ACTA ARITHMETICA
164.1 (2014)

Kloosterman sums in residue rings

by

J. Bourgain (Princeton, NJ) and M. Z. Garaev (Morelia)

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 the Brun–Titchmarsh theorem, and, making use of multilinear exponential sum bounds for general moduli, we estimate short Kloosterman sums, hence generalizing our earlier work [3] to the setting of general moduli.

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

2. Statement of our results. We start with the additive properties of the reciprocal-set.

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

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

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.

2010 *Mathematics Subject Classification*: Primary 11L05.
Key words and phrases: Kloosterman sums, multilinear exponential sums, general modulus, congruences.

DOI: 10.4064/aa164-1-4

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

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

satisfies

$$J_{2k} < (2k)^k \Big(\frac{N^{2k-1}}{m} + 1 \Big) N^k.$$

We recall that an *incomplete Kloosterman sum* is a sum of the form

$$\sum_{x=M+1}^{M+N} e_m(ax^* + bx),$$

where a and b are integers with $\gcd(a, m) = 1$. 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

$$\Big| \sum_{x=1}^{m} e_m(ax^* + bx) \Big| \le \tau(m) m^{1/2}$$

(see for example [7, Corollary 11.12]). This implies that for $N < m$ one has

$$\Big| \sum_{x=M+1}^{M+N} e_m(ax^* + bx) \Big| < m^{1/2+o(1)}.$$

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

$$S = \sum_{x_1=M_1+1}^{M_1+N_1} \sum_{x_2=M_2+1}^{M_2+N_2} \alpha_1(x_1)\alpha_2(x_2) e_m(ax_1^* x_2^*),$$

where $\alpha_i(x_i) \in \mathbb{C}$, $|\alpha_i(x_i)| \le 1$, 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 $I_1 = [1, N_1]$ and $I_2 = [1, N_2]$. Then uniformly over all positive integers k_1, k_2 and $\gcd(a, m) = 1$ we have*

$$\begin{aligned} \Big| \sum_{x_1 \in I_1} \sum_{x_2 \in I_2} \alpha_1(x_1)\alpha_2(x_2) e_m(ax_1^* x_2^*) \Big| \\ < (2k_1)^{45k_1^2/k_2} (2k_2)^{45k_2^2/k_1} (\log m)^{2(k_1/k_2 + k_2/k_1)} \\ \times \Big(\frac{N_1^{k_1-1}}{m^{1/2}} + \frac{m^{1/2}}{N_1^{k_1}} \Big)^{1/(2k_1k_2)} \Big(\frac{N_2^{k_2-1}}{m^{1/2}} + \frac{m^{1/2}}{N_2^{k_2}} \Big)^{1/(2k_1k_2)} N_1 N_2. \end{aligned}$$

Given N_1, N_2 we choose k_1, k_2 such that

$$N_1^{2(k_1-1)} < m \le N_1^{2k_1}, \qquad N_2^{2(k_2-1)} < m \le N_2^{2k_2}$$

and the bound will be nontrivial unless each of N_1 and N_2 is within m^{ε}-ratio of an element of $\{m^{1/(2l)} : l \in \mathbb{Z}_+\}$. Thus, we have the following

Corollary 1. *Let $I_1 = [1, N_1]$ and $I_2 = [1, N_2]$, where for $i = 1$ or $i = 2$,*

$$N_i \notin \bigcup_{j \ge 1} [m^{1/(2j)-\varepsilon},\, m^{1/(2j)+\varepsilon}].$$

Then

$$\max_{(a,m)=1} \Big| \sum_{x_1=1}^{N_1} \sum_{x_2=1}^{N_2} \alpha_1(x_1)\alpha_2(x_2) e_m(a x_1^* x_2^*) \Big| < m^{-\delta} N_1 N_2$$

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 $x^{\theta} \le q \le 2x^{\theta}$, where $\theta < 1$ is close to 1. Then*

$$\pi(x; q, a) < \frac{cx}{\phi(q) \log (x/q)}$$

with $c = 2 - c_1(1-\theta)^2$, for some absolute constant $c_1 > 0$ and all x sufficiently large in terms of θ.

Recall that for $(a, q) = 1$, $\pi(x; q, a)$ denotes the number of primes $p \le x$ with $p \equiv a \pmod q$. The constants implied in Theorem 4 are 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 sum.

Theorem 5. *Let $N > m^c$, where c is a small fixed positive constant. Then*

$$\max_{(a,m)=1} \Big| \sum_{n \le N} e_m(an^*) \Big| < \frac{(\log \log m)^{O(1)}}{(\log m)^{1/2}} N,$$

where the implied constant 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

$$\sum_{n=1}^{m} e_m(an^*) = \mu(m),$$

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 arbitrarily small fixed positive 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 $|A_i| > q^{\gamma}$ $(1 \le i \le k)$ and also*

$$\max_{\xi \in \mathbb{Z}_{q_1}} |A_i \cap \pi_{q_1}^{-1}(\xi)| < q_1^{-\gamma}|A_i| \quad \textit{for all } q_1 \mid q,\ q_1 > q^{\varepsilon}.$$

Then

$$\max_{\xi \in \mathbb{Z}_q^*} \Big| \sum_{x_1 \in A_1} \cdots \sum_{x_k \in A_k} e_q(\xi x_1 \ldots x_k) \Big| < C q^{-\tau} |A_1| \ldots |A_k|.$$

Here, $|A \cap \pi_{q_1}^{-1}(\xi)|$ 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

$$\max_{\xi \in \mathbb{Z}_q^*} \sum_{x_1 \in A_1} \cdots \sum_{x_{k-1} \in A_{k-1}} \Big| \sum_{x_k \in A_k} e_q(\xi x_1 \ldots x_{k-1} x_k) \Big| < C q^{-\tau} |A_1| \ldots |A_k|.$$

Indeed, applying the Cauchy–Schwarz inequality, it follows that

$$\Big(\sum_{x_1 \in A_1} \cdots \sum_{x_{k-1} \in A_{k-1}} \Big| \sum_{x_k \in A_k} e_q(\xi x_1 \ldots x_{k-1} x_k) \Big| \Big)^2 \\ \le |A_1| \ldots |A_{k-1}| \sum_{x_k' \in A_k} \Big| \sum_{x_1 \in A_1} \cdots \sum_{x_k \in A_k} e_q(\xi x_1 \ldots x_{k-1}(x_k - x_k')) \Big|.$$

