Kloosterman sums in residue rings

J. Bourgain
Institute for Advanced Study,
Princeton, NJ 08540, USA
bourgain@ias.edu

M. Z. Garaev
Centro de Ciencias Matemáticas,
Universidad Nacional Autónoma de México,
Morelia 58089, Michoacán, México
garaev@matmor.unam.mx

Abstract

In the present paper, we generalize some of the results on Kloosterman sums proven in [3] for prime moduli to general moduli. This requires to establish the corresponding additive properties of the reciprocal set

$$I^{-1} = \{x^{-1} : x \in I\},$$

where $I$ is an interval in the ring of residue classes modulo a large positive integer. We apply our bounds on multilinear exponential sums to the Brun-Titchmarsh theorem and the estimate of very short Kloosterman sums, hence generalizing our earlier work to the setting of general modulus.

1 Introduction

In what follows, $\mathbb{Z}_m$ denotes the ring of residue classes modulo a large positive integer $m$ which frequently will be associated with the set $\{0, 1, \ldots, m - 1\}$. 
Given an integer $x$ coprime to $m$ (or an invertible element of $\mathbb{Z}_m$) we use $x^*$ or $x^{-1}$ to denote its multiplicative inverse modulo $m$.

Let $I$ be an interval in $\mathbb{Z}_m$. In the present paper we establish some additive properties of the reciprocal-set

$$I^{-1} = \{x^{-1} : x \in I\}.$$  

We apply our results to estimate some double Kloosterman sums, to Brun-Titchmarsh theorem and, involving multilinear exponential sum bounds of general modulus, we estimate short Kloosterman sums. These extends some results of our work [3] from prime moduli to the general.

Throughout the paper we use the abbreviation $e_m(z) := e^{2\pi iz/m}$.

2 Statement of our results

We start with the additive properties of reciprocal-set.

**Theorem 1.** Let $I = [1, N]$. Then the number $J_{2k}$ of solutions of the congruence

$$x_1^* + \ldots + x_k^* \equiv x_{k+1}^* + \ldots + x_{2k}^* \pmod{m}, \quad x_1, \ldots, x_{2k} \in I,$$

satisfies

$$J_{2k} < (2k)^{90k^3} (\log N)^{4k^2} \left( \frac{N^{2k-1}}{m} + 1 \right) N^k.$$

The following statement is a version of Theorem 1, where the variables $x_j$ are restricted to prime numbers. By $\mathcal{P}$ we denote the set of primes.

**Theorem 2.** Let $I = [1, N]$. Then the number $J_{2k}$ of solutions of the congruence

$$x_1^* + \ldots + x_k^* \equiv x_{k+1}^* + \ldots + x_{2k}^* \pmod{m}, \quad x_1, \ldots, x_{2k} \in I \cap \mathcal{P},$$

satisfies

$$J_{2k} < (2k)^k \left( \frac{N^{2k-1}}{m} + 1 \right) N^k.$$
We recall that the incomplete Kloosterman sum is the sum of the form
\[ \sum_{x=M+1}^{M+N} e_m(ax^* + bx), \]
where \( a \) and \( b \) are integers, \( \gcd(a, m) = 1 \). Here the summation over \( x \) is restricted to \( \gcd(x, m) = 1 \) (if the range of summation is empty, then we consider this sum to be equal to zero). As a consequence of the Weil bounds it is known that
\[ \left| \sum_{x=1}^{m} e_m(ax^* + bx) \right| \leq \tau(m) m^{1/2}, \]
see for example [7, Corollary 11.12]. This implies that for \( N < m \) one has the bound
\[ \left| \sum_{x=M+1}^{M+N} e_m(ax^* + bx) \right| < m^{1/2+o(1)}. \]

For \( M = 0 \) and \( N \) very small (that is, \( N = m^{o(1)} \)) these sums have been estimated by Korolev [11].

The incomplete bilinear Kloosterman sum
\[ S = \sum_{x_1=M+1}^{M_1+N_1} \sum_{x_2=M_2+1}^{M_2+N_2} \alpha_1(x_1)\alpha_2(x_2)e_m(ax_1^*x_2^*), \]
where \( \alpha_i(x_i) \in \mathbb{C}, |\alpha_i(x_i)| \leq 1, \) is also well known in the literature. When \( M_1 = M_2 = 0 \) the sum \( S \) (in a more general form in fact) has been estimated by Karatsuba [9, 10] for very short ranges of \( N_1 \) and \( N_2 \).

Theorem 1 leads to the following improvement of the range of applicability of Karatsuba’s estimate [9].

**Theorem 3.** Let \( I_1 = [1, N_1], I_2 = [1, N_2] \). Then uniformly over all positive integers \( k_1, k_2 \) and \( \gcd(a, m) = 1 \) we have
\[ \left| \sum_{x_1 \in I_1, x_2 \in I_2} \alpha_1(x_1)\alpha_2(x_2)e_m(ax_1^*x_2^*) \right| < (2k_1)^{\frac{45k_2^2}{k_1}} (2k_2)^{\frac{45k_1^2}{k_2}} (\log m)^{\frac{1}{2} + \frac{k_2}{k_1}} \times \]
\[ \times \left( \frac{N_{k_1}^{k_{1}-1}}{m^{1/2}} + \frac{N_{k_2}^{k_{2}-1}}{N_1^{1/2}} \right)^{1/(2k_2)} \left( \frac{N_{k_1}^{1/2}}{m^{1/2}} + \frac{m^{1/2}}{N_2^{k_2}} \right)^{1/(2k_1)} N_1 N_2. \]
Given $N_1, N_2$ we choose $k_1, k_2$ such that
\[ N_1^{2(k_1-1)} < m \leq N_1^{2k_1}, \quad N_2^{2(k_2-1)} < m \leq N_2^{2k_2} \]
and the bound will be nontrivial unless both $N_1, N_2$ are within $m^\varepsilon$-ratio of an element of $\{ m^{\frac{1}{l}}, l \in \mathbb{Z}_+ \}$. Thus, we have the following

**Corollary 1.** Let $I_1 = [1, N_1], I_2 = [1, N_2]$, where for $i = 1$ or $i = 2$
\[ N_i \not\in \bigcup_{j \geq 1} [m^{\frac{1}{j} - \varepsilon}, m^{\frac{1}{j} + \varepsilon}]. \]
Then
\[
\max_{(a,m)=1} \left| \sum_{x_1=1}^{N_1} \sum_{x_2=1}^{N_2} \alpha_1(x_1) \alpha_2(x_2) e_m(ax_1^* x_2^*) \right| < m^{-\delta} N_1 N_2
\]
for some $\delta = \delta(\varepsilon) > 0$.

We shall then apply our bilinear Kloosterman sum bound to the Brun-Titchmarsh theorem and improve the result of Friedlander-Iwaniec [5] on $\pi(x; q, a)$ as follows:

**Theorem 4.** Let $q \sim x^\theta$, where $\theta < 1$ is close to 1. Then
\[
\pi(x; q, a) < cx \phi(q) \log \frac{x}{q}
\]
with $c = 2 - c_1(1 - \theta)^2$, for some absolute constant $c_1 > 0$ and all sufficiently large $x$ in terms of $\theta$.

Recall that for $(a, q) = 1$, $\pi(x; q, a)$ denotes the number of primes $p \leq x$ with $p \equiv a \pmod{q}$. The constant $c_1$ is effective and can be made explicit. We mention that for primes $q$ Theorem 4 is contained in our work [3].

Finally, we shall apply multilinear exponential sum bounds from [2] (see Lemma 1 below) to establish the following estimate of a short linear Kloosterman sums.

**Theorem 5.** Let $N > m^c$ where $c$ is a small fixed positive constant. Then we have the bound
\[
\max_{(a,m)=1} \left| \sum_{n \leq N} e_m(an^*) \right| < \frac{(\log \log m)^{O(1)}}{(\log m)^{1/2}} N,
\]
where the implied constants may depend only on $c$. 
This improves some results of Korolev [11]. We also refer the reader to [12] for some variants of the problem. We remark that a stronger bound is claimed in [8], but the proof there is in doubt.

