appropriate reference and, for completeness, present the proof of inequality (24) in Sec. 5.

If $l\ge 4$, by using the second estimate from (20) and (24) for $\rho=1/2$ and, taking into account the fact that

$$a\cdot\frac{1}{a^{l/2}}\le\frac{1}{a}\le\frac{1}{\exp(\sqrt{\gamma_2 w/2}/2)}\cdot\frac{1}{a^{1/2}}$$

and that $w\ge\sigma r$, we obtain the estimate

$$\Sigma^2\ll\frac{(\log m\,\log\log m)^l}{\exp(\sqrt{\gamma_2 w/2}/2)}\cdot\sum_{a|m}\frac{1}{a^{1/2}}\ll\exp\biggl(\Bigl(-\frac12+\varepsilon\Bigr)\cdot\sqrt{\frac{\gamma_2 w}{2}}+\gamma(1/2)\frac{r^{1/2}}{\log r}\biggr)\ll\exp(-\sqrt{\gamma w}\,).$$

Note that, in the second inequality of estimate (20), we did not use the additional multiplier $\exp(\gamma_2 w/(2\,\log a))$ (in the denominator) and estimated it by 1.

Thus, for $l\ge 4$, we can write

$$\Delta_w^l(m)\ll\exp(-\sqrt{\gamma w}\,),\qquad\gamma>0.\tag{25}$$

But if $l=3$, then, choosing

$$Q_1=\exp\biggl(\sqrt{\frac{\gamma_2 w\,\log r}{\log\log r}}\biggr)>\exp\biggl(\sqrt{\frac{\gamma_2 w}{2}}\biggr)$$

and again invoking the second formula from (20), we obtain

$$\Sigma^2\ll(\log m\,\log\log m)^3\times\biggl(\sum_{a|m,\,a\le Q_1}\frac{1}{a^{1/2}\exp(3\gamma_2 w/(2\,\log a))}+\sum_{a|m,\,a>Q_1}\frac{1}{a^{1/2}\exp(3\gamma_2 w/(2\,\log a))}\biggr).$$

Note that here the presence of the multiplier $\exp(3\gamma_2 w/(2\,\log a))$ in the denominator of the second formula from (20) is now essential.

Applying (24) with $\rho = 1/2$ and using the inequality $w > \sigma r$, we obtain the following estimate with some positive γ:

$$\sum_{a|m,\, a\le Q_1} \ll \exp\biggl(-\frac{\gamma_2 w}{\log Q_1}\biggr)\cdot\sum_{a|m}\frac{1}{a^{1/2}}$$
$$\ll \exp\biggl(-\sqrt{\frac{\gamma_2 w\,\log\log r}{\log r}}+\gamma\biggl(\frac12\biggr)\cdot\frac{\sqrt{r}}{\log r}\biggr)\ll \exp\biggl(-\sqrt{\frac{\gamma w\,\log\log r}{\log r}}\,\biggr).$$

Further, choosing

$$\delta=\frac{\log\log r}{2\,\log r}$$

and applying (24) with $\rho = 1/2-\delta$, we see that the following estimate is satisfied with some positive γ:

$$\sum_{a|m,\, a> Q_1} \ll \frac{1}{Q_1^{\delta}}\cdot\sum_{a|m}\frac{1}{a^{1/2-\delta}}$$
$$\ll \exp\biggl(-\delta\cdot\sqrt{\frac{\gamma_2 w\,\log r}{\log\log r}}+\gamma\biggl(\frac12-\delta\biggr)\frac{r^{1/2+\delta}}{\log r}\biggr)\ll \exp\biggl(-\sqrt{\frac{\gamma w\,\log\log r}{\log r}}\,\biggr),$$

because

$$\delta\cdot\sqrt{\frac{\gamma_2 w\,\log r}{\log\log r}}=\sqrt{\frac{\gamma_2 w\,\log\log r}{4\,\log r}}\ge\sqrt{\frac{\gamma_2\sigma r\,\log\log r}{4\,\log r}}\ge\sqrt{\frac{r}{\log r}}=\frac{r^{1/2+\delta}}{\log r}.$$

Thus, for $l=3$, we obtain

$$\Delta_w^3(m)\ll\exp\biggl(-\sqrt{\frac{\gamma w\,\log\log r}{\log r}}\,\biggr),\qquad \gamma>0. \tag{26}$$