We fix $x_k' \in A_k$ such that

$$\Big(\sum_{x_1 \in A_1} \cdots \sum_{x_{k-1} \in A_{k-1}} \Big| \sum_{x_k \in A_k} e_q(\xi x_1 \ldots x_{k-1} x_k) \Big| \Big)^2 \\ \le |A_1| \ldots |A_{k-1}|\, |A_k| \Big| \sum_{x_1 \in A_1} \cdots \sum_{x_{k-1} \in A_{k-1}} \sum_{x_k \in A_k'} e_q(\xi x_1 \ldots x_{k-1} x_k \Big|,$$

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 body $D \subset \mathbb{R}^n$, symmetric with respect to 0. Recall that, for a lattice $\Gamma \subset \mathbb{R}^n$ and $i = 1, \dots, n$, the ith *successive minimum* $\lambda_i(D, \Gamma)$ of the set D with respect to the lattice Γ is defined as the minimal number λ such that the set λD contains i linearly independent vectors of the lattice Γ. Obviously, $\lambda_1(D, \Gamma) \le \dots \le \lambda_n(D, \Gamma)$. 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*

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

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*

$$\prod_{i=1}^{n} \min\{\lambda_i(D, \Gamma), 1\} \le \frac{(2n+1)!!}{|D \cap \Gamma|}.$$

We also need the following lemma due to Karatsuba [9].

Lemma 3. *The following bound holds:*

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

4. Proofs of Theorems 1–3

Proof of Theorem 1. It suffices to consider the case $kN^k < m$ as otherwise the statement is trivial. For $\lambda = 0, 1, \dots, m-1$ denote

$$J(\lambda) = \{(x_1, \dots, x_k) \in I^k : x_1^* + \dots + x_k^* \equiv \lambda \pmod{m}\}.$$

Let

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

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
$$D = \{(u,v)\in\mathbb{R}^2 : |u|\le N^k,\ |v|\le kN^{k-1}\}.$$
If we denote by μ_1,μ_2 the successive minima of the body D with respect to the lattice Γ_λ, Corollary 2 yields
$$\prod_{i=1}^{2}\min\{\mu_i,1\}\le \frac{15}{|\Gamma_\lambda\cap D|}.$$
Observe that for $(x_1,\dots,x_k)\in J(\lambda)$ one has
$$\lambda x_1\dots x_k \equiv x_2\dots x_k+\dots+x_1\dots x_{k-1} \pmod m,$$
implying
$$(x_1\dots x_k,\ x_2\dots x_k+\dots+x_1\dots x_{k-1})\in \Gamma_\lambda\cap D.$$
Thus, for $\lambda\in\Omega$ we have $\mu_1\le 1$. We split the set Ω into two subsets:
$$\Omega' = \{\lambda\in\Omega : \mu_2\le 1\},\qquad \Omega''=\{\lambda\in\Omega:\mu_2>1\}.$$
We have
$$J_{2k} = \sum_{\lambda\in\Omega'}|J(\lambda)|^2 + \sum_{\lambda\in\Omega''}|J(\lambda)|^2. \tag{1}$$

Case 1: $\lambda\in\Omega'$, that is, $\mu_2\le 1$. Let $(u_i,v_i)\in\mu_i D\cap\Gamma_\lambda$, $i=1,2$, be linearly independent. Then
$$0\ne u_1v_2-v_1u_2\equiv u_1\lambda u_2 - u_2\lambda u_1\equiv 0 \pmod m,$$
whence
$$|u_1v_2-v_1u_2|\ge m.$$
Also
$$|u_1v_2-v_1u_2|\le 2k\mu_1\mu_2N^{2k-1}\le \frac{30kN^{2k-1}}{|\Gamma_\lambda\cap D|}.$$
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 $|u|\le N^k$, $|v|\le kN^{k-1}$ is bounded by
$$|\Gamma_\lambda\cap D|\le \frac{30kN^{2k-1}}{m}. \tag{2}$$
Note that for $\lambda\in\Omega'$ the sets
$$\mathcal{W}_\lambda := \{(u,v) : (u,v)\in\Gamma_\lambda\cap D,\ \gcd(u,m)=1\}$$

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

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

we get

$$\sum_{\lambda\in\Omega'} |J(\lambda)|^2 = \sum_{\lambda\in\Omega'} \Big(\sum_{\substack{(u,v)\in\Gamma_\lambda\cap D\\ \gcd(u,m)=1}} \ \sum_{(x_1,\dots,x_k)\in S(u,v)} 1\Big)^2.$$

Applying the Cauchy–Schwarz inequality and taking into account (2), we get

$$\sum_{\lambda\in\Omega'} |J(\lambda)|^2 \le \frac{30kN^{2k-1}}{m} \sum_{\lambda\in\Omega'} \ \sum_{\substack{(u,v)\in\Gamma_\lambda\cap D\\ \gcd(u,m)=1}} \Big(\sum_{(x_1,\dots,x_k)\in S(u,v)} 1\Big)^2. \tag{3}$$

From the disjointness of the sets W_λ it follows that the sum on the right is bounded by the number of solutions of the system

$$\begin{cases} x_1\dots x_k = y_1\dots y_k,\\ x_1\dots x_{k-1} + \dots + x_2\dots x_k = y_2\dots y_k + \dots + y_1\dots y_{k-1}, \end{cases}$$

in positive integers $x_i, y_j \le N$ coprime to m. Hence, by Lemma 3,

$$\sum_{\lambda\in\Omega'} |J(\lambda)|^2 < 30k(2k)^{80k^3}(\log N)^{4k^2}\frac{N^{3k-1}}{m}. \tag{4}$$

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 $\widehat{\lambda} \in \mathbb{Q}$ such that

$$\widehat{\lambda} x_1\dots x_k = x_2\dots x_k + \dots + x_1\dots x_{k-1} \quad \text{for } (x_1,\dots,x_k) \in J(\lambda).$$

Thus,

$$\begin{aligned}\sum_{\lambda\in\Omega''} |J(\lambda)|^2 &\le \sum_{\widehat{\lambda}\in\mathbb{Q}} \Big|\{(x_1,\dots,x_k)\in I^k : \frac{1}{x_1}+\dots+\frac{1}{x_k} = \widehat{\lambda}\Big|^2\\ &= \Big|\Big\{(x_1,\dots,x_{2k})\in[1,N]^{2k} : \frac{1}{x_1}+\dots+\frac{1}{x_k} = \frac{1}{x_{k+1}}+\dots+\frac{1}{x_{2k}}\Big\}\Big|\\ &< (2k)^{80k^3}(\log N)^{4k^2}N^k.\end{aligned}$$

Inserting this and (4) into (1), we obtain

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

which concludes the proof of Theorem 1.