Since
\[ \sum_{n=1}^{m} e_m(a n^*) = \mu(m), \]
in Theorem 5 one can assume that \( N < m \). We also note that the aforementioned consequence of the Weil bounds gives a stronger estimate in the case \( N > m^{1/2 + c_0} \) for any fixed constant \( c_0 \).

### 3 Lemmas

The following result, which we state as a lemma, has been proved by Bourgain [2]. It is based on results from additive combinatorics, in particular sum-product estimates. This lemma will be used in the proof of our results on short Kloosterman sums.

**Lemma 1.** For all \( \gamma > 0 \) there exist \( \varepsilon = \varepsilon(\gamma) > 0 \), \( \tau = \tau(\gamma) > 0 \) and \( k = k(\gamma) \in \mathbb{Z}_+ \) such that the following holds.

Let \( A_1, \ldots, A_k \subset \mathbb{Z}_q \), \( q \) arbitrary, and assume \( |A_i| > q^\gamma \) \((1 \leq i \leq k)\) and also
\[
\max_{\xi \in \mathbb{Z}_{q_1}} |A_i \cap \pi_{q_1}^{-1}(\xi)| < q_1^{-\gamma}|A_i| \quad \text{for all} \quad q_1 | q, q_1 > q^\varepsilon.
\]

Then
\[
\max_{\xi \in \mathbb{Z}_q^*} \left| \sum_{x_1 \in A_1} \cdots \sum_{x_k \in A_k} e_q(\xi x_1 \cdots x_k) \right| < C q^{-\tau} |A_1| \cdots |A_k|.
\]

Here, the notation \( |A \cap \pi_{q_1}^{-1}(\xi)| \) can be viewed as the number of solutions of the congruence \( x \equiv \xi \pmod{q_1} \), \( x \in A \).

Clearly, the conclusion of Lemma 1 can be stated in basically equivalent form
\[
\max_{\xi \in \mathbb{Z}_q^*} \sum_{x_1 \in A_1} \cdots \sum_{x_{k-1} \in A_{k-1}} \sum_{x_k \in A_k} e_q(\xi x_1 \cdots x_{k-1} x_k) < C q^{-\tau} |A_1| \cdots |A_k|.
\]
Indeed applying the Cauchy-Schwarz inequality, it follows that

\[
\left( \sum_{x_1 \in A_1} \cdots \sum_{x_{k-1} \in A_{k-1}} x_k \sum_{x_k \in A_k} e_q(\xi x_1 \cdots x_{k-1}x_k) \right)^2 \leq |A_1| \cdots |A_{k-1}| \sum_{x_k \in A_k} \left| \sum_{x_1 \in A_1} \cdots \sum_{x_{k-1} \in A_{k-1}} e_q(\xi x_1 \cdots x_{k-1}(x_k - x'_k)) \right|.
\]

We fix \( x'_k \in A_k \) such that

\[
\left( \sum_{x_1 \in A_1} \cdots \sum_{x_{k-1} \in A_{k-1}} x_k \sum_{x_k \in A_k} e_q(\xi x_1 \cdots x_{k-1}x_k) \right)^2 \leq |A_1| \cdots |A_{k-1}| |A_k| \sum_{x_1 \in A_1} \cdots \sum_{x_{k-1} \in A_{k-1}} \sum_{x_k \in A'_k} e_q(\xi x_1 \cdots x_{k-1}x_k),
\]

where \( A'_k = A_k - \{ x'_k \} \). Then we observe that the set \( A'_k \) also satisfies the condition of Lemma 1.

We need some facts from the geometry of numbers. Recall that a lattice in \( \mathbb{R}^n \) is an additive subgroup of \( \mathbb{R}^n \) generated by \( n \) linearly independent vectors. Take an arbitrary convex compact and symmetric with respect to 0 body \( D \subset \mathbb{R}^n \). Recall that, for a lattice \( \Gamma \subset \mathbb{R}^n \) and \( i = 1, \ldots, n \), the \( i \)-th successive minimum \( \lambda_i(D, \Gamma) \) of the set \( D \) with respect to the lattice \( \Gamma \) is defined as the minimal number \( \lambda \) such that the set \( \lambda D \) contains \( i \) linearly independent vectors of the lattice \( \Gamma \). Obviously, \( \lambda_1(D, \Gamma) \leq \cdots \leq \lambda_n(D, \Gamma) \). We need the following result given in [1, Proposition 2.1] (see also [13, Exercise 3.5.6] for a simplified form that is still enough for our purposes).

**Lemma 2.** We have

\[
|D \cap \Gamma| \leq \prod_{i=1}^{n} \left( \frac{2i}{\lambda_i(D, \Gamma)} + 1 \right).
\]

Denoting, as usual, by \((2n+1)!!\) the product of all odd positive numbers up to \(2n+1\), we get the following

**Corollary 2.** We have

\[
\prod_{i=1}^{n} \min\{\lambda_i(D, \Gamma), 1\} \leq \frac{(2n+1)!!}{|D \cap \Gamma|}.
\]
Lemma 3. The following bound holds:

\[
\left| \left\{ (x_1, \ldots, x_{2k}) \in [1, N]^{2k} : \frac{1}{x_1} + \ldots + \frac{1}{x_k} = \frac{1}{x_{k+1}} + \ldots + \frac{1}{x_{2k}} \right\} \right| < (2k)^{80k^3} (\log N)^{4k^2} N^k.
\]

4 Proof of Theorems 1 and 2

First we prove Theorem 1. It suffices to consider the case \( kN^{k-1} < m \) as otherwise the statement is trivial. For \( \lambda = 0, 1, \ldots, m - 1 \) denote

\[ J(\lambda) = \left\{ (x_1, \ldots, x_k) \in I^k : x_1^* + \ldots + x_k^* \equiv \lambda \pmod{m} \right\}. \]

Let

\[ \Omega = \{ \lambda \in [1, m - 1] : |J(\lambda)| \geq 1 \} \]

Since \( J(0) = 0 \), we have

\[ J_{2k} = \sum_{\lambda \in \Omega} |J(\lambda)|^2. \]

Consider the lattice

\[ \Gamma_\lambda = \{(u, v) \in \mathbb{Z}^2 : \lambda u \equiv v \pmod{m}\} \]

and the body

\[ D = \{(u, v) \in \mathbb{R}^2 : |u| \leq N^k, |v| \leq kN^{k-1}\}. \]

Denoting by \( \mu_1, \mu_2 \) the consecutive minimas of the body \( D \) with respect to the lattice \( \Gamma_\lambda \), by Corollary 2 it follows

\[ \prod_{i=1}^{2} \min\{\mu_i, 1\} \leq \frac{15}{|\Gamma_\lambda \cap D|}. \]

Observe that for \( (x_1, \ldots, x_k) \in J(\lambda) \) one has

\[ \lambda x_1 \ldots x_k \equiv x_2 \ldots x_k + \ldots + x_1 \ldots x_{k-1} \pmod{m}, \]

implying

\[ (x_1 \ldots x_k, x_2 \ldots x_k + \ldots + x_1 \ldots x_{k-1}) \in \Gamma_\lambda \cap D. \]
Thus, for $\lambda \in \Omega$ we have $\mu_1 \leq 1$. We split the set $\Omega$ into two subsets:

$$\Omega' = \{ \lambda \in \Omega : \mu_2 \leq 1 \}, \quad \Omega'' = \{ \lambda \in \Omega : \mu_2 > 1 \}.$$ 

We have

$$J_{2k} = \sum_{\lambda \in \Omega'} |J(\lambda)|^2 + \sum_{\lambda \in \Omega''} |J(\lambda)|^2. \quad (1)$$

