Sumsets of reciprocals in prime fields
and multilinear Kloosterman sums

J. Bourgain and M. Z. Garaev

Abstract. We obtain new results on the additive properties of the set $I^{-1} = \{x^{-1}: x \in I\}$, where $I$ is an arbitrary interval in the field of residue classes modulo a large prime $p$. Combining our results with estimates of multilinear exponential sums, we obtain new results on incomplete multilinear Kloosterman sums.

Keywords: congruences modulo a prime, sumsets, multilinear exponential sums, multilinear Kloosterman sums, distribution of primes.

§ 1. Introduction

Throughout the paper $p$ is a large prime and $\mathbb{F}_p$ is the field of residue classes modulo $p$. We often identify residue classes with their concrete representatives. The cardinality of a finite set $X$ is denoted by $|X|$. Unless otherwise stated, $\varepsilon$ stands for a small positive constant. Given an integer $x$ coprime to $p$ (or an element $x$ of $\mathbb{F}_p^* = \mathbb{F}_p \setminus \{0\}$), we write $x^*$ or $x^{-1}$ for the multiplicative inverse of $x$ modulo $p$.

Let $I$ be a non-zero interval in $\mathbb{F}_p$. The additive properties of the reciprocal set $I^{-1} = \{x^{-1}: x \in I\}$ were studied in [1] along with applications to Kloosterman sums. It was proved that for every $\delta > 0$ there is a $k \in \mathbb{Z}_+$ such that the cardinality of the sumset $k(I^{-1}) = \{x_1^{-1} + \cdots + x_k^{-1}: x_i \in I\}$ satisfies the estimate $|k(I^{-1})| > p^{-\delta} \min\{|I|^2, p\}$.

In the most interesting case $|I| < p^{1/2}$ it follows that $|k(I^{-1})| > |I|^2 p^{-\delta}$. Recent results in [2] (see Lemma 10 below) yield that

$$|I^{-1} + I^{-1}| > \min\{|I|^2, \sqrt{p|I|}\}|I|^{o(1)}.$$  \hspace{1cm} (1)

In particular, if $|I| < p^{1/3}$, then $|I^{-1} + I^{-1}| > |I|^{2+o(1)}$.

We shall establish new additive properties of $I^{-1}$. Combining our results with recent bounds in [3] for multilinear exponential sums, we then obtain new bounds for multilinear Kloosterman sums.

AMS 2010 Mathematics Subject Classification. 11L05, 11L07, 11N05.

© 2014 Russian Academy of Sciences (DoM), London Mathematical Society, Turpion Ltd.
The structure of this paper is as follows. In §2 we state our results on the additive properties of $I^{-1}$ and the bounds for Kloosterman sums. In §3 we give some basic preliminaries which are used throughout the paper. In §§4–6 we give some background and prove lemmas. The proofs of our results on the additive properties of the reciprocals of intervals (Theorems 1–6) are given in §7. The proofs of Theorems 7–13 and Theorem 14 on a continuous analogue of Karatsuba’s estimate are given in §8. In §9 we prove Theorem 15 on $\pi(x) - \pi(x - y)$, Theorem 16 on linear Kloosterman sums and Theorem 17 on the Brun–Titchmarsh estimate.

In this paper we consider only the case of prime moduli. The case of composite moduli will be considered in a forthcoming paper.

§2. Statement of results

2.1. Sums of the reciprocals of elements in an interval. We recall that $I$ stands for an arbitrary non-zero interval in $\mathbb{F}_p$. We start with results on the additive properties of $I^{-1}$.

**Theorem 1.** For every positive integer constant $k$ we have an estimate

$$J_{2k} < \left( |I|^{2k \delta} + \frac{|I|^{2k}}{p} \right) |I|^{o(1)}, \quad (2)$$

where $J_{2k}$ is the number of solutions of the congruence $x_1^{-1} + \cdots + x_k^{-1} = x_{k+1}^{-1} + \cdots + x_{2k}^{-1}$, $x_1, \ldots, x_{2k} \in I$.

We recall that (2) is equivalent to saying that for every $\varepsilon > 0$ there is a $c = c(k; \varepsilon) > 0$ such that

$$J_{2k} < c \left( |I|^{2k \delta} + \frac{|I|^{2k}}{p} \right) |I|^\varepsilon.$$

**Corollary 1.** Suppose that $|I| < p^{\frac{1}{4}}$. Then for every positive integer constant $k$,

$$|k(I^{-1})| > |I|^{2k \delta + o(1)}.$$

We note that for $k = 3$ one has a stronger bound

$$|I^{-1} + I^{-1} + I^{-1}| > |I|^{1.55 + o(1)}$$

(see §10). The following result concerns a ternary additive congruence for $I^{-1}$.