But if $l=2$, then, for $\varepsilon>0$ for $\sigma\ge\sigma_5(s,\varepsilon)$, we have

$$\Delta_w^2(m)\ll m^{\varepsilon}. \tag{27}$$

Besides, note that if the number of divisors m is at most $\exp(\sqrt{\log m}\,)$, then, for $l\ge 3$, the following estimate holds:

$$\Delta_w^l(m)\ll\exp(-\sqrt{\gamma w}\,),\qquad \gamma>0. \tag{28}$$

5. PROOF OF FORMULA (24)

Suppose that $m=p_1^{\alpha_1}\cdots p_t^{\alpha_t}$, $p_1<\cdots<p_t$, is the canonical expansion of a number m in primes. If $q_1<\cdots<q_t$ are the first t primes, then $q_j\asymp j\,\log j$, $p_j\ge q_j$, and it is clear that $t\ll\log m/\log\log m$. Let us estimate the following sum:

$$\sum_{a|m}a^{-\rho}=\sum_{\beta_1,\dots,\beta_t=0}^{\alpha_1,\dots,\alpha_t}p_1^{-\rho\beta_1}\cdots p_t^{-\rho\beta_t}\le\sum_{\beta_1=0}^{\alpha_1}\cdots\sum_{\beta_t=0}^{\alpha_t}q_1^{-\rho\beta_1}\cdots q_t^{-\rho\beta_t}$$
$$=\prod_{j=1}^{t}\sum_{\beta_j=0}^{\alpha_j}q_j^{-\rho\beta_j}\le\prod_{j=1}^{t}\sum_{\beta=0}^{\infty}q_j^{-\rho\beta}=\prod_{j=1}^{t}(1-q_j^{-\rho})^{-1},$$

$$\log\sum_{a|m}a^{-\rho}\le-\sum_{j=1}^{t}\log(1-q_j^{-\rho})\le 2^{\rho}\log\bigl((1-2^{-\rho})^{-1}\bigr)\cdot\sum_{j=1}^{t}q_j^{-\rho}$$

$$\ll 2^{\rho}\log\bigl((1-2^{-\rho})^{-1}\bigr)\cdot\sum_{j=2}^{t}(j\ \log j)^{-\rho}$$
$$\ll 2^{\rho}\log\bigl((1-2^{-\rho})^{-1}\bigr)\cdot(1-\rho)^{-1}\cdot t^{1-\rho}(\log t)^{-\rho}$$
$$\ll 2^{\rho}\log\bigl((1-2^{-\rho})^{-1}\bigr)\cdot(1-\rho)^{-1}\cdot(\log m)^{1-\rho}(\log\log m)^{-1}.$$

Formula (24) is proved.

6. ON CHARACTER SUMS

Lemma 3. *Suppose that $a \mid m$, $\chi(x) \in \Xi_a$ is a character modulo m, the number m_2 defined by* (3) *is greater than* 1 *and $\chi^{(1)}$ from Lemma 1. Then the error R in the formula*

$$\sum_{x\in K_s^D(s^w)}\chi(x+b)=\sum_{\substack{x\in K_s^D(s^w)\\ x+b,m_2)=1}}\chi^{(1)}(x+b)=\frac{\varphi(m_2)}{m_2}\cdot\sum_{x\in K_s^D(s^w)}\chi^{(1)}(x+b)+R$$

satisfies the following estimate:

$$|R|\ll|K_s^D(s^w)|\cdot\bigl(R_w^1(m,a)+R_w^2(m,a)\bigr),$$

where the quantities $R_w^{1,2}(m,a)$ are defined in the previous section in (7), (8).

Remark. Obviously, the sum $R_w^1(m,a)+R_w^2(m,a)$, can be estimated from above via $\Delta_w(m,a)$. If $m_2=1$, then, obviously, $R=0$. But if χ is a principal character modulo m, then $a=1$, $m_2=m$ and, in view of Remark 1 to Lemma 1 and the third estimate from (20), Lemma 3 implies the following formula for $w\ge\sigma r$:

$$|K_s^D(s^w,m)|=\frac{\varphi(m)}{m}\cdot|K_s^D(s^w)|\cdot\left(1+O\left(\exp\left(-\sqrt{\frac{\gamma_2 w}{2}}\right)\cdot\log m\ \log\log m\right)\right);\qquad(29)$$

This formula, practically, can be found in [6].