Proof of Theorem 2. This proof follows the same lines, with the only difference that instead of Lemma 3 one should apply the bound

$$\left|\left\{(x_1,\dots,x_{2k})\in([1,N]\cap\mathcal{P})^{2k} : \frac{1}{x_1}+\dots+\frac{1}{x_k}=\frac{1}{x_{k+1}}+\dots+\frac{1}{x_{2k}}\right\}\right| < (2k)^k\left(\frac{N}{\log N}\right)^k.$$

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,

$$|S|^{k_2}\le N_1^{k_2-1}\sum_{x_1\in I_1}\Big|\sum_{x_2\in I_2}\alpha_2(x_2)e_m(ax_1^*x_2^*)\Big|^{k_2}.$$

Thus, for some $\sigma(x_1)\in\mathbb{C}$ with $|\sigma(x_1)|=1$,

$$|S|^{k_2}\le N_1^{k_2-1}\sum_{y_1,\dots,y_{k_2}\in I_2}\Big|\sum_{x_1\in I_1}\sigma(x_1)e_m(ax_1^*(y_1^*+\dots+y_{k_2}^*)\Big|.$$

Again by Hölder's inequality,

$$|S|^{k_1k_2}\le N_1^{k_1k_2-k_1}N_2^{k_1k_2-k_2}\sum_{\lambda=0}^{p-1}J_{k_2}(\lambda;N_2)\Big|\sum_{x_1\in I_1}\sigma(x_1)e_m(ax_1^*\lambda\Big|^{k_1},$$

where $J_k(\lambda;N)$ is the number of solutions of the congruence

$$x_1^*+\dots+x_k^*\equiv\lambda\ (\mathrm{mod}\ m),\qquad x_i\in[1,N].$$

Then applying the Cauchy–Schwarz inequality and using

$$\sum_{\lambda=0}^{p-1}J_{k_2}(\lambda;N_2)^2=J_{2k_2}(N_2),\qquad \sum_{\lambda=0}^{p-1}\Big|\sum_{x_1\in I_1}\sigma(x_1)e_m(ax_1^*\lambda\Big|^{2k_1}\le mJ_{2k_1}(N_1),$$

we get

$$|S|^{2k_1k_2}\le mN_1^{2k_1k_2-2k_1}N_2^{2k_1k_2-2k_2}J_{2k_1}(N_1)J_{2k_2}(N_2). \tag{5}$$

Applying Theorem 1, we obtain

$$|S|^{2k_1k_2}\le(2k_1)^{90k_1^3}(2k_2)^{90k_2^3}(\log N_1)^{4k_1^2}(\log N_2)^{4k_2^2}\times N_1^{2k_1k_2}N_2^{2k_1k_2}\left(\frac{N_1^{k_1-1}}{m^{1/2}}+\frac{m^{1/2}}{N_1^{k_1}}\right)\left(\frac{N_2^{k_2-1}}{m^{1/2}}+\frac{m^{1/2}}{N_2^{k_2}}\right).$$

Thus,

$$|S| < (2k_1)^{45k_1^2/k_2}(2k_2)^{45k_2^2/k_1}(\log m)^{2(k_1/k_2+k_2/k_1)}$$
$$\times \left(\frac{N_1^{k_1-1}}{m^{1/2}} + \frac{m^{1/2}}{N_1^{k_1}}\right)^{1/(2k_1k_2)} \left(\frac{N_2^{k_2-1}}{m^{1/2}} + \frac{m^{1/2}}{N_2^{k_2}}\right)^{1/(2k_1k_2)} N_1N_2,$$

which finishes the proof of Theorem 3.

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

$$\begin{aligned}
\mathcal{A} &= \{n \le x : n \equiv a \pmod q\},\\
\mathcal{A}_d &= \{n \in \mathcal{A} : n \equiv 0 \pmod d\},\\
S(\mathcal{A}, z) &= |\{n \in \mathcal{A} : (n,p) = 1 \text{ for } p < z, (p,q) = 1\}|,\\
r_d &= |\mathcal{A}_d| - \frac{x}{qd}.
\end{aligned}$$

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

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

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

Take an integer k such that

$$\frac{1}{2k-1} \le \frac{\delta}{2} < \frac{1}{2k-3}.$$

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

$$N = q^{1/(2k-1)}, \qquad M = D/N.$$

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

$$S(\mathcal{A}, z) \le \frac{(2+\varepsilon)x}{\phi(q)\log D} + R(M,N).$$

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

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

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

$$0.5M_1 < m \le M_1, \quad 0.5N_1 < n \le N_1$$

for some $1 \le M_1 \le M$ and $1 \le N_1 \le N$ with $M_1N_1q > x^{1-\varepsilon}$. Then according to [6, p. 262] we have the bound

$$R(M,N) \ll \frac{x}{qM_1N_1} \sum_{0<|h|\le H} \sum_{m\sim M_1} \Big|\sum_{n\sim N_1} \gamma(h;n)e_q(ahm^*n^*)\Big| + \frac{x^{1-\varepsilon}}{q},$$

where

$$H = qM_1N_1x^{3\varepsilon-1} \le qDx^{3\varepsilon-1} \ll x^{c\delta^3+3\varepsilon}.$$

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

$$R(M,N) \ll x^{3\varepsilon} \sum_{m\le M} \Big|\sum_{n\le N} \gamma(n)e_{q_1}(a_1m^*n^*)\Big| + \frac{x^{1-\varepsilon}}{q},$$

where, say, $q^{1-\delta^2} \le q_1 \le q$ and $\gcd(a_1,q_1) = 1$. Then our Theorem 3 applied with $k_1 = k$ and $k_2 \sim k$ (defined from $M^{2(k_2-1)} < m \le M^{2k_2}$) 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