Case 1: $\lambda \in \Omega'$, that is $\mu_2 \leq 1$. Let $(u_i, v_i) \in \mu_i D \cap \Gamma_\lambda, i = 1, 2$, be linearly independent. Then

$$0 \neq u_1 v_2 - v_1 u_2 \equiv u_1 \lambda u_2 - u_2 \lambda u_1 \equiv 0 \pmod{m},$$

whence

$$|u_1 v_2 - v_1 u_2| \geq m.$$ 

Also

$$|u_1 v_2 - v_1 u_2| \leq 2k \mu_1 \mu_2 N^{2k-1} \leq 30kN^{2k-1} \frac{|\Gamma_\lambda \cap D|}{|\Gamma_\lambda \cap D|}.$$ 

Thus, for $\lambda \in \Omega'$, the number $|\Gamma_\lambda \cap D|$ of solutions of the congruence

$$\lambda u \equiv v \pmod{m}$$

in integers $u, v$ with $|u| \leq N^k, |v| \leq kN^{k-1}$ is bounded by

$$|\Gamma_\lambda \cap D| \leq \frac{30kN^{2k-1}}{m}. \quad (2)$$

Note that for $\lambda \in \Omega'$ the sets

$$W_\lambda := \{ (u, v); (u, v) \in \Gamma_\lambda \cap D, \gcd(u, m) = 1 \}$$

are pairwise disjoint. Therefore, if we denote by $S(u, v)$ the set of $k$-tuples $(x_1, \ldots, x_k)$ of positive integers $x_1, \ldots, x_k \leq N$ coprime to $m$ with

$$x_1 \ldots x_k = u, \quad x_2 \ldots x_k + \ldots + x_1 \ldots x_{k-1} = v,$$

we get

$$\sum_{\lambda \in \Omega'} |J(\lambda)|^2 = \sum_{\lambda \in \Omega'} \left( \sum_{(u, v) \in \Gamma_\lambda \cap D, \gcd(u, m) = 1} \sum_{(x_1, \ldots, x_k) \in S(u, v)} 1 \right)^2.$$
Applying the Cauchy-Schwarz inequality and taking into account (2), we get
\[
\sum_{\lambda \in \Omega'} |J(\lambda)|^2 \leq \frac{30kN^{2k-1}}{m} \sum_{\lambda \in \Omega'} \sum_{(u,v) \in \Gamma_{\lambda} \cap D \atop \gcd(u,m)=1} \left( \sum_{x_1, \ldots, x_k \in S(u,v)} 1 \right)^2
\]
(3)

From the disjointness of sets $W_\lambda$ it follows that the summation on the right hand side of (3) is bounded by the number of solutions of the system of equations
\[
\begin{align*}
    x_1 \ldots x_k &= y_1 \ldots y_k, \\
    x_1 \ldots x_{k-1} + \ldots + x_2 \ldots x_k &= y_2 \ldots y_k + \ldots + y_1 \ldots y_{k-1},
\end{align*}
\]
in positive integers $x_i, y_j \leq N$ coprime to $m$. Hence, by Lemma 3, it follows that
\[
\sum_{\lambda \in \Omega'} |J(\lambda)|^2 \leq 30k(2k)^{80k^3}(\log N)^{4k^2} \frac{N^{3k-1}}{m}.
\]
(4)

**Case 2:** $\lambda \in \Omega''$, that is $\mu_2 > 1$. Then the vectors from $\Gamma_{\lambda} \cap D$ are linearly dependent and in particular there is some $\hat{\lambda} \in \mathbb{Q}$ such that
\[
\hat{\lambda}x_1 \ldots x_k = x_2 \ldots x_k + \ldots + x_1 \ldots x_{k-1}
\]
for $(x_1, \ldots, x_k) \in J(\lambda)$.

Thus,
\[
\sum_{\lambda \in \Omega''} |J(\lambda)|^2 \leq \sum_{\hat{\lambda} \in \mathbb{Q}} \left| \left\{ (x_1, \ldots, x_k) \in I^k; \frac{1}{x_1} + \ldots + \frac{1}{x_k} = \hat{\lambda} \right\} \right|^2
\]
\[
= \left| \left\{ (x_1, \ldots, x_{2k}) \in [1,N]^{2k}; \frac{1}{x_1} + \ldots + \frac{1}{x_k} = \frac{1}{x_{k+1}} + \ldots + \frac{1}{x_{2k}} \right\} \right|
\]
\[
< (2k)^{80k^3}(\log N)^{4k^2} N^k.
\]

Inserting this and (4) into (1), we obtain
\[
J_{2k} < (2k)^{90k^3}(\log N)^{4k^2} \left( \frac{N^{2k-1}}{m} + 1 \right) N^k
\]
which concludes the proof of Theorem 1.

The proof of Theorem 2 follows the same line with the only difference that instead of Lemma 3 one should apply the bound
\[
\left| \left\{ (x_1, \ldots, x_{2k}) \in ([1,N] \cap \mathcal{P})^{2k}; \frac{1}{x_1} + \ldots + \frac{1}{x_k} = \frac{1}{x_{k+1}} + \ldots + \frac{1}{x_{2k}} \right\} \right|
\]
\[
< (2k)^k \left( \frac{N}{\log N} \right)^k.
\]
4.1 Proof of Theorem 3

Let
\[ S = \sum_{x_1 \in I_1} \sum_{x_2 \in I_2} \alpha_1(x_1) \alpha_2(x_2) e_m(ax_1^* x_2^*). \]

Then by Hölder’s inequality
\[ |S|^{k_2} \leq N_1^{k_2-1} \sum_{x_1 \in I_1} \left| \sum_{x_2 \in I_2} \alpha_2(x_2) e_m(ax_1^* x_2^*) \right|^{k_2}. \]

Thus, for some \( \sigma(x_1) \in \mathbb{C} \), \( |\sigma(x_1)| = 1 \),
\[ |S|^{k_2} \leq N_1^{k_2-1} \sum_{y_1, \ldots, y_k \in I_2} \left| \sum_{x_1 \in I_1} \sigma(x_1) e_m(ax_1^* (y_1^* + \ldots + y_k^*)) \right|. \]

Again by Hölder’s inequality,
\[ |S|^{k_1 k_2} \leq N_1^{k_1 k_2 - k_1} N_2^{k_1 k_2 - k_2} \sum_{\lambda=0}^{p-1} J_{k_2}(\lambda; N_2) \left| \sum_{x_1 \in I_1} \sigma(x_1) e_m(ax_1^* \lambda) \right|^{k_1}, \]
where \( J_k(\lambda; N) \) is the number of solutions of the congruence
\( x_1^* + \ldots + x_k^* \equiv \lambda \pmod{m}, \quad x_i \in [1, N] \).