Proof of Lemma 3. Everywhere in the proof of Lemma 3, in the summation over $d \mid m_2$ and $q \mid m_2$, we assume that $d,q>1$:

$$|R|\le\sum_{d|m_2}\left|\sum_{\substack{x\in K_s^D(s^w)\\ x+b\equiv 0\ (\mathrm{mod}\,d)}}\chi^{(1)}(x+b)-\frac{1}{d}\cdot\sum_{x\in K_s^D(s^w)}\chi^{(1)}(x+b)\right|$$
$$=\sum_{d|m_2}\frac{1}{d}\left|\sum_{1\le z\le d-1}\sum_{x\in K_s^D(s^w)}\chi^{(1)}(x+b)\exp\left(2\pi i\frac{z(x+b)}{d}\right)\right|$$
$$\le\sum_{d|m_2}\frac{1}{d}\sum_{q|d}S_{q,w}(\chi^{(1)},b)\le\sum_{q|m_2}\left(\sum_{d|m_2,\,q|d}\frac{1}{d}\right)S_{q,w}(\chi^{(1)},b)\ll\log\log\overline{m_2}\cdot\sum_{q|m_2}\frac{S_{q,w}(\chi^{(1)},b)}{q}.$$

Now, using Lemma 1, the definition of the sums $S_{q,w}(\chi,b)$, $S_{q,w}$, the relation $(q,a)=1$ (see (3)), and the Abel transformation, we obtain

$$|R|\ll a^{-1/2}\log\log\overline{m_2}\cdot\sum_{q|m_2}\frac{1}{q}\sum_{\substack{1\le y\le a\\ a,y)=1}}\sum_{\substack{1\le z\le q\\ z,q)=1}}\left|\sum_{x\in K_s^D(s^w)}\exp\left(2\pi i\left(\frac{zx}{q}+\frac{yx}{a}\right)\right)\right|$$
$$=a^{-1/2}\cdot\log\log\overline{m_2}\cdot\sum_{q|m_2}\frac{S_{aq,w}}{q}\le a^{-1/2}\cdot\log\log\overline{m_2}\cdot\sum_{2\le q\le m_2}\frac{S_{aq,w}}{q}$$
$$\ll a^{-1/2}\log\log\overline{m_2}\cdot\left(\sum_{2\le q\le m_2}\frac{1}{q^2}\sum_{d\le q}S_{ad,w}+\frac{1}{m_2}\sum_{d\le m_2}S_{ad,w}\right)$$

$$\le a^{-1/2}\log\log\overline{m_2}\cdot\biggl(\sum_{2\le q\le m_2}\frac{1}{q^2}\sum_{d\le aq}S_{d,w}+\frac{1}{m_2}\sum_{d\le am_2}S_{d,w}\biggr).$$

Now, using Lemma 2 and the definition of the quantities $R_w^{1,2}(m,a)$ (see (7), (8)), we conclude the proof of Lemma 3. □

Theorem 1. *Suppose that we are given $\varepsilon>0$ and $w\ge\sigma r$, where $\sigma\ge\sigma_0(s,\varepsilon)$ is sufficiently large. Suppose that, for a natural number m, we are given the divisor $a\mid m$ and a nonprincipal character $\chi(x)$ modulo m such that $\chi\in\Xi_a$, $a>1$. Then the following upper bound for the character sum is valid:*

$$\biggl|\sum_{x\in K_s^D(s^w)}\chi(x+b)\biggr|\ll|K_s^D(s^w)|\cdot\Delta_w(m,a),$$

where the value $\Delta_w(m,a)$ is defined by (10).

Proof. By Lemma 3, it suffices to estimate the sum

$$\Sigma=\sum_{x\in K_s^D(s^w)}\chi^{(1)}(x+b). \tag{30}$$

Applying Lemma 1, we see that

$$|\Sigma|\ll a^{-1/2}\cdot S_{a,w}\le a^{-1/2}\cdot\sum_{d\le a}S_{d,w}.$$

Further, let us use Lemma 2 and obtain the estimate

$$|\Sigma|\ll|K_s^D(s^w)|\cdot\frac{1}{a^{1/2}}\cdot\biggl(\exp\biggl(\frac{\gamma_1\log a}{\exp(\gamma_2 w/\log a)}\biggr)-1\biggr).$$

Theorem 1 immediately follows from the last estimate, the definition of the quantities $R_w^j(m,a)$, $\Delta_w(m,a)$, formulas (7)–(10), and the estimate given by Lemma 3. □

Remark. The required estimate of the sum (30) can be found by applying Schmidt's approach from [3] (just as in [2]) rather than using Lemma 4 from Konyagin's paper [1]. The inequality

$$S_{a,w}\le\sum_{d\le a}S_{d,w}$$

used in the proof of Theorem 1 seems rather rough, at first glance, but is, nevertheless, sufficiently sharp.