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

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, and $\gcd(a,m) = 1$. Then for any coefficients $\alpha(p), \beta(q) \in \mathbb{C}$ with $|\alpha(p)|, |\beta(q)| \le 1$, we have*

$$\Big|\sum_{p\le N_1} \sum_{q\le N_2} \alpha(p)\beta(q)e_m(ap^*q^*)\Big|$$
$$< (2k_1)^{1/k_2}(2k_2)^{1/k_1}\bigg(\frac{N_1^{k_1-1}}{m^{1/2}} + \frac{m^{1/2}}{N_1^{k_1}}\bigg)^{1/(2k_1k_2)}\bigg(\frac{N_2^{k_2-1}}{m^{1/2}} + \frac{m^{1/2}}{N_2^{k_2}}\bigg)^{1/(2k_1k_2)} N_1N_2,$$

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))

$$|S|^{2k_1k_2} \le mN_1^{2k_1k_2-2k_1} N_2^{2k_1k_2-2k_2} J_{2k_1}(N_1)J_{2k_2}(N_2),$$

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

$$p_1^* + \cdots + p_k^* \equiv p_{k+1}^* + \cdots + p_{2k}^* \pmod m$$

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

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

$$\frac{1}{p_1q_1} + \cdots + \frac{1}{p_kq_k} = \frac{1}{p_{k+1}q_{k+1}} + \cdots + \frac{1}{p_{2k}q_{2k}}$$

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

$$T_{2k}(K, L) < k^{4k}\left(\frac{K}{\log K}\right)^k \left(\frac{L}{\log L}\right)^k.$$

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

$$\frac{p_1 \cdots p_{2k}q_1 \cdots q_{2k}}{p_{i_0}q_{i_0}} \equiv 0 \pmod{p_{i_0}q_{i_0}}.$$

Since $p_i \ne q_j$, it follows that p_{i_0} appears in the sequence $p_1, \ldots, p_{2k}$ at least twice. Thus, the sequence $p_1, \ldots, p_{2k}$ contains at most k different prime numbers. Accordingly, 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 proof of Theorems 1 and 2, with the only difference that in the course of proof we replace 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 congruence*

$$\frac{1}{p_1q_1} + \cdots + \frac{1}{p_kq_k} \equiv \frac{1}{p_{k+1}q_{k+1}} + \cdots + \frac{1}{p_{2k}q_{2k}} \pmod m$$

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 with $2L < K$. Then for any coefficients $\alpha(p), \beta(q; r) \in \mathbb{C}$ with $|\alpha(p)|, |\beta(q; r)| \le 1$, we have*

$$\max_{\gcd(a,m)=1}\Big|\sum_{p\le N}\sum_{0.5K<q\le K}\sum_{r\le L}\alpha(p)\beta(q;r)e_m(ap^*q^*r^*)\Big|$$
$$< k_1^{2/k_2}k_2^{2/k_1}\Big(\frac{N^{k_1-1}}{m^{1/2}}+\frac{m^{1/2}}{N^{k_1}}\Big)^{1/(2k_1k_2)}\Big(\frac{(KL)^{k_2-1}}{m^{1/2}}+\frac{m^{1/2}}{(KL)^{k_2}}\Big)^{1/(2k_1k_2)}NKL,$$

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 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

$$\mathcal{G} = \{x < N : p_1 \ge N^\alpha,\ p_r \ge N^\beta,\ p_1 \dots p_r < N^{1-\beta}\},$$

where $p_1 \ge \dots \ge p_r$ are the largest prime factors of x and

$$0.1 > \alpha > \beta > 1/\log N$$

are parameters to specify. Note that the number of positive integers not exceeding N which are products of at most $r-1$ prime numbers is estimated by

$$\sum_{k=1}^{r-1}\sum_{\substack{p_1\dots p_k\le N\\ p_1\ge\dots\ge p_k}} 1 \ll \frac{N}{\log N} + \sum_{k=2}^{r-1}\sum_{p_2\dots p_k\le N^{(k-1)/k}} \frac{N}{p_2\dots p_k\log(N/(p_2\dots p_k))}$$
$$\ll \frac{N}{\log N} + \sum_{k=2}^{r-1}\sum_{p_2\le N}\dots\sum_{p_k\le N}\frac{N}{p_2\dots p_k\log N}$$
$$\ll \frac{N(\log\log N)^{r-1}}{\log N}.$$

Here and below, the implied constants may depend only on r. Hence,

$$N - |\mathcal{G}| \le \frac{cN(\log\log N)^{r-1}}{\log N} + \sum_{\substack{x<N\\ p_1<N^\alpha}} 1 + \sum_{\substack{x<N\\ p_r<N^\beta}} 1 + \sum_{\substack{x<N\\ p_1\dots p_r>N^{1-\beta}}} 1,$$

for some constant $c = c(r) > 0$. Next, we have

$$\sum_{\substack{x<N\\ p_1\dots p_r>N^{1-\beta}}} 1 \le \sum_{\substack{y<N^\beta\\ p_1\dots p_r<N/y\\ p_1\ge\dots\ge p_r\ge P(y)}} 1$$
$$\ll \sum_{y<N^\beta}\sum_{\substack{p_2\dots p_r<(N/y)^{(r-1)/r}\\ p_2\ge\dots\ge p_r\ge P(y)}} \frac{N}{yp_2\dots p_r\log(N/(yp_2\dots p_r))}$$
$$\ll \frac{N}{\log N}\sum_{y<N^\beta}\sum_{P(y)\le p_r\le N^{1/r}} \frac{\big(\log\frac{\log N}{\log p_r}\big)^{r-2}}{yp_r}.$$

We would like to prove that the quantity on the right hand side is $\ll \beta N\big(\log\frac{1}{\beta}\big)^{r-1}$. This is trivially true if $N^{\beta^2}<2$, as in this case we have

$$\begin{aligned}\frac{N}{\log N}\sum_{y<N^\beta}\sum_{P(y)\le p_r\le N^{1/r}}\frac{(\log\frac{\log N}{\log p_r})^{r-2}}{yp_r}\\ &\ll \frac{N}{\log N}(\log\log N)^{r-2}\sum_{y<N^\beta}\sum_{p_r\le N}\frac{1}{yp_r}\\ &\ll \beta N(\log\log N)^{r-1}\ll \beta N(\log\tfrac{1}{\beta})^{r-1}.\end{aligned}$$