Then applying the Cauchy-Schwarz inequality and using
\[ \sum_{\lambda=0}^{p-1} J_{k_2}(\lambda; N_2)^2 = J_{2k_2}(N_2), \quad \sum_{\lambda=0}^{p-1} \left| \sum_{x_1 \in I_1} \sigma(x_1) e_m(ax_1^* \lambda) \right|^{2k_1} \leq mJ_{2k_1}(N_1). \]
we get
\[ |S|^{2k_1 k_2} \leq pN_1^{2k_1 k_2 - k_1} N_2^{2k_1 k_2 - k_2} J_{2k_1}(N_1) J_{2k_2}(N_2). \quad (5) \]

Applying Theorem 1, we obtain
\[ |S|^{2k_1 k_2} \leq (2k_1)^{90k_1^2} (2k_2)^{90k_2^2} (\log N_1)^{4k_1^2} (\log N_2)^{4k_2^2} \times \]
\[ \times N_1^{2k_1 k_2} N_2^{2k_1 k_2} \left( \frac{N_1^{k_1-1}}{m^{1/2}} + \frac{m^{1/2}}{N_1^{k_1}} \right) \left( \frac{N_2^{k_2-1}}{m^{1/2}} + \frac{m^{1/2}}{N_2^{k_2}} \right). \]

Thus,
\[ |S| < (2k_1)^{45k_1^2 / k_2} (2k_2)^{45k_2^2 / k_1} (\log m)^{2(k_1 + k_2)} \times \]
\[ \times \left( \frac{N_1^{k_1-1}}{m^{1/2}} + \frac{m^{1/2}}{N_1^{k_1}} \right)^{1/(2k_1 k_2)} \left( \frac{N_2^{k_2-1}}{m^{1/2}} + \frac{m^{1/2}}{N_2^{k_2}} \right)^{1/(2k_1 k_2)} N_1 N_2, \]
which finishes the proof of Theorem 3.
5 Proof of Theorem 4

Let $\varepsilon$ be a positive constant very small in terms of $\delta = 1 - \theta$ (say, $\varepsilon = \delta^4$). Denote

\begin{align*}
A &= \{n \leq x; n \equiv a \pmod{q}\}, \\
A_d &= \{n \in A; n \equiv 0 \pmod{d}\}, \\
S(A, z) &= |\{n \in A; (n, p) = 1 \text{ for } p < z, (p, q) = 1\}|, \\
r_d &= |A_d| - \frac{x}{qd}.
\end{align*}

We take $z = D^{1/2}$, where $D$ is the level of distribution. We shall define $D$ to satisfy

\[ D \sim \left(\frac{x}{q}\right)^{1+c\delta^2} \sim x^{\delta+o(\delta^2)} \sim q^{\delta+O(\delta^3)}, \]

where $c$ is a suitable absolute positive constant ($c = 0.01$ will do).

Take integer $k$ such that

\[ \frac{1}{2k - 1} < \delta < \frac{1}{2k - 3}. \]

Having in mind [6, Theorem 12.21], we consider the factorization $D = MN$ in the form

\[ N = q^{1/(2k-1)}, \quad M = \frac{D}{N}. \]

Following the proof of [6, Theorem 13.1] we find that

\[ S(A, z) \leq \frac{(2 + \varepsilon)x}{\phi(q) \log D} + R(M, N). \]

Here the remainder $R(M, N)$ is estimated by

\[ R(M, N) \ll \sum_{\substack{m \leq M, n \leq N \\gcd(mn, q) = 1}} \alpha_m \beta_n r_{mn}, \]

the implied constant may depend on $\varepsilon$. Our aim is to prove the bound $R(M, N) \ll x^{1-\varepsilon}q^{-1}$. For this we may assume that $\alpha_m, \beta_n$ are supported on dyadic intervals

\[ 0.5M_1 < m \leq M_1, \quad 0.5N_1 < n \leq N_1. \]
for some $1 \leq M_1 \leq M$ and $1 \leq N_1 \leq N$ with $M_1 N_1 q \geq x^{1-\varepsilon}$. Then according to [6, p.262] we have the bound

$$R(M, N) \ll \frac{x}{q M_1 N_1} \sum_{0<|h| \leq H} \sum_{m \sim M_1} \left| \sum_{n \sim N_1} \gamma(h; n) e_q (ahm^* n^*) \right| + \frac{x^{1-\varepsilon}}{q},$$

where

$$H = q M_1 N_1 x^{3\varepsilon-1} \leq q Dx^{3\varepsilon-1} \ll x^{c\delta^3 + 3\varepsilon}.$$ 

In particular, $\gcd(h, q) < q^{O(\delta^3)}$. Thus, for some $\gamma(n) \in \mathbb{C}$ with $|\gamma(n)| \leq 1$ we have

$$R(M, N) \ll x^{3\varepsilon} \sum_{m \leq M} \left| \sum_{n \leq N} \gamma(n) e_q (a_1 m^* n^*) \right| + \frac{x^{1-\varepsilon}}{q},$$

where, say, $q^{1-\delta^2} \leq q_1 \leq q$ and $\gcd(a_1, q_1) = 1$. Then our Theorem 3 applied with $k_1 = k_2 = k$ implies that

$$R(M, N) \ll MN^{1-c_0/k^2} + \frac{x^{1-\varepsilon}}{q} < D^{1-c_0 \delta^2} + \frac{x^{1-\varepsilon}}{q},$$

where $c_0 > 0$ is an absolute constant. Therefore, from the choice $D \sim x^{\delta + c\delta^2}$ with $0 < c < 0.5c_0$, we obtain

$$S(A, z) < \frac{(2 - c' \delta^2)x}{\phi(q) \log(x/q)}$$

for some absolute constant $c' > 0$. The result follows.

6 Proof of Theorem 5

The proof of Theorem 5 is based on Bourgain’s multilinear exponential sum bounds for general moduli [2], see Lemma 1 above. We will also need a version of Theorem 3 on bilinear Kloosterman sum estimates with the variables of summation restricted to prime and almost prime numbers.

6.1 Double Kloosterman sums with primes and almost primes

As a consequence of Theorem 2 we have the following bilinear Kloosterman sum estimate.
Corollary 3. Let $N_1, N_2, k_1, k_2$ be positive integers, $\gcd(a, m) = 1$. Then for any coefficients $\alpha(p), \beta(q) \in \mathbb{C}$ with $|\alpha(p)|, |\beta(q)| \leq 1$, we have

\[
\left| \sum_{p \leq N_1} \sum_{q \leq N_2} \alpha(p)\beta(q)e_m(ap^{k_1}q^{k_2}) \right| < 2^{(2k_1)\frac{1}{k_1} + (2k_2)\frac{1}{k_2}} \left( \frac{N_1^{k_1-1}}{m^{1/2}} + \frac{m^{1/2}}{N_1^{k_1}} \right)^{1/(2k_1k_2)} \left( \frac{N_2^{k_2-1}}{m^{1/2}} + \frac{m^{1/2}}{N_2^{k_2}} \right)^{1/(2k_1k_2)} N_1N_2,
\]

where the variables $p$ and $q$ of the summations are restricted to prime numbers.

Indeed, denoting the quantity on the left hand side by $|S|$ and following the proof of Theorem 3 we arrive at the bound (see (5))

\[
|S|^{2k_1k_2} \leq mN_1^{2k_1k_2-2k_1}N_2^{2k_1k_2-2k_2} J_{2k_1}(N_1)J_{2k_2}(N_2),
\]

where in our case $J_{2k}(N)$ denotes the number of solutions of the congruence

\[ p^*_1 + \ldots + p^*_k \equiv p^*_{k+1} + \ldots + p^*_{2k} \pmod{m} \]

in prime numbers $p_1, \ldots, p_{2k} \leq N$. The statement then follows by the bounds for $J_{2k}(N)$ given in Theorem 2.

Lemma 4. Let $K, L$ be large positive integers, $2L < K$. Then uniformly over $k$ the number $T_{2k}(K, L)$ of solutions of the diophantine equation

\[
1/p_1q_1 + \ldots + 1/p_kq_k = 1/p_{k+1}q_{k+1} + \ldots + 1/p_{2k}q_{2k}
\]

in prime numbers $p_i, q_i$ satisfying $0.5K < p_i < K$ and $q_i < L$ is bounded by

\[
T_{2k}(K, L) < k^k \left( \frac{K}{\log K} \right)^k \left( \frac{L}{\log L} \right)^k.
\]

The proof is straightforward. For any given $1 \leq i_0 \leq 2k$ we have

\[
\frac{p_1 \ldots p_{2k}q_1 \ldots q_{2k}}{p_{i_0}q_{i_0}} \equiv 0 \pmod{p_{i_0}q_{i_0}}
\]

Since $p_i \neq q_j$, it follows that $p_{i_0}$ appears in the sequence $p_1, \ldots, p_{2k}$ at least two times. Thus, the sequence $p_1, \ldots, p_{2k}$ contains at most $k$ different prime
numbers. Correspondingly, the sequence \( q_1, \ldots, q_{2k} \) contains at most \( k \) different prime numbers. Therefore, there are at most

\[
k^{2k} \left( \frac{0.9K}{\log K} \right)^k k^{2k} \left( \frac{1.1L}{\log L} \right)^k < k^{4k} \left( \frac{K}{\log K} \right)^k \left( \frac{L}{\log L} \right)^k
\]

possibilities for \((p_1, \ldots, p_{2k}, q_1, \ldots, q_{2k})\). The result follows.