Theorem 2. *Suppose that $N\ge s^{w+\rho}$ and the assumptions of Theorem 1 are satisfied. Then the following estimate holds:*

$$\biggl|\sum_{x\in K_s^D(N)}\chi(x+b)\biggr|\le|K_s^D(N)|\cdot\bigl(\Delta_w(m,a)+(k+1)^{-\rho}\bigr).$$

Proof. Suppose that $s^\beta\le N<s^{\beta+1}$. Let us express N in the base s number system: $N=\mu_0+\cdots+\mu_\beta s^\beta$. We split the set $K_s^D(N)=\Omega_1\sqcup\Omega_2$, where Ω_1 consists of numbers $n=\eta_0+\cdots+\eta_\beta s^\beta$ for which $\eta_j=\mu_j$, $w\le j\le\beta$, while Ω_2 consists of all the other numbers. Obviously, $|\Omega_1|\le(k+1)^w$. The additional set can be expressed as the sum of the sets

$$\Omega_2=K_s^D(s^w)+s^w\cdot K_s^D(N_1),\qquad\text{where}\quad N_1=\mu_w+\mu_{w+1}s+\cdots+\mu_\beta s^{\beta-w}.$$

Therefore,

$$|\Omega_2|=|K_s^D(s^w)|\cdot|K_s^D(N_1)|\le|K_s^D(N)|$$

and

$$\begin{aligned}\left|\sum_{x\in K_s^D(N)}\chi(x+b)\right| &\le \left|\sum_{x\in\Omega_1}\chi(x+b)\right| + \left|\sum_{x\in\Omega_2}\chi(x+b)\right| \\ &\le (k+1)^w + \left|\sum_{b_1\in K_s^D(N_1)}\sum_{x\in K_s^D(s^w)}\chi(x+b+s^w b_1)\right| \\ &\le (k+1)^w + \sum_{b_1\in K_s^D(N_1)}\left|\sum_{x\in K_s^D(s^w)}\chi(x+b+s^w b_1)\right| \\ &\le (k+1)^w + |K_s^D(N)|\Delta_w(m,a)\end{aligned}$$

(we have used Theorem 1). It remains to note that

$$|K_s^D(N)| \ge |K_s^D(s^{w+\rho})| \ge (k+1)^{w+\rho} \qquad \text{and} \qquad (k+1)^w \le |K_s^D(N)|/(k+1)^\rho.$$

The theorem is proved. □

Remark 4. Let us recall that, under the assumptions of Theorem 1, it is required that $w \ge \sigma r$. If, moreover, we require that

$$\rho \ge \sigma^* r \frac{\log s}{\log(k+1)},$$

we see that the condition $N \ge s^{w+\rho}$, which is equivalent to

$$N \gg m^{\sigma+(\log s/\log(k+1))\sigma^*},$$

implies

$$\left|\sum_{x\in K_s^D(N)}\chi(x+b)\right| \le |K_s^D(N)|\cdot\big(\Delta_w(m,a) + O(m^{-\sigma^*})\big).$$

Remark 5. It can be shown that the principal character modulo m for the number $N \ge m^\sigma$ satisfies a formula similar to (29); however, in what follows, we shall only need the simple inequality

$$|K_s^D(N)| \ll |K_s^D(N,m)|\cdot\frac{m}{\varphi(m)}$$

(exceptionally to state, in a more compact form, the results concerning the number of solutions of congruences; these results are presented in Secs. 7 and 8 of the present paper). The above inequality can be obtained by analogy with Theorem 2, and hence the proof is not given here.