Let now $N^{\beta^2}\ge 2$. Since

$$\frac{N}{\log N}\sum_{y<N^\beta}\sum_{N^{\beta^2}\le p_r\le N}\frac{(\log\frac{\log N}{\log p_r})^{r-2}}{yp_r}\ll \beta N\big(\log\tfrac{1}{\beta}\big)^{r-1},$$

it follows that

(6)
$$\sum_{\substack{x<N\\ p_1\ldots p_r>N^{1-\beta}}}1\ll \frac{N}{\log N}\sum_{y<N^\beta}\sum_{P(y)\le p_r\le N^{\beta^2}}\frac{(\log\frac{\log N}{\log p_r})^{r-2}}{yp_r}+\beta N\big(\log\tfrac{1}{\beta}\big)^{r-1}.$$

Next, splitting the sum over p_r into intervals of the type $N^{\beta^{k+1}}\le p_r\le N^{\beta^k}$ and denoting by k_0 the largest positive integer with $N^{\beta^{k_0}}\ge 2$ we get

$$\begin{aligned}\sum_{y<N^\beta}\sum_{P(y)\le p_r\le N^{\beta^2}}\frac{(\log\frac{\log N}{\log p_r})^{r-2}}{yp_r}&\le\sum_{k=2}^{k_0}\sum_{\substack{y<N^\beta\\ P(y)\le N^{\beta^k}}}\sum_{N^{\beta^{k+1}}\le p_r\le N^{\beta^k}}\frac{(\log\frac{\log N}{\log p_r})^{r-2}}{yp_r}\\ &\ll\sum_{k=2}^{k_0}\sum_{\substack{y<N^\beta\\ P(y)\le N^{\beta^k}}}\frac{(k\log\frac{1}{\beta})^{r-1}}{y}=(\log\tfrac{1}{\beta})^{r-1}\sum_{k=2}^{k_0}\Bigg(k^{r-1}\sum_{\substack{y<N^\beta\\ P(y)\le N^{\beta^k}}}\frac{1}{y}\Bigg)\\ &\ll\big(\log\tfrac{1}{\beta}\big)^{r-1}\sum_{k=2}^{k_0}\Bigg(k^{r-1}\sum_{\substack{N^{\beta^{k/2}}\le y<N^\beta\\ P(y)\le N^{\beta^k}}}\frac{1}{y}\Bigg)+\big(\log\tfrac{1}{\beta}\big)^{r-1}\sum_{k=2}^{k_0}k^{r-1}(\log N^{\beta^{k/2}}).\end{aligned}$$

Then observing that

$$\sum_{k\ge 2}k^{r-1}(\log N^{\beta^{k/2}})\ll\beta\log N\sum_{k\ge 2}\frac{k^{r-1}}{10^{(k-2)/2}}\ll\beta\log N,$$

from (6) it follows that

$$\sum_{\substack{x<N\\ p_1\dots p_r>N^{1-\beta}}} 1 \ll \frac{N\big(\log\frac{1}{\beta}\big)^{r-1}}{\log N}\sum_{k\ge 2}\Bigg(k^{r-1}\sum_{\substack{N^{\beta^{k/2}}\le y<N^{\beta}\\ P(y)\le N^{\beta^k}}}\frac{1}{y}\Bigg)+\beta N\big(\log\tfrac{1}{\beta}\big)^{r-1}.$$

Let $\Psi(x,y)$, as usual, denote the number of positive integers $\le x$ having no prime divisors $>y$. Denote by j_0 the integer with $2^{j_0}\le N^{\beta^{k/2}}<2^{j_0+1}$. Then splitting the range of y into dyadic intervals and using the well-known bound $\Psi(u,v)\ll u\exp\big(-\frac{\log u}{2\log v}\big)$ uniformly over $u\ge v\ge 2$ (see Tenenbaum [14, p. 359]), we get

$$\begin{aligned}\sum_{\substack{N^{\beta^{k/2}}\le y<N^{\beta}\\ P(y)\le N^{\beta^k}}}\frac{1}{y} &\ll \sum_{j_0\le j\ll\beta\log N}\frac{1}{2^j}\Psi(2^j,N^{\beta^k}) \ll \sum_{j_0\le j\ll\beta\log N}\exp\Big(-\frac{\log 2^j}{2\log N^{\beta^k}}\Big)\\ &\ll \sum_{j_0\le j\ll\beta\log N}\exp\Big(-\frac{\log 2^{j_0}}{2\log N^{\beta^k}}\Big)\\ &\ll \beta\log N\exp(-0.1(1/\beta)^{k/2}) \ll \beta\log N\exp(-10^{(k-1)/2}).\end{aligned}$$

It follows that

$$\sum_{k\ge 2}\Bigg(k^{r-1}\sum_{\substack{N^{\beta^{k/2}}\le y<N^{\beta}\\ P(y)\le N^{\beta^k}}}\frac{1}{y}\Bigg)\ll \beta\log N\sum_{k\ge 2}k^{r-1}\exp(-10^{(k-1)/2})\ll\beta\log N$$

and therefore

$$\sum_{\substack{x<N\\ p_1\dots p_r>N^{1-\beta}}} 1 \ll \beta N\big(\log\tfrac{1}{\beta}\big)^{r-1}.$$

Thus, we have

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

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

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

$$\sum_{\substack{x<N\\ p_1\dots p_{r-1}>N^{1-\beta_1}}} 1 \ll \beta_1 N\big(\log\tfrac{1}{\beta_1}\big)^{r-2}.$$

Hence,

$$N-|\mathcal{G}|\le c_1\beta N\big(\log\tfrac{1}{\beta}\big)^{r-1}+c_2\beta_1 N\big(\log\tfrac{1}{\beta_1}\big)^{r-2}+\Psi(N,N^{\alpha})+\sum_{\substack{x<N\\ p_r<N^{\beta}\\ p_1\dots p_{r-1}\le N^{1-\beta_1}}}1.$$

Observing that

$$\sum_{\substack{x<N\\ p_r<N^\beta\\ p_1\dots p_{r-1}\le N^{1-\beta_1}}} 1 \le \sum_{p_1\dots p_{r-1}\le N^{1-\beta_1}} \Psi\Big(\frac{N}{p_1\dots p_{r-1}}, N^\beta\Big),$$

we get

$$\begin{aligned} N-|\mathcal{G}| &\le c_1\beta N(\log \tfrac{1}{\beta})^{r-1} + c_2\beta_1 N(\log \tfrac{1}{\beta_1})^{r-2} \\ &\quad + \Psi(N,N^\alpha) + \sum_{p_1\dots p_{r-1}\le N^{1-\beta_1}} \Psi\Big(\frac{N}{p_1\dots p_{r-1}}, N^\beta\Big). \end{aligned}$$