Now following the same line as the proof of Theorems 1 and 2, with the only difference that in the course of the proof we substitute Lemma 3 by Lemma 4, we get the following statement.

**Lemma 5.** Let \( K, L \) be large positive integers, \( 2L < K \). Then uniformly over \( k \) the number \( J_{2k}(K, L) \) of solutions of the diophantine equation

\[
\sum_{p_1 q_1} + \ldots + \sum_{p_k q_k} \equiv \sum_{p_{k+1} q_{k+1}} + \ldots + \sum_{p_{2k} q_{2k}} \pmod{m}
\]

in prime numbers \( p_i, q_i \) satisfying \( 0.5K < p_i < K \) and \( q_i < L \) is bounded by

\[
J_{2k}(K, L) < k^{4k} \left( \frac{(KL)^{2k-1}}{m} + 1 \right) (KL)^k.
\]

From Lemma 5 we get the following corollary.

**Corollary 4.** Let \( N, K, L, k_1, k_2 \) be positive integers, \( 2L < K \). Then for any coefficients \( \alpha(p), \beta(q; r) \in \mathbb{C} \) with \( |\alpha(p)|, |\beta(q; r)| \leq 1 \), we have

\[
\max_{\gcd(a, m) = 1} \left| \sum_{p \leq N} \sum_{0.5K < q \leq K} \sum_{r \leq L} \alpha(p) \beta(q; r) e_m(ap^* q^* r^*) \right| < k_1^{\frac{1}{2}} k_2^{\frac{1}{2}} \left( \frac{N^{k_1 - 1}}{m^{1/2}} + \frac{m^{1/2}}{N^{k_1}} \right)^{1/(2k_1 k_2)} \left( \frac{(KL)^{k_2 - 1}}{m^{1/2}} + \frac{m^{1/2}}{(KL)^{k_2}} \right)^{1/(2k_1 k_2)} NKL,
\]

where the variables \( p, q \) and \( r \) of the summations are restricted to prime numbers.

### 6.2 Proof of Theorem 5

Denote \( \varepsilon := \log N / \log m > c \). As we have mentioned before, we can assume that \( \varepsilon < 4/7 \).
In what follows, \( r \) is a large absolute integer constant. More explicitly, we define \( r \) to be the choice of \( k \) in Lemma 1 with, say, \( \gamma = 1/10 \). Denote
\[
G = \{ x < N : \quad p_1 \geq N^\alpha, \quad p_r \geq N^\beta, \quad p_1 p_2 \cdots p_r < N^{1-\beta} \},
\]
where \( p_1 \geq p_2 \geq \ldots \geq p_r \) are the largest prime factors of \( x \) and
\[
0.1 > \alpha \geq \beta > \frac{1}{\log N}
\]
are parameters to specify. Note that the number of positive integers not exceeding \( N \) and consisting on products of at most \( r - 1 \) prime numbers is estimated by
\[
\sum_{k=1}^{r-1} \sum_{\substack{p_1 \cdots p_k \leq N \\ p_1 \geq \cdots \geq p_k}} 1 \ll \frac{N}{\log N} + \sum_{k=2}^{r-1} \sum_{\substack{p_2 \cdots p_k \leq N^{(k-1)/k} \\ p_2 \leq \cdots \leq p_k}} \frac{N}{p_2 \cdots p_k \log(N/(p_2 \cdots p_k))}
\]
\[
\ll \frac{N}{\log N} + \sum_{k=2}^{r-1} \sum_{p_2 \leq N} p_2 \cdots p_k \log N \ll \frac{N(\log \log N)^{r-1}}{\log N}.
\]
Here and below the implied constants may depend only on \( r \). Hence, we have
\[
N - |G| \leq \frac{cN(\log \log N)^{r-1}}{\log N} + \sum_{x < N, \quad p_1 < N^\alpha} 1 + \sum_{x < N, \quad p_r < N^\beta} 1 + \sum_{x < N, \quad p_1 p_2 \cdots p_r > N^{1-\beta}} 1,
\]
for some constant \( c = c(r) > 0 \). Next, we have
\[
\sum_{x < N, \quad p_1 p_2 \cdots p_r > N^{1-\beta}} 1 \leq \sum_{y \leq N^\beta} 1 \leq \sum_{y \leq N^\beta} \frac{N}{yp_2 \cdots p_r \log(N/(yp_2 \cdots p_r))}
\]
\[
\ll \frac{N(\log \log N)^{r-1}}{y \log N} \ll \beta N(\log \log N)^{r-1}.
\]
Let $\Psi(x, y)$, as usual, denote the number of positive integers $\leq x$ having no prime divisors $> y$. Thus, we have

$$N - |G| \leq c_1 \beta N (\log \log N)^{r-1} + \Psi(N, N^\alpha) + \sum_{\substack{x < N \atop p_r < N^\beta}} 1,$$

for some constant $c_1 = c_1(r) > 0$.

Letting $0.1 > \beta_1 > \beta$ be another parameter, we similarly observe that

$$\sum_{\substack{x < N \atop p_1 \ldots p_{r-1} > N^{1-\beta_1}}} 1 \leq \sum_{\substack{y < N^{\beta_1} \atop p_1 \ldots p_{r-1} \leq N/y}} 1 \ll \sum_{y < N^{\beta_1}} \frac{N (\log \log N)^{r-2}}{y \log N} \ll \beta_1 N (\log \log N)^{r-2}.$$

Hence,

$$N - |G| \leq c_1 \beta N (\log \log N)^{r-1} + c_2 \beta_1 N (\log \log N)^{r-2} + \Psi(N, N^\alpha) + \sum_{\substack{x < N \atop p_r < N^\beta \atop p_1 \ldots p_{r-1} \leq N^{1-\beta_1}}} 1,$$

Observing that

$$\sum_{\substack{x < N \atop p_1 \ldots p_{r-1} \leq N^{1-\beta_1}}} 1 \leq \sum_{p_1 \ldots p_{r-1} \leq N^{1-\beta_1}} \Psi\left(\frac{N}{p_1 \ldots p_{r-1}}, N^\beta\right),$$

we get

$$N - |G| \leq c_1 \beta N (\log \log N)^{r-1} + c_2 \beta_1 N (\log \log N)^{r-2} + \Psi(N, N^\alpha) + \sum_{p_1 \ldots p_{r-1} \leq N^{1-\beta_1}} \Psi\left(\frac{N}{p_1 \ldots p_{r-1}}, N^\beta\right).$$

By the classical result of de Bruijn [4] if $y > (\log x)^{1+\delta}$, where $\delta > 0$ is a fixed constant, then

$$\Psi(x, y) \leq xu^{-(1+o(1))} \quad \text{as} \quad u = \frac{\log x}{\log y} \to \infty.$$
We now take 
\[ \alpha = \frac{1}{\log \log m}, \quad \beta = \frac{\log \log m}{(\log m)^{1/2}}, \quad \beta_1 = \beta \log \log m = \frac{(\log \log m)^2}{(\log m)^{1/2}} \]
and then have
\[
N - |\mathcal{G}| < \alpha^{\frac{1}{2}} N + \sum_{p_1 \ldots p_{r-1} < N^{1-\beta_1}} \frac{N}{p_1 \ldots p_{r-1}} \left( \frac{\beta_1}{\beta_1} \right)^{\frac{1}{2}} + c\beta N (\log \log m)^{r-1} \]
\[
< \left( \alpha^{\frac{1}{2}} + (\log \log N)^{r-1} \left( \frac{\beta_1}{\beta_1} \right)^{\frac{1}{2}} + c\beta (\log \log m)^{r-1} \right) N \]
\[
< c_4 \beta (\log \log m)^{r-1} N. \]