Corollary 1. *If $m = p$ is a prime and χ is a nonprincipal character modulo p, then, for an arbitrary $\varepsilon > 0$, there exists a $\sigma = \sigma(\varepsilon)$ such that, for $N > m^\sigma$, the following estimate holds:*

$$\left|\sum_{x\in K_s^D(N)}\chi(x+b)\right| \ll |K_s^D(N)|\cdot p^{-1/2+\varepsilon}.$$

Corollary 2. *If m is an arbitrary natural number, χ is a nonprincipal character modulo m, then, for a sufficiently large σ and for $N > m^\sigma$, the following estimate holds:*

$$\left|\sum_{x\in K_s^D(N)}\chi(x+b)\right| \ll |K_s^D(N)|\cdot\exp(-\gamma\sqrt{\sigma\,\log m}\,)$$

with some positive $\gamma = \gamma(s)$.

Corollary 1 (it can be found in [2]) immediately follows from Theorem 2 (in the remark, σ^* must be equal to $1/2$) and estimates (11) (compare with Remark 2 to Lemma 1), while Corollary 2 follows from Theorem 2 and estimates (19).

7. ON THE NUMBER OF SOLUTIONS OF THE CONGRUENCE $x_1 \cdots x_l \equiv \lambda \pmod m$

In what follows, $(\lambda, m) = 1$. Let us recall that by $T_l(N, m, \lambda)$ we denote the number of solutions of the congruence

$$x_1 \cdots x_l \equiv \lambda \pmod m, \qquad x_j \in K_s^D(N)$$

(obviously, we can assume $x_j \in K_s^D(N, m)$).

Theorem 3. *Suppose that $N \ge s^{w+\rho_0}$, $(m, \lambda) = 1$, $\varepsilon > 0$ $w \ge \sigma r$, where $\sigma \ge \sigma_0(s, \varepsilon)$ is sufficiently large, and*

$$\rho_0 = r\frac{\log s}{\log(k+1)} \asymp \log m.$$

Then

$$T_l(N, m, \lambda) = \frac{|K_s^D(N, m)|^l}{\varphi(m)} + O\biggl(\frac{|K_s^D(N)|^l}{\varphi(m)} \cdot \Delta_w^l(m)\biggr).$$

Proof. Obviously,

$$\begin{aligned}\biggl|T_l(N, m, \lambda) - \frac{|K_s^D(N, m)|^l}{\varphi(m)}\biggr| &\le \frac{|K_s^D(N)|^l}{\varphi(m)} \cdot \sum_{\chi \,(\mathrm{mod}\, m),\, \chi \ne \chi_0} \biggl|\sum_{x \in K_s^D(N)} \chi(x)\biggr|^l \\ &\ll \frac{|K_s^D(N)|^l}{\varphi(m)} \cdot \sum_{a \mid m,\, a > 1} |\Xi_a| \biggl(\Delta_w(m, a) + \frac{1}{m}\biggr)^l = \frac{|K_s^D(N)|^l}{\varphi(m)} \cdot \Delta_w^l(m)\end{aligned}$$

(we have used Theorem 2 and the remark to it as well as Definition (21) for $\Delta_w^l(m)$). The theorem is proved. □

Remark. The assumptions of Theorem 3 are satisfied for $N \ge m^\sigma$ with a sufficiently large $\sigma \ge \sigma_1(s, \varepsilon)$.

Corollary 3. *Suppose that $m = p$ is a prime and the assumptions of Theorem 3 are satisfied. Then*

$$T_l(N, p, \lambda) = \frac{|K_s^D(N, p)|^l}{p-1} \cdot \bigl(1 + O(p^{-l/2+1+l\varepsilon})\bigr).$$

Corollary 3 follows from (22); it was stated in [2], but with an inaccuracy: $|K_s^D(N)|$ was written in the numerator instead of $|K_s^D(N, p)|$. For $l \ge 3$, Corollary 3 establishes an asymptotic formula for $T_l(N, p, \lambda)$, and, for $l = 1, 2$, it provides an upper bound for this quantity. For $l = 1$, this estimate is sometimes less sharp than the trivial estimate

$$T^1(N, p, \lambda) \ll |K_s^D(N)| p^{-\log s/\log k}.$$

Corollary 4. *Suppose that m is such that the minimal divisor $a_0 \mid m$ distinct from one satisfies the inequality*

$$a_0 \ge \exp\biggl(\frac{\gamma_2 w}{\log \gamma_1 \gamma_2 w}\biggr).$$

Then, for a sufficiently large σ and $N \ge s^{w+\rho_0}$, $w \ge \sigma r$, the following relation holds:

$$T_l(N, m, \lambda) = \frac{|K_s^D(N, m)|^l}{\varphi(m)} \cdot \bigl(1 + O(a_0^{-l/2+1+(l+1)\varepsilon})\bigr).$$

Corollary 4 follows from (23), Remark 5 to Theorem 2, and the inequality $m/\varphi(m) \ll \log\log m$. For $l \ge 3$, Corollary 4 yields an asymptotic formula for $T_l(N, m, \lambda)$, and, for $l = 1, 2$, it gives an upper bound.