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

$$\Psi(x,y)\le xu^{-u(1+o(1))} \qquad \text{as } u=\frac{\log x}{\log y}\to\infty.$$

We now take

$$\alpha=\frac{1}{\log\log m},\qquad \beta=\frac{\log\log m}{(\log m)^{1/2}},\qquad \beta_1=\beta\log\log m=\frac{(\log\log m)^2}{(\log m)^{1/2}}$$

and obtain

$$\begin{aligned} N-|\mathcal{G}| &< \alpha^{1/(2\alpha)}N \\ &\quad + \sum_{p_1\dots p_{r-1}<N^{1-\beta_1}} \frac{N}{p_1\dots p_{r-1}}\Big(\frac{\beta}{\beta_1}\Big)^{\beta_1/(2\beta)} + c\beta N(\log\log m)^{r-1} \\ &< \Big(\alpha^{1/(2\alpha)} + (\log\log N)^{r-1}\Big(\frac{\beta}{\beta_1}\Big)^{\beta_1/(2\beta)} + c_3\beta(\log\log m)^{r-1}\Big)N \\ &< c_4\beta(\log\log m)^{r-1}N. \end{aligned}$$

Therefore

$$\Big|\sum_{x<N} e_m(ax^*)\Big| \le c_4\beta(\log\log m)^{r-1}N + \Big|\sum_{x\in\mathcal{G}} e_m(ax^*)\Big|. \tag{7}$$

The sum $\sum_{x\in\mathcal{G}} e_m(ax^*)$ may be bounded by

$$\sum_{p_1}\dots\sum_{p_r}\Big|\sum_{y} e_m(ap_1^*\dots p_r^* y^*)\Big|, \tag{8}$$

where the summations are over primes $p_1,\dots,p_r$ and integers y such that

$$p_1\ge\dots\ge p_r,\quad p_1\ge N^\alpha,\quad p_r\ge N^\beta,\quad p_1\dots p_r\le N^{1-\beta}$$

and

$$y<\frac{N}{p_1\dots p_r},\qquad P(y)\le p_r.$$

Note that if t and T are such that

$$\left(1-\frac{c_0}{\log m}\right)p_r < t < p_r, \quad \left(1-\frac{c_0}{\log m}\right)\frac{N}{p_1\dots p_r} < T < \left(1+\frac{c_0}{\log m}\right)\frac{N}{p_1\dots p_r},$$

where $c_0 > 0$ is any constant, then in (8) we can replace the condition on y with

$$P(y) \le t, \qquad y < T,$$

up to adding to (8) 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 $p_1, \dots, p_r$ into subintervals of the form $[L, L + L(\log m)^{-1}]$ and choosing suitable t and T we find that for some numbers $M_1, \dots, M_r$ with

$$M_1 > \dots > M_r, \quad M_1 \ge N^{\alpha}/2, \quad M_r \ge N^{\beta}/2, \quad M_1 \dots M_r < N^{1-\beta},$$

one has

$$\text{(9)} \quad \Big|\sum_{x\in\mathcal{G}} e_m(ax^*)\Big| < \frac{N(\log\log m)^{O(1)}}{\log m} + (\log m)^{3r}\sum_{p_1\in I_1}\dots\sum_{p_r\in I_r}\Big|\sum_{\substack{y\le M\\ P(y)\le M_r}} e_m(ap_1^*\dots p_r^* y^*)\Big|,$$

where

$$I_j = \left[M_j, M_j + \frac{M_j}{\log m}\right], \qquad M = \frac{N}{M_1\dots M_r} \ge N^{\beta}.$$

Denote

$$W = \sum_{p_1\in I_1}\dots\sum_{p_r\in I_r}\Big|\sum_{\substack{y\le M\\ P(y)\le M_r}} e_m(ap_1^*\dots p_r^* y^*)\Big|.$$

Applying the Cauchy–Schwarz inequality, we get

$$W^2 \le M_1\dots M_r \sum_{y\le M}\sum_{z\le M}\Big|\sum_{p_1\in I_1}\dots\sum_{p_r\in I_r} e_m\big(ap_1^*\dots p_r^*(y^*-z^*)\big)\Big|.$$

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 $\gcd(y-z,m) \le e^{10\log m/\log\log m}$, we get the bound

$$\text{(10)} \qquad W^2 \le \frac{N^2}{M} + \frac{N^2}{e^{\log m/\log\log m}} + NM|S| \le 2N^{2-\beta} + \frac{N^2}{M_1\dots M_r}|S|,$$

where

$$S = \sum_{p_1 \in I_1} \dots \sum_{p_r \in I_r} e_{m_1}(bp_1^* \dots p_r^*).$$

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: $M_r > N^{\alpha^3}$. Then $M_j > N^{\alpha^3}$ for all $j = 1, \dots, r$. 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 $k_1, \dots, k_r$ be positive integers defined from

$$M_i^{2k_i-1} < m_1 \leq M_i^{2k_i+1}.$$

Since $M_i > N^{\alpha^3} > m^{c\alpha^3}$, 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

$$|S|^{2^r k_1 \dots k_r} \leq \Big(\prod_{i=1}^r M_i^{2^r k_1 \dots k_r - 2k_i}\Big) \sum_{\substack{p_{11}, \dots, p_{1k_1} \in I_1 \cap \mathcal{P} \\ q_{11}, \dots, q_{1k_1} \in I_1 \cap \mathcal{P}}} \dots \sum_{\substack{p_{r1}, \dots, p_{rk_r} \in I_r \cap \mathcal{P} \\ q_{r1}, \dots, q_{rk_r} \in I_r \cap \mathcal{P}}} e^{2\pi i b\{\dots\}/m_1},$$

where $\{\dots\}$ indicates the expression

$$(p_{11}^* + \dots + p_{1k_1}^* - q_{11}^* - \dots - q_{1k_1}^*) \cdots (p_{r1}^* + \dots + p_{rk_r}^* - q_{r1}^* - \dots - q_{rk_r}^*).$$