Therefore
\[
\left| \sum_{x < N} e_m(ax^*) \right| \leq c_4 \beta (\log \log m)^{r-1} N + \left| \sum_{x \in \mathcal{G}} e_m(ax^*) \right|. \quad (6)
\]
The sum \( \sum_{x \in \mathcal{G}} e_m(ax^*) \) may be bounded by
\[
\sum_{p_1} \sum_{p_2} \ldots \sum_{p_r} \left| \sum_y e_m(ap_1^*p_2^* \ldots p_r^*y^*) \right|, \quad (7)
\]
where the summations are taken over primes \( p_1, p_2, \ldots, p_r \) and integers \( y \) such that
\[
p_1 \geq p_2 \geq \ldots \geq p_r; \quad p_1 \geq N^{\alpha}; \quad p_r \geq N^{\beta}; \quad p_1 p_2 \ldots p_r \leq N^{1-\beta} \quad (8)
\]
and
\[
y < \frac{N}{p_1 p_2 \ldots p_r}; \quad P(y) \leq p_r.
\]
Note that if \( t \) and \( T \) are such that
\[
(1 - \frac{c_0}{\log m}) p_r < t < p_r, \quad \left(1 - \frac{c_0}{\log m}\right) \frac{N}{p_1 p_2 \ldots p_r} < T < \frac{N}{p_1 p_2 \ldots p_r}, \quad (9)
\]
where \( c_0 > 0 \) is any constant, then we can substitute the condition on \( y \) with
\[
P(y) \leq t; \quad y < T \quad (10)
\]
by changing the sum (7) with an additional term of size at most

\[ \frac{N(\log \log m)^{O(1)}}{\log m}. \]

Now we split the range of summation of primes \( p_1, p_2, \ldots, p_r \) into subintervals of the form \([L, L + L(\log m)^{-1}]\) and choosing suitable \( t \) and \( T \) we obtain that for some numbers \( M_1, M_2, \ldots, M_r \) with

\[ M_1 > M_2 > \ldots > M_r, \quad M_1 \geq \frac{N^\alpha}{2}, \quad M_r \geq \frac{N^\beta}{2}, \quad M_1 M_2 \ldots M_r < N^{1-\beta} \]

(11)
one has

\[ \left| \sum_{x \in \mathcal{G}} e_m(ax^*) \right| < \frac{N(\log \log m)^{O(1)}}{\log m} \]

\[ + (\log m)^{3r} \sum_{p_1 \in I_1} \sum_{p_2 \in I_2} \ldots \sum_{p_r \in I_r} \sum_{y \leq M} \sum_{P(y) \leq M_r} e_m(ap_1^*p_2^* \ldots p_r^*y^*). \]

(12)

where

\[ I_j = \left[ M_j, M_j + \frac{M_j}{\log m} \right], \quad M = \frac{N}{M_1 M_2 \ldots M_r} \geq N^\beta. \]

Denote

\[ W = \sum_{p_1 \in I_1} \sum_{p_2 \in I_2} \ldots \sum_{p_r \in I_r} \sum_{y \leq M} \sum_{P(y) \leq M_r} e_m(ap_1^*p_2^* \ldots p_r^*y^*). \]

Applying the Cauchy-Schwarz inequality, we get

\[ W^2 \leq M_1 M_2 \ldots M_r \sum_{y \leq M} \sum_{z \leq M} \left| \sum_{p_1 \in I_1} \sum_{p_2 \in I_2} \ldots \sum_{p_r \in I_r} e_m\left(ap_1^*p_2^* \ldots p_r^*(y^* - z^*)\right) \right|. \]

Taking into account the contribution from the pairs \( y \) and \( z \) with, say,

\[ \gcd(y - z, m) > e^{10 \log m/\log \log m} \]

and then fixing the pairs \( y \) and \( z \) with \( \gcd(y - z, m) \leq e^{10 \log m/\log \log m} \), we get the bound

\[ W^2 \leq \frac{N^2}{M} + \frac{N^2}{e^{\log m/\log \log m}} + NM|S| \leq 2N^{2-\beta} + \frac{N^2}{M_1 M_2 \ldots M_r}|S|, \]

(13)
where
\[ |S| = \left| \sum_{p_1 \in I_1} \sum_{p_2 \in I_2} \cdots \sum_{p_r \in I_r} e_{m_1} (bp_1^* p_2^* \cdots p_r^*) \right|. \]

Here \( b \) and \( m_1 \) are some positive integers satisfying
\[ \gcd(b, m_1) = 1, \quad m_1 \geq me^{-10 \log m / \log \log m}. \]

We consider two cases, depending on whether \( M_r > N^{\alpha^3} \) or \( M_r \leq N^{\alpha^3} \).

**Case 1.** Let \( M_r > N^{\alpha^3} \). Hence \( M_j > N^{\alpha^3} \) for all \( j = 1, 2, \ldots, r \). The idea is to use Theorem 2 and amplify each of these factors to size \( m^{1/3 + o(1)} \) say and then apply Lemma 1.

Let \( k_1, \ldots, k_r \) be positive integers defined from
\[ M_i^{2k_i - 1} < m_1 \leq M_i^{2k_i + 1}. \]

Since \( M_j > N^{\alpha^3} > m^{\alpha^3} \), it follows that
\[ k_i < \frac{1}{c \alpha^3} = \frac{(\log \log m)^3}{c}. \]

Consequently applying Hölder’s inequality, we get the bound
\[ |S|^{2^{k_1} k_2 \cdots k_r} \leq \left( \prod_{i=1}^r M_i^{2^{k_1} k_2 \cdots k_r - 2k_i} \right) \sum_{p_{11}, \ldots, p_{1k_1} \in I_1 \cap P} \cdots \sum_{q_{r1}, \ldots, q_{rk_r} \in I_r \cap P} e^{2\pi i b \{\ldots\}/m_1}, \]

where \( \{\ldots\} \) indicates the expression
\[ (p_{11}^* + \cdots + p_{1k_1}^* - q_{11}^* - \cdots - q_{1k_1}^*) \cdots (p_{r1}^* + \cdots + p_{rk_r}^* - q_{r1}^* - \cdots - q_{rk_r}^*) \]

Next, we can fix the variables \( q_{ij} \) and then get that for some integers \( \mu_1, \ldots, \mu_r \) there is the bound
\[ \frac{|S|}{M_1 M_2 \cdots M_r} \leq \left( \frac{|S_1|}{M_1^{k_1} M_2^{k_2} \cdots M_r^{k_r}} \right)^{1/(2^{k_1} k_2 \cdots k_r)}, \quad (14) \]

where
\[ S_1 = \sum_{p_{11}, \ldots, p_{1k_1} \in I_1 \cap P} \cdots \sum_{p_{r1}, \ldots, p_{rk_r} \in I_r \cap P} e^{2\pi i b (p_{11}^* + \cdots + p_{1k_1}^* - \mu_1) \cdots (p_{r1}^* + \cdots + p_{rk_r}^* - \mu_r)/m_1}. \]
Let $A_1, \ldots, A_r$ be subsets of $\mathbb{Z}_{m_1}$ defined by

\[
A_1 = \{p_{11} + \ldots + p_{1k_1} - \mu_1; \quad (p_{11}, \ldots, p_{1k_1}) \in (I_1 \cap \mathcal{P})^{k_1}\}, \\
\vdots \\
A_r = \{p_{r1} + \ldots + p_{rk_r} - \mu_r; \quad (p_{r1}, \ldots, p_{rk_r}) \in (I_r \cap \mathcal{P})^{k_r}\},
\]

where $p_{ij}^*$ are calculated modulo $m_1$. Then we have

\[
S_1 = \sum_{\lambda_1 \in A_1} \cdots \sum_{\lambda_r \in A_r} I_1(\lambda_1) \cdots I_r(\lambda_r)e^{2\pi i b_1 \lambda_1 \cdots \lambda_r/m_1},
\]

where $I_j(\lambda)$ is the number of solutions of the congruence

\[
p_{1j}^* + \ldots + p_{kj}^* - \mu_j \equiv \lambda \pmod{m_1}; \quad (p_{1j}, \ldots, p_{kj}) \in (I_j \cap \mathcal{P})^{k_j}.
\]