Corollary 5. *Suppose that m is such that the number of divisors m is at most $\exp(\sqrt{\log m}\,)$ (for example, $m = p^\alpha$, where p is a prime). Then, for $l \geq 3$, under the assumptions of Theorem 3 with some positive γ, the following estimate holds:*

$$T_l(N,m,\lambda) = \frac{|K_s^D(N,m)|^l}{\varphi(m)} \cdot \bigl(1 + O\bigl(\exp(-\sqrt{\gamma w}\,)\bigr)\bigr) = \frac{|K_s^D(N,m)|^l}{\varphi(m)} \cdot \bigl(1 + O\bigl(\exp(-\sqrt{\gamma\ \log m}\,)\bigr)\bigr).$$

Corollary 5 follows from (28).

Corollary 6. *Under the assumptions of Theorem 3 with some positive γ, for any arbitrary natural number m the following relations are satisfied:*

1) If $l \geq 4$, then, for a sufficiently large σ, the following asymptotic formula holds:

$$T_l(N,m,\lambda) = \frac{|K_s^D(N,m)|^l}{\varphi(m)} \cdot \bigl(1 + O\bigl(\exp(-\sqrt{\gamma w}\,)\bigr)\bigr) = \frac{|K_s^D(N,m)|^l}{\varphi(m)} \cdot \bigl(1 + O\bigl(\exp(-\sqrt{\gamma\ \log m}\,)\bigr)\bigr).$$

2) If $l = 3$, then, for a sufficiently large σ the following asymptotic formula holds:

$$\begin{aligned} T_3(N,m,\lambda) &= \frac{|K_s^D(N,m)|^3}{\varphi(m)} \cdot \left(1 + O\left(\exp\left(-\sqrt{\frac{\gamma w\ \log\log r}{\log r}}\,\right)\right)\right) \\ &= \frac{|K_s^D(N,m)|^3}{\varphi(m)} \cdot \left(1 + O\left(\exp\left(-\sqrt{\frac{\gamma\ \log m\ \log\log\log m}{\log\log m}}\,\right)\right)\right). \end{aligned}$$

3) If $l = 2$, then, for an arbitrary positive ε and for sufficiently large σ, the following estimate holds:

$$T_2(N,m,\lambda) \ll \frac{|K_s^D(N)|^2}{\varphi(m)} \cdot m^\varepsilon.$$

Conclusion 1) follows from (25), conclusion 2) follows from (26), and conclusion 3) from (27). Again, in Corollary 6, just as in Corollary 5, we must use Remark 5 to Theorem 2 to pass from $|K_s^D(N)|$ to $|K_s^D(N,m)|$ in the estimate of the remainder.

8. ON THE EXCEPTIONAL SET FOR THE CONGRUENCE $x_1x_2 \equiv \lambda \pmod m$

Theorem 4. *Suppose that $N \geq s^{w+\rho_0}$, $\varepsilon > 0$, and $w \geq \sigma r$, where σ is sufficiently large. Also, suppose that*

$$B = \{\lambda \pmod m : (z,m) = 1,\ \lambda \neq ab \pmod m \mid a,b \in K_s^D(N,m)\}.$$

Then

$$|B| \ll \varphi(m) \cdot \left(\frac{m}{\varphi(m)}\right)^4 \cdot \Delta_w^4(m).$$

From estimate (25) of $\Delta_w^4(m)$ we immediately obtain the following assertion.

Corollary. *Under the assumptions of Theorem 4, for any arbitrary natural number m, the following estimate holds:*

$$|B| \ll \varphi(m) \cdot \exp(-\sqrt{\gamma w}\,) \leq \varphi(m) \cdot \exp(-\sqrt{\gamma\ \log m}\,), \qquad \gamma > 0;$$

but if $m = p$ is a prime, then, for any sufficiently large σ (depending on the given positive ε), the inequality $|B| \ll p^\varepsilon$ holds.

Proof of Theorem 4. In what follows, $\mathbb{Z}_m = (\mathbb{Z}/m\mathbb{Z})$. To prove Theorem 4, let us recall several definitions.