**Theorem 2.** Suppose that $|I| < p^{\frac{1}{3}}$. Then for every element $\lambda \in \mathbb{F}_p$ with

$$\lambda \notin I^{-1} \cup \{0\}, \quad (3)$$

we have

$$J < |I|^{\frac{2}{3} + o(1)},$$

where $J$ is the number of solutions of the congruence $x^{-1} + y^{-1} + z^{-1} = \lambda$, $x, y, z \in I$. 

The constraint (3) appears because otherwise the congruence in Theorem 2 may have $|I|^{1+o(1)}$ solutions (for example, $z = \lambda^{-1}$ and $x + y = 0$).

It follows easily from Theorem 2 that for $|I| < p^{\frac{3}{46}}$ one has

$$|I^{-1} + I^{-1} + I^{-1}| > |I|^\frac{7}{1} + o(1).$$

The following assertion shows that an optimal estimate holds for small $I$.

**Theorem 3.** Suppose that $|I| < p^{\frac{1}{13}}$. Then

$$J_6 < |I|^{3+o(1)}$$

where $J_6$ is the number of solutions of the congruence $x_1^{-1} + x_2^{-1} + x_3^{-1} = x_4^{-1} + x_5^{-1} + x_6^{-1}$, $x_1, \ldots, x_6 \in I$. In particular, for $|I| < p^{\frac{1}{13}}$ we have

$$|I^{-1} + I^{-1} + I^{-1}| > |I|^{3+o(1)}.$$

**Theorem 4.** There is an absolute constant $c > 0$ such that for every positive integer constant $k$ and any interval $I \subset \mathbb{F}_p$ with $|I| < p^{\frac{c}{2k}}$ we have

$$J_{2k} < |I|^{k+o(1)}$$

where $J_{2k}$ is the number of solutions of the congruence $x_1^{-1} + \cdots + x_k^{-1} = x_{k+1}^{-1} + \cdots + x_{2k}^{-1}$, $x_1, \ldots, x_{2k} \in I$. In particular, for such intervals $I$ we have

$$|k(I^{-1})| > |I|^{k+o(1)}.$$

**Remark 1.** It follows from the proof of Theorem 4 that one can take $c = 1/4$.

**Theorem 5.** Suppose that $I = [1, N]$. Then we have

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

where $J_{2k}$ is the number of solutions of the congruence $x_1^* + \cdots + x_k^* \equiv x_{k+1}^* + \cdots + x_{2k}^* \pmod{p}$, $x_1, \ldots, x_{2k} \in I$.

We also state a version of Theorem 5 in the case when the variables $x_j$ are restricted to prime numbers. The set of primes is denoted by $\mathcal{P}$.

**Theorem 6.** Suppose that $I = [1, N]$. Then we have

$$J_{2k} < (2k)^{k} \left( \frac{N^{2k-1}}{p} + 1 \right) N^k,$$

where $J_{2k}$ is the number of solutions of the congruence $x_1^* + \cdots + x_k^* \equiv x_{k+1}^* + \cdots + x_{2k}^* \pmod{p}$, $x_1, \ldots, x_{2k} \in I \cap \mathcal{P}$. 
2.2. Incomplete multilinear Kloosterman sums. In what follows we use the abbreviation $e_p(z) = e^{2\pi i z/p}$. The incomplete Kloosterman sums

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

where $a$ and $b$ are integers with $(a, p) = 1$, are well known and have a variety of applications in number theory. As a consequence of Weil’s bounds, these sums are estimated by $O(p^{1/2} \log p)$. For $M = 0$ and very small $N$ (of order $p^{o(1)}$) these sums were estimated by Korolev [4].

The incomplete bilinear Kloosterman sums

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

where $\alpha_i(x_i) \in \mathbb{C}$, $|\alpha_i(x_i)| \leq 1$, are also well known. Note that if one of the parameters $N_1$, $N_2$ is much larger than $p^{1/2}$, then $S$ can easily be estimated. For example, if $N_1^{1-c} > p^{1/2}$ for some constant $c > 0$, then Weil’s bound yields that

$$
|S|^2 \leq N_1 \sum_{x_1=M_1+1}^{M_1+N_1} \left| \sum_{x_2=M_2+1}^{M_2+N_2} \alpha_2(x_2) e_p(ax_1^*x_2^*) \right|^2
\leq N_1 \sum_{y=M_2+1}^{M_2+N_2} \sum_{z=M_2+1}^{M_2+N_2} e_p(ax_1^*(y^* - z^*)) \leq N_1^2 N_2 + N_1 N_2^2 \sqrt{p} \log p,
$$

whence

$$
|S| < (N_2^{-\frac{1}{2}} + N_1^{-\frac{c}{2}})(N_1 N_2)^{1+o(1)}.
$$

Thus the most non-trivial case occurs when $N_i < p^{1/2}$. For $M_1 = M_2 = 0$ the sum $S$ (in a more general form) was estimated by Karatsuba [5], [6] for very short ranges of $N_1$ and $N_2$, and by the first author [1] for arbitrary $M_1$, $M_2$ provided that $N_1 N_2 > p^{1/2+\varepsilon}$. Baker [7] gave an explicit version of Bourgain’s result.