We apply Cauchy-Schwarz inequality to the sum over $\lambda_1, \ldots, \lambda_{r-1}$ and get

\[
|S_1|^2 \leq J_{2k_1}(M_1) \cdots J_{2k_r}(M_r) \sum_{\lambda_1 \in A_1} \cdots \sum_{\lambda_{r-1} \in A_{r-1}} \left| \sum_{\lambda_r \in A_r} I_r(\lambda_r)e^{2\pi i b_1 \lambda_1 \cdots \lambda_{r-1} \lambda_r/m_1} \right|^2,
\]

where

\[
J_{2k_j}(M_j) = \sum_{\lambda \in A_j}(I_j(\lambda))^2.
\]

Changing the order of summation, we get

\[
|S_1|^2 \leq J_{2k_1}(M_1) \cdots J_{2k_{r-1}}(M_{r-1}) \times \sum_{\lambda_r, \lambda'_r \in A_r} I_r(\lambda_r)I_r(\lambda'_r) \left| \sum_{\lambda_1 \in A_1} \cdots \sum_{\lambda_{r-1} \in A_{r-1}} e^{2\pi i b_1 \lambda_1 \cdots \lambda_{r-1} (\lambda_r - \lambda'_r)/m_1} \right|.
\]

We apply the Cauchy-Schwarz inequality to the sum over $\lambda_r, \lambda'_r$ and get

\[
|S_1|^4 \leq (J_{2k_1}(M_1) \cdots J_{2k_r}(M_r))^2 \times \sum_{\lambda_r, \lambda'_r \in A_r} \left| \sum_{\lambda_1 \in A_1} \cdots \sum_{\lambda_{r-1} \in A_{r-1}} e^{2\pi i b_1 \lambda_1 \cdots \lambda_{r-1} (\lambda_r - \lambda'_r)/m_1} \right|^2.
\]

We can fix $\lambda'_r \in A_r$ such that

\[
|S_1|^4 \leq (J_{2k_1}(M_1) \cdots J_{2k_r}(M_r))^2 |A_r| \times \sum_{\lambda_r \in A'_r} \left| \sum_{\lambda_1 \in A_1} \cdots \sum_{\lambda_{r-1} \in A_{r-1}} e^{2\pi i b_1 \lambda_1 \cdots \lambda_{r-1} \lambda_r/m_1} \right|^2,
\]

\[20\]
where \( A'_r = A_r - \{ \lambda'_r \} \). Using the trivial bound

\[
\left| \sum_{\lambda_1 \in A_1} \ldots \sum_{\lambda_{r-1} \in A_{r-1}} e^{2\pi ib\lambda_1 \ldots \lambda_{r-1} \lambda_r/m_1} \right|^2 \\
\leq |A_1| \cdots |A_{r-1}| \left| \sum_{\lambda_1 \in A_1} \ldots \sum_{\lambda_{r-1} \in A_{r-1}} e^{2\pi ib\lambda_1 \ldots \lambda_{r-1} \lambda_r/m_1} \right|,
\]

we get

\[
|S_1|^4 \leq (J_{2k_i}(M_1) \ldots J_{2k_r}(M_r))^2 |A_1| \cdots |A_r| \times \\
\sum_{\lambda_r \in A'_r} \left| \sum_{\lambda_1 \in A_1} \ldots \sum_{\lambda_{r-1} \in A_{r-1}} e^{2\pi ib\lambda_1 \ldots \lambda_{r-1} \lambda_r/m_1} \right|,
\]

From the definition of \( A_i \) we have \( |A_i| \leq M_i^{k_i} \). From the choice of \( k_i \) and Theorem 2 we also have

\[
J_{2k_i}(M_i) < 2(2k_i)^{k_i} M_i^{k_i}.
\]

Thus,

\[
|S_1|^4 \leq \left( \prod_{i=1}^r (4k_i)^{k_i} M_i^{3k_i} \right) \times \sum_{\lambda_r \in A'_r} \left| \sum_{\lambda_1 \in A_1} \ldots \sum_{\lambda_{r-1} \in A_{r-1}} e^{2\pi ib\lambda_1 \ldots \lambda_{r-1} \lambda_r/m_1} \right|,
\]

Let \( \gamma = 1/10 \) and define \( \varepsilon = \varepsilon(\gamma) > 0 \) to be the absolute constant from Lemma 1. We shall verify that the sets \( A_1, \ldots, A_r \) satisfy the condition of Lemma 1 with \( q = m_1 \) (note that if \( A_r \) satisfies the condition of Lemma 1 then also does \( A'_r \)). From the definition of \( A_i \) and the connection between the cardinality of a set and the corresponding additive energies, we have

\[
|A_i| \geq \frac{(M_i/(2 \log M_i))^{2k_i}}{J_{2k_i}(M_i)} \geq \frac{M_i^{k_i}}{2(2k_i)^{k_i} (2 \log M_i)^{2k_i}}.
\]

From the choice of \( k_i \) it then follows that

\[
|A_i| \geq \frac{m_1^{1/3}}{2(2k_i)^{k_i} (2 \log M_i)^{2k_i}} = m_1^{1/3+o(1)}.
\]

Thus, the first condition \( |A_i| > m_1^{1/10} \) is satisfied.
Next, let $q_1 | m_1$, $q_1 > m_1^5$ and let $\xi \in \mathbb{Z}_{q_1}$. Let $T_i$ be the number of solutions of the congruence

$$x \equiv \xi \pmod{q_1}; \quad x \in A_i.$$ 

It follows that $T_i$ is bounded by the number of solutions of the congruence

$$p_1^* + \ldots + p_{k_i}^* \equiv \xi + \mu_1 \pmod{q_1}; \quad (p_1, \ldots, p_{k_i}) \in (I_i \cap \mathcal{P})^{k_i}.$$ 

Consider two possibilities here. If $M_i > q_1^{1/8}$ say, then we fix $p_2, \ldots, p_{k_i}$ and we have at most $1 + M_i q_1^{-1}$ possibilities for $p_1$. Thus, using (16), we get

$$\left(1 + \frac{M_i}{q_1}\right) M_i^{k_i-1} < \frac{M_i^k}{q_1^{1/9}} < q_1^{-1/10} |A_i|.$$ 

Therefore, in this case the condition of Lemma 1 is satisfied.