By the *convolution* $(f*g)(x)$ of two functions f and g, $f, g\colon \mathbb{Z}_m \to \mathbb{C}$, we mean the function

$$(f*g)(x) = \sum_{z\in\mathbb{Z}_m^*} f(z)\overline{g(zx^{-1})}, \qquad x \in \mathbb{Z}_m^*.$$

Suppose that χ is a character modulo m. By the *Fourier transform* of a function $f\colon \mathbb{Z}_m \to \mathbb{C}$ we mean the function

$$\widehat{f}(\chi) = \sum_{x\in\mathbb{Z}_m^*} f(x)\chi(x).$$

The following lemma is well known.

Lemma 4. *Suppose that $f, g\colon \mathbb{Z}_m \to \mathbb{C}$ are some functions. Then*

$$\sum_{x\in\mathbb{Z}_m^*} f(x)\overline{g(x)} = \frac{1}{\varphi(m)}\sum_{\chi} \widehat{f}(\chi)\overline{\widehat{g}(\chi)}, \tag{31}$$

where the summation on the right-hand side of (31) *is over characters of the group $\mathbb{Z}_m^*$.*

The relation (31) and the equality $\widehat{(f*g)}(\chi) = \widehat{f}(\chi)\overline{\widehat{g}(\chi)}$ imply the analog of formula (31) for the convolution.

Lemma 5. *Suppose that $f, g\colon \mathbb{Z}_m \to \mathbb{C}$ are some functions. Then*

$$\sum_{x\in\mathbb{Z}_m^*} |(f*g)(x)|^2 = \frac{1}{\varphi(m)}\sum_{\chi} |\widehat{f}(\chi)|^2|\widehat{g}(\chi)|^2.$$

Consider the functions

$$\mu_1(t) = \bigl|\{x \in K_s^D(N) : x \equiv t \pmod m\}\bigr|, \qquad t \in \mathbb{Z}_m^*,$$
$$\mu_2(t) = \bigl|\{x \in K_s^D(N) : x \equiv t^{-1} \pmod m\}\bigr|, \qquad t \in \mathbb{Z}_m^*.$$

Obviously, we have

$$|K_s^D(N,m)| = \sum_{t\in\mathbb{Z}_m^*} \mu_1(t) = \sum_{t\in\mathbb{Z}_m^*} \mu_2(t),$$
$$\widehat{\mu}_1(\chi) = \sum_{x\in K_s^D(N)} \chi(x), \qquad \widehat{\mu}_2(\chi) = \sum_{x\in K_s^D(N)} \overline{\chi(x)}. \tag{32}$$

Suppose that

$$f_1(t) = \mu_1(t) - \frac{|K_s^D(N,m)|}{\varphi(m)}, \qquad f_2(t) = \mu_2(t) - \frac{|K_s^D(N,m)|}{\varphi(m)}.$$

Then

$$\sum_{x\in\mathbb{Z}_m^*} f_1(t) = \sum_{x\in\mathbb{Z}_m^*} f_2(x) = 0.$$

Besides, for any nonprincipal character χ, we have

$$\widehat{\mu}_i(\chi) = \widehat{f}_i(\chi), \qquad i = 1, 2. \tag{33}$$

Consider the sum

$$\Sigma = \sum_{x\in\mathbb{Z}_m^*} |(f_1*f_2)(x)|^2.$$

On the one hand,

$$\Sigma = \sum_{x\in\mathbb{Z}_m^*} |(f_1 * f_2)(x)|^2 = \sum_{x\in\mathbb{Z}_m^*} \left| \sum_{z\in\mathbb{Z}_m^*} f_1(z)\overline{f_2(zx^{-1})} \right|^2$$
$$= \sum_{x\in\mathbb{Z}_m^*} \left| \sum_{z\in\mathbb{Z}_m^*} \left(\mu_1(z) - \frac{|K_s^D(N,m)|}{\varphi(m)}\right)\left(\mu_2(zx^{-1}) - \frac{|K_s^D(N,m)|}{\varphi(m)}\right) \right|^2$$
$$= \sum_{x\in\mathbb{Z}_m^*} \left| \sum_{z\in\mathbb{Z}_m^*} \mu_1(z)\mu_2(zx^{-1}) - \frac{|K_s^D(N,m)|^2}{\varphi(m)} \right|^2;$$

hence we have a lower bound for Σ of the form

$$\Sigma \geq \sum_{x\in B} \left| \sum_{z\in\mathbb{Z}_m^*} \mu_1(z)\mu_2(zx^{-1}) - \frac{|K_s^D(N,m)|^2}{\varphi(m)} \right|^2 = |B| \cdot \frac{|K_s^D(N,m)|^4}{(\varphi(m))^2}. \tag{34}$$