Next, we can fix the variables q_{ij} and then infer that for some integers $\mu_1, \dots, \mu_r$,

$$\frac{|S|}{M_1 \dots M_r} \leq \Big(\frac{|S_1|}{M_1^{k_1} \dots M_r^{k_r}}\Big)^{1/(2^r k_1 \dots k_r)}, \tag{11}$$

where

$$S_1 = \sum_{p_{11}, \dots, p_{1k_1} \in I_1 \cap \mathcal{P}} \dots \sum_{p_{r1}, \dots, p_{rk_r} \in I_r \cap \mathcal{P}} e^{2\pi i b(p_{11}^* + \dots + p_{1k_1}^* - \mu_1) \cdots (p_{r1}^* + \dots + p_{rk_r}^* - \mu_r)/m_1}.$$

Let $A_1, \dots, A_r$ be subsets of $\mathbb{Z}_{m_1}$ defined by

$$A_1 = \{p_{11}^* + \dots + p_{1k_1}^* - \mu_1 : (p_{11}, \dots, p_{1k_1}) \in (I_1 \cap \mathcal{P})^{k_1}\},$$
$$\dots$$
$$A_r = \{p_{r1}^* + \dots + p_{rk_r}^* - \mu_r : (p_{r1}, \dots, p_{rk_r}) \in (I_r \cap \mathcal{P})^{k_r}\},$$

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

$$S_1 = \sum_{\lambda_1 \in A_1} \dots \sum_{\lambda_r \in A_r} I_1(\lambda_1) \dots I_r(\lambda_r) e^{2\pi i b \lambda_1 \dots \lambda_r / m_1},$$

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

$$p_{j1}^* + \dots + p_{jk_j}^* - \mu_j \equiv \lambda \pmod{m_1}, \qquad (p_{j1}, \dots, p_{jk_j}) \in (I_j \cap \mathcal{P})^{k_j}.$$

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

$$|S_1|^2 \le J_{2k_1}(M_1) \dots J_{2k_r}(M_r) \times \sum_{\lambda_1 \in A_1} \dots \sum_{\lambda_{r-1} \in A_{r-1}} \Big| \sum_{\lambda_r \in A_r} I_r(\lambda_r) e^{2\pi i b \lambda_1 \dots \lambda_{r-1} \lambda_r / m_1} \Big|^2,$$

where

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

Changing the order of summation, we get

$$|S_1|^2 \le J_{2k_1}(M_1) \dots J_{2k_{r-1}}(M_{r-1}) \times \sum_{\lambda_r, \lambda_r' \in A_r} I_r(\lambda_r) I_r(\lambda_r') \Big| \sum_{\lambda_1 \in A_1} \dots \sum_{\lambda_{r-1} \in A_{r-1}} e^{2\pi i b \lambda_1 \dots \lambda_{r-1} (\lambda_r - \lambda_r') / m_1} \Big|.$$

We apply the Cauchy–Schwarz inequality to the sum over λ_r, λ_r' to get

$$|S_1|^4 \le (J_{2k_1}(M_1) \dots J_{2k_r}(M_r))^2 \times \sum_{\lambda_r, \lambda_r' \in A_r} \Big| \sum_{\lambda_1 \in A_1} \dots \sum_{\lambda_{r-1} \in A_{r-1}} e^{2\pi i b \lambda_1 \dots \lambda_{r-1} (\lambda_r - \lambda_r') / m_1} \Big|^2.$$

We can fix $\lambda_r' \in A_r$ such that

$$|S_1|^4 \le (J_{2k_1}(M_1) \dots J_{2k_r}(M_r))^2 |A_r| \times \sum_{\lambda_r \in A_r'} \Big| \sum_{\lambda_1 \in A_1} \dots \sum_{\lambda_{r-1} \in A_{r-1}} e^{2\pi i b \lambda_1 \dots \lambda_{r-1} \lambda_r / m_1} \Big|^2,$$

where $A_r' = A_r - \{\lambda_r'\}$. Using the trivial bound

$$\Big| \sum_{\lambda_1 \in A_1} \dots \sum_{\lambda_{r-1} \in A_{r-1}} e^{2\pi i b \lambda_1 \dots \lambda_{r-1} \lambda_r / m_1} \Big|^2 \le |A_1| \dots |A_{r-1}| \Big| \sum_{\lambda_1 \in A_1} \dots \sum_{\lambda_{r-1} \in A_{r-1}} e^{2\pi i b \lambda_1 \dots \lambda_{r-1} \lambda_r / m_1} \Big|,$$

we get

$$|S_1|^4 \le (J_{2k_1}(M_1)\dots J_{2k_r}(M_r))^2|A_1|\dots|A_r| \\ \times \sum_{\lambda_r\in A_r'}\Big|\sum_{\lambda_1\in A_1}\dots\sum_{\lambda_{r-1}\in A_{r-1}} e^{2\pi ib\lambda_1\dots\lambda_{r-1}\lambda_r/m_1}\Big|.$$

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

$$J_{2k_i}(M_i) < (5k_i)^{k_i}M_i^{k_i}.$$

Thus,

$$(12)\qquad |S_1|^4 \le \Big(\prod_{i=1}^{r}(5k_i)^{2k_i}M_i^{3k_i}\Big) \\ \times \sum_{\lambda_r\in A_r'}\Big|\sum_{\lambda_1\in A_1}\dots\sum_{\lambda_{r-1}\in A_{r-1}} e^{2\pi ib\lambda_1\dots\lambda_{r-1}\lambda_r)/m_1}\Big|,$$

Let $\gamma = 1/10$ and define $\varepsilon = \varepsilon(\gamma) > 0$ to be the absolute constant from Lemma 1. We shall verify that the sets $A_1,\dots,A_r$ satisfy the condition of Lemma 1 with $q = m_1$ (note that if A_r satisfies the condition of Lemma 1, so does A_r'). From the choice of k_i, the conditions on M_i and distribution of primes (in short intervals if needed) it follows that the interval I_i contains at least $M_i(2\log m)^{-2}$ primes coprime to m. From the definition of A_i and the connection between the cardinality of a set and the corresponding additive energies, we have

$$(13)\qquad |A_i| \ge \frac{(M_i(2\log m)^{-2})^{2k_i}}{J_{2k_i}(M_i)} \ge \frac{M_i^{k_i}}{(5k_i)^{k_i}(2\log m)^{4k_i}}.$$

From the choice of k_i it then follows that

$$|A_i| \ge \frac{m_1^{1/3}}{(5k_i)^{k_i}(2\log m)^{4k_i}} = m_1^{1/3+o(1)}.$$

Thus, the first condition $|A_i| > m_1^{1/10}$ is satisfied.