Let now $M_i < q_1^{1/8}$. Define $k_i'$ from the condition

$$M_i^{4k_i' + 1} < q_1 < M_i^{4k_i' + 5}.$$ 

We then have $2k_i' < k_i$. Thus,

$$T_i \leq M_i^{k_i - 2k_i'} J_{2k_i'}(M_i),$$

where $J_{2k_i'}(M_i)$, as before, denotes the number of solutions of the congruence

$$p_1^* + \ldots + p_{k_i'}^* \equiv p_{k_i'+1}^* + \ldots + p_{2k_i'}^* \pmod{q_1}; \quad (p_1, \ldots, p_{2k_i'}) \in (I_i \cap \mathcal{P})^{2k_i'}.$$ 

From the choice of $k_i$ and Theorem 2 we get that

$$J_{2k_i'}(M_i) < 2(2k_i)^{k_i} M_i^{k_i'}. $$

Therefore, using (16)

$$T_i \leq 2(2k_i)^{k_i} M_i^{k_i - k_i'} \leq 2(2k_i)^{k_i} M_i^{k_i} q_1^{-1/9} < q_1^{-1/10} |A_i|.$$ 

Thus, the condition of Lemma 1 is satisfied and hence we have

$$\sum_{\lambda_r \in A_r} \sum_{\lambda_1 \in A_1} \ldots \sum_{\lambda_{r-1} \in A_{r-1}} e^{2\pi ib\lambda_1 \ldots \lambda_{r-1} \lambda_r / m_1} \left| m^{-\tau} |A_1| \ldots |A_r| \right| < m^{-\gamma} |A_1| \ldots |A_r|.$$
for some absolute constant $\tau > 0$ (see the discussion followed to Lemma 1). Inserting this into (15) and using estimates $k_i \ll (\log \log m)^{3}$ and $|A_i| \leq M_i^{k_i}$, we get

$$|S_1|^4 < m^{-\tau/5}M_1^{k_1}M_2^{k_2} \ldots M_r^{k_r}.$$  

Thus, from (14) it follows that

$$\frac{|S|}{M_1M_2 \ldots M_r} < m^{-c_1(\log \log m)^{-3\gamma}}$$

and from (13) we get

$$W < 2N^{1-0.5\beta}.$$  

Inserting this into (12) and using (6), we conclude the proof.

**Case 2.** Let now $M_r < N^{\alpha_3}$. In this case we fix all the factors except $p_1, p_2, p_r$. We apply Corollary 3 or Corollary 4. We either choose for the first factor $p_1$ and the second factor $p_2$ or for the first factor $p_1p_r$ and the second factor $p_2$. Because $M_1 > N^{\alpha_1}$ and $M_r < N^{\alpha_3}$ we will get in one of the cases the required saving. Let us give some details of this argument.

Define $k_1, k_2 \in \mathbb{Z}_+$ such that

$$M_1^{k_1-1} < m_1^{1/2} \leq M_1^{k_1}, \quad M_2^{k_2-1} < m_1^{1/2} \leq M_2^{k_2}.$$  

From the definition of $\alpha$ and $\beta$ we have

$$k_1 \leq \frac{1}{c} \log \log m; \quad k_2 \leq \frac{1}{c\beta} \ll \frac{(\log m)^{1/2}}{\log \log m}.$$  

Let

$$\delta = \frac{k_1 \log M_r}{3\log M_1}.$$  

Note that $\delta \leq \frac{1}{c}(\log \log m)^{-1}$. We further consider three subcases:

**Case 2.1.** Let $M_1^{k_1-1+\delta} < m_1^{1/2} \leq M_1^{k_1-\delta}$. Then we apply Corollary 3 and get

$$\frac{|S|}{M_1M_2 \ldots M_r} < (\log m)^{1/2} \left( \frac{M_1^{k_1-1}}{m_1^{1/2}} + \frac{m_1^{1/2}}{M_1^{k_1}} \right)^{1/(2k_1k_2)} \leq 2(\log m)^{1/2}M_1^{-\delta/(2k_1k_2)} = 2(\log m)^{1/2}M_r^{-1/(6k_2)}.$$  

23
Using the upper bound for $k_2$ and the lower bound $M_r \geq N^\beta$ it follows that
\[
\frac{|S|}{M_1 M_2 \ldots M_r} < 2(\log m)^{1/2} e^{-0.01c^2\beta^2 \log m}.
\]

**Case 2.2.** Let $M_1^{k_1-\delta} < m_1^{1/2} \leq M_1^{k_1}$. We apply Corollary 4 in the form
\[
\frac{|S|}{M_1 M_2 \ldots M_r} < (\log m)^{(M_1 M_r)^{k_1-1} \frac{m_1^{1/2}}{m_1^{1/2}} + \frac{m_1^{1/2}}{(M_1 M_r)^{k_1}})^{1/(2k_1k_2)}
\]
\[
< (\log m)^{(\frac{M_r^{k_1-1} M_1^{1-\delta}}{M_1^{1-\delta}} + \frac{1}{M_1^{k_1}})}^{1/(2k_1k_2)}.
\]

**Case 2.3.** Let now $M_1^{k_1-1} < m_1^{1/2} \leq M_1^{k_1-1+\delta}$. Then $k_1 \geq 2$ and we apply Corollary 4 with $k_1$ replaced by $k_1 - 1$ in the form
\[
\frac{|S|}{M_1 M_2 \ldots M_r} < (\log m)^{1/2} \left(\frac{(M_1 M_r)^{k_1-2}}{m_1^{1/2}} + \frac{m_1^{1/2}}{(M_1 M_r)^{k_1-1}}\right)^{1/(2k_1k_2)}
\]
\[
< (\log m)^{1/2} \left(\frac{M_r^{k_1-2} M_1^{1-\delta}}{M_1} + \frac{M_1^{\delta}}{M_r^{k_1-1}}\right)^{1/(2k_1k_2)}.
\]

In all three subcases we get the bound
\[
\frac{|S|}{M_1 M_2 \ldots M_r} < 2(\log m)e^{-c'\beta^2 \log m}
\]
for some constant $c' > 0$. Thus, we eventually arrive at the bound
\[
W < Ne^{-c'\beta^2 \log m \log m}
\]
for some constant $c' > 0$. Inserting this into (12) and using (6), we conclude that
\[
\left| \sum_{x < N} e_m(ax^r) \right| \ll \beta(\log \log m)^{r-1} N + Ne^{-c''\beta^2 \log m \log m} \ll \frac{(\log \log m)^r}{(\log m)^{1/2}} N.
\]
References

[1] U. Betke, M. Henk and J. M. Wills, ‘Successive-minima-type inequalities’, *Discr. Comput. Geom.*, 9 (1993), 165–175.

[2] J. Bourgain, ‘The sum-product theorem in \( \mathbb{Z}_q \) with \( q \) arbitrary’, *J. Analyse Math.* 106 (2008), 1–93.

[3] J. Bourgain and M. Z. Garaev, ‘Sumsets of reciprocals in prime fields and multilinear Kloosterman sums’, *Preprint*.

[4] N. G. de Bruijn, ‘On the number of positive integers \( \leq x \) and free prime factors > \( y \), II’, *Indag. Math.* 28 (1966), 239-247.

[5] J. Friedlander and H. Iwaniec, *The Brun-Titchmarsh theorem*, *Analytic number theory* (Kyoto, 1996), 85-93, London Math. Soc. Lecture Note Ser., 247, Cambridge Univ. Press, Cambridge, 1997.

[6] J. Friedlander and H. Iwaniec, *Opera de Cribro*, American Mathematical Society, Colloquium Publications, 57, 2010.

[7] H. Iwaniec and E. Kowalski, *Analytic number theory*, Amer. Math. Soc., Providence, RI, 2004.

[8] A. A. Karatsuba, ‘New estimates of short Kloosterman sums’, *Math. Notes* 88:3 (2010), 347–359. Prepared by E. A. Karatsuba, M. A. Korolev and I. S. Rezvyakova on notes and drafts of A. A. Karatsuba.

[9] A. A. Karatsuba, ‘Analogues of Kloosterman sums’, *Izv. Math.* 59:5 (1995), 971–981.

[10] A. A. Karatsuba, ‘Fractional parts of functions of a special form’, *Izv. Math.* 59:4 (1995), 721–740.

[11] M. A. Korolev, ‘Incomplete Kloosterman sums and their applications’, *Izv. Math.* 64:6 (2000), 1129-1152.

[12] M. A. Korolev, ‘Short Kloosterman sums with weights’, *Math. Notes* 88:3 (2010), 374-385.

[13] T. Tao and V. Vu, *Additive combinatorics*, Cambridge Stud. Adv. Math., 105, Cambridge University Press, Cambridge, 2006.