(Here we have taken into account the fact that if $x \in B$, then the congruence $\xi\eta \equiv x \pmod m$ is unsolvable in numbers $\xi, \eta \in K_s^D(N,m)$, while the sum

$$\sum_{z\in\mathbb{Z}_m^*} \mu_1(z)\mu_2(zx^{-1})$$

is exactly the number of solutions of the congruence $\xi\eta \equiv x \pmod m$, $\xi, \eta \in K_s^D(N,m)$ and hence, for each $x \in B$ in (34), the internal sum over z is zero.)

On the other hand, applying Lemma 5 and taking (32), (33) into account, we obtain

$$\Sigma = \frac{1}{\varphi(m)} \sum_{\chi} |\widehat{f_1}(\chi)|^2 |\widehat{f_2}(\chi)|^2 = \frac{1}{\varphi(m)} \sum_{\chi,\, \chi\neq\chi_0} |\widehat{f_1}(\chi)|^2 |\widehat{f_2}(\chi)|^2 = \frac{1}{\varphi(m)} \sum_{\chi,\, \chi\neq\chi_0} \left| \sum_{x\in K_s^D(N)} \chi(x) \right|^4.$$

Let us find an upper bound for the sum Σ. By Theorem 2 and Remark 4, we have

$$\Sigma \leq \frac{|K_s^D(N)|^4}{\varphi(m)} \sum_{a|m,\, a>1} |\Xi_a| \left(\Delta_w(m,a) + \frac{1}{m}\right)^4 = \frac{|K_s^D(N)|^4}{\varphi(m)} \Delta_w^4(m). \tag{35}$$

Applying estimates (34), (35) of Σ, we obtain

$$|B| \frac{|K_s^D(N,m)|^4}{(\varphi(m))^2} \ll \frac{|K_s^D(N)|^4}{\varphi(m)} \Delta_w^4(m).$$

Theorem 4 now follows from Remark 5 to Theorem 2. □

ACKNOWLEDGMENTS

This work was supported by Presidential grants no. MD-3003.2006.1 and no. MK-1726.2006.1, by the Russian Foundation for Basic Research, grants no. 06-01-00518 and no. 06-01-00383, and by INTAS, grant no. 03-51-5070.

REFERENCES

1. S. Konyagin, "Arithmetic properties of integers with missing digits: distribution in residue classes," Period. Math. Hungar. **42** (1–2), 145–162 (2001).
2. N. G. Moshchevitin, "On numbers with restricted digits," Dokl. Ross. Akad. Nauk [Russian Acad. Sci. Dokl. Math.] **384** (6), 167–170 (2002) [Russian Acad. Sci. Dokl. Math.] **65** (3), 350–352 (2002).
3. W. Schmidt, "On normal numbers," Pacific J. Math. **10**, 661–672 (1960).
4. P. Erdős, C. Mauduit, and A. Sarközy, "On arithmetic properties of integers with missing digits. I: Distribution in residue classes," J. Number Theory **70**, 99–120 (1998).
5. W. D. Banks, A. Conflitti, and I. E. Shparlinski, "Character sums over integers with restricted g-ary digits," Illinois J. Math. **46**, 819–836 (2002).

6. W. D. Banks and I. E. Shparlinski, "Arithmetic properties of numbers with restricted digits," Acta Arith. **112**, 313–332 (2004).
7. N. G. Moshchevitin, "On numbers with missing digits: an elementary proof of a result due to S. V. Konyagin," Chebyshevskii Sb. **3** (3), 93–99 (2002).
8. M. B. Nathanson, *Additive Number Theory. Inverse Problems and the Geometry of Sumsets*, in *Graduate Texts in Math.* (Springer, Berlin, 1996), Vol. 165.
9. G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers*, 4th edition, (Oxford Univ. Press, Oxford, 1975).
10. S. M. Voronin and A. A. Karatsuba, *Riemann's Zeta Function* (Fizmatlit, Moscow, 1994) [in Russian].