Next, let $q_1 \,|\, m_1$, $q_1 > m_1^{\varepsilon}$ and let $\xi \in \mathbb{Z}_{q_1}$. Let T_i be the number of solutions of the congruence

$$x \equiv \xi \pmod{q_1}, \qquad x \in A_i.$$

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

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

Consider two possibilities here. If $M_i \ge q_1^{1/8}$ say, then we fix $p_2,\dots,p_{k_i}$ and we have at most $1 + M_iq_1^{-1}$ possibilities for p_1. Thus, using (13), we get

$$T_i \le \Big(1 + \frac{M_i}{q_1}\Big)M_i^{k_i-1} < \frac{M_i^{k_i}}{q_1^{1/9}} < q_1^{-1/10}|A_i|.$$

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,

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

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

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

From the choice of k_i and Theorem 2 we get

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

Therefore, using (13),

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

Thus, the condition of Lemma 1 is satisfied and hence

$$\sum_{\lambda_r \in A_r'} \Big| \sum_{\lambda_1 \in A_1} \cdots \sum_{\lambda_{r-1} \in A_{r-1}} e^{2\pi i b \lambda_1 \ldots \lambda_{r-1} \lambda_r / m_1} \Big| < m^{-\tau} |A_1| \ldots |A_r|$$

for some absolute constant $\tau > 0$ (see the discussion following Lemma 1). Inserting this into (12) and using the estimates $k_i \ll (\log\log m)^3$ and $|A_i| \le M_i^{k_i}$, we get

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

Thus, from (11) it follows that

$$\frac{|S|}{M_1 \ldots M_r} < m^{-c_1 (\log\log m)^{-3r}}$$

and from (10) we get

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

Inserting this into (9) and using (7), we conclude the proof.

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

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

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

From the definition of α and β we have

$$k_1 \le \frac{1}{c} \log\log m, \qquad k_2 \le \frac{1}{c\beta} \ll \frac{(\log m)^{1/2}}{\log\log m}.$$

Let
$$\delta = \frac{k_1 \log M_r}{3 \log M_1}.$$
Note that $\delta \le \frac{1}{c}(\log\log m)^{-1}$. We further consider three subcases:

Case 2.1: $M_1^{k_1-1+\delta} < m_1^{1/2} \le M_1^{k_1-\delta}$. Then we apply Corollary 3 to get (recall that $|I_j| \sim M_j/\log m$)
$$\frac{|S|}{M_1 \ldots M_r} < 0.1\left(\frac{M_1^{k_1-1}}{m_1^{1/2}} + \frac{m_1^{1/2}}{M_1^{k_1}}\right)^{1/(2k_1k_2)} < M_1^{-\delta/(2k_1k_2)} = M_r^{-1/(6k_2)}.$$
The upper bound for k_2 and the lower bound $M_r \ge N^\beta$ yield
$$\frac{|S|}{M_1 \ldots M_r} < e^{-0.01c^2\beta^2 \log m}.$$

Case 2.2: $M_1^{k_1-\delta} < m_1^{1/2} \le M_1^{k_1}$. We apply Corollary 4 in the form
$$\begin{aligned}\frac{|S|}{M_1 \ldots M_r} &< \left(\frac{(M_1M_r)^{k_1-1}}{m_1^{1/2}} + \frac{m_1^{1/2}}{(M_1M_r)^{k_1}}\right)^{1/(2k_1k_2)}\\ &< \left(\frac{M_r^{k_1-1}}{M_1^{1-\delta}} + \frac{1}{M_r^{k_1}}\right)^{1/(2k_1k_2)}.\end{aligned}$$

Case 2.3: $M_1^{k_1-1} < m_1^{1/2} \le M_1^{k_1-1+\delta}$. Then $k_1 \ge 2$ and we apply Corollary 4 with k_1 replaced by $k_1 - 1$ in the form
$$\begin{aligned}\frac{|S|}{M_1 \ldots M_r} &< \left(\frac{(M_1M_r)^{k_1-2}}{m_1^{1/2}} + \frac{m_1^{1/2}}{(M_1M_r)^{k_1-1}}\right)^{1/(2k_1k_2)}\\ &< \left(\frac{M_r^{k_1-2}}{M_1} + \frac{M_1^{\delta}}{M_r^{k_1-1}}\right)^{1/(2k_1k_2)}.\end{aligned}$$

In all three subcases we get the bound
$$\frac{|S|}{M_1 \ldots M_r} < e^{-c'\beta^2 \log m}$$
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 (9) and using (7), we conclude that
$$\begin{aligned}\Big|\sum_{x<N} e_m(ax^*)\Big| &\ll \beta(\log\log m)^{r-1}N + Ne^{-c'''\beta^2 \log m}(\log m)^{3r}\\ &\ll \frac{(\log\log m)^r}{(\log m)^{1/2}}N.\end{aligned}$$

References

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

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

[3] J. Bourgain and M. Z. Garaev, *Sumsets of reciprocals in prime fields and multilinear Kloosterman sums*, Izv. Math., to appear.

[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*, in: Analytic Number Theory (Kyoto, 1996), London Math. Soc. Lecture Note Ser. 247, Cambridge Univ. Press, Cambridge, 1997, 85–93.

[6] J. Friedlander and H. Iwaniec, *Opera de Cribro*, Colloq. Publ. 57, Amer. Math. Soc., 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 (2010), 347–359 (prepared by E. A. Karatsuba, M. A. Korolev and I. S. Rezvyakova from notes and drafts of A. A. Karatsuba).

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

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

[11] M. A. Korolev, *Incomplete Kloosterman sums and their applications*, Izv. Math. 64 (2000), 1129–1152.

[12] M. A. Korolev, *Short Kloosterman sums with weights*, Math. Notes 88 (2010), 374–385.

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

[14] G. Tenenbaum, *Introduction to Analytic and Probabilistic Number Theory*, Cambridge Stud. Adv. Math. 46, Cambridge Univ. Press, Cambridge, 1995.

J. Bourgain
Institute for Advanced Study
Princeton, NJ 08540, U.S.A.
E-mail: bourgain@ias.edu

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

Received on 8.9.2013 (7583)