The incomplete $n$-linear Kloosterman sums

$$
\sum_{x_1=M_1+1}^{M_1+N_1} \cdots \sum_{x_n=M_n+1}^{M_n+N_n} e_p(a_1 x_1 + \cdots + a_n x_n + a_{n+1}(x_1 \cdots x_n)^*),
$$

where $a_i \in \mathbb{Z}$, $(a_{n+1}, p) = 1$, were studied for arbitrary $n$ by Luo [8] and Shparlinski [9]. The main tools in their study were Burgess’ bounds [10] for incomplete Gauss sums.

We shall combine our Theorems 1–5 with an estimate for multilinear exponential sums in [3] (see Lemma 1 below) to get new bounds for Kloosterman sums.

In what follows $\alpha_1(x_1), \ldots, \alpha_n(x_n)$ stand for arbitrary complex numbers with $|\alpha_i(x_i)| \leq 1$. 
Theorem 7. For all intervals \( I_1, I_2 \) with \( |I_1| > p^{\frac{1}{18}} \) and \( |I_2| > p^{\frac{5}{18}+\varepsilon} \) we have

\[
\max_{(a,p)=1} \left| \sum_{x_1 \in I_1} \sum_{x_2 \in I_2} \alpha_1(x_1)\alpha_2(x_2)e_p(ax_1^*x_2^*) \right| < p^{-\delta}|I_1||I_2|
\]

for some \( \delta = \delta(\varepsilon) > 0 \).

Note that if \( |I_1| \) and \( |I_2| \) are of orders \( p^{\frac{1}{18}} \) and \( p^{\frac{5}{18}+\varepsilon} \) respectively, then \( |I_1||I_2| \) is of order \( p^{\frac{5}{18}+\frac{13}{36}+\varepsilon} \).

Remark 2. Theorem 7 remains valid for the more general sum

\[
\sum_{x_1 \in I_1} \sum_{x_2 \in I_2} \alpha_1(x_1)\alpha_2(x_2)e_p(ax_1^*x_2^* + bx_1x_2).
\]

This can be shown by combining our Theorem 3 with Lemma A.8 in [1].

When \( M_1 = M_2 = 0 \), we prove the following result that extends the range of applicability of Karatsuba’s estimate [6].

Theorem 8. Suppose that \( I_1 = [1, N_1], \ I_2 = [1, N_2] \). Then the following estimate holds uniformly with respect to all positive integers \( k_1 \) and \( k_2 \):

\[
\max_{(a,p)=1} \left| \sum_{x_1 \in I_1} \sum_{x_2 \in I_2} \alpha_1(x_1)\alpha_2(x_2)e_p(ax_1^*x_2^*) \right| < (2k_1)^{\frac{45k_1^2}{p^{\frac{1}{36}}}} (2k_2)^{\frac{45k_2^2}{p^{\frac{1}{36}}}} (\log p)^{2(k_1^2+k_2^2)} \times \left( \frac{N_1^{k_1-1}}{p^{\frac{1}{4}}} + \frac{p^{\frac{1}{2}}}{N_1^{k_1}} \right)^{\frac{1}{0.1}} \left( \frac{N_2^{k_2-1}}{p^{\frac{1}{4}}} + \frac{p^{\frac{1}{2}}}{N_2^{k_2}} \right)^{\frac{1}{0.1}} N_1N_2.
\]

Given \( N_1, N_2 \), we choose \( k_1, k_2 \) such that

\[
N_1^{2(k_1-1)} < p \leq N_1^{2k_1}, \quad N_2^{2(k_2-1)} < p \leq N_2^{2k_2}.
\]

Then the bound will be non-trivial unless each of the numbers \( N_1 \) and \( N_2 \) lies within the \( p^\varepsilon \)-ratio of an element of \( \{p^{\frac{1}{18}}, l \in \mathbb{Z}_+ \} \). Thus we get the following corollary.

Corollary 2. Suppose that \( I_1 = [1, N_1] \) and \( I_2 = [1, N_2] \), where for \( i = 1 \) or \( i = 2 \) we have

\[
N_i \notin \bigcup_{j \geq 1} [p^{\frac{1}{18}-\varepsilon}, p^{\frac{1}{18}+\varepsilon}].
\]

Then there is a \( \delta = \delta(\varepsilon) > 0 \) such that

\[
\max_{(a,p)=1} \left| \sum_{x_1 \in I_1} \sum_{x_2 \in I_2} \alpha_1(x_1)\alpha_2(x_2)e_p(ax_1^*x_2^*) \right| < p^{-\delta}N_1N_2.
\]

Theorem 9. Let \( I_1, I_2 \subset \mathbb{F}_p \) be arbitrary intervals of sizes \( N_1, N_2 \) respectively. Then

\[
\max_{(a,p)=1} \left| \sum_{x_1 \in I_1} \sum_{x_2 \in I_2} \alpha_1(x_1)\alpha_2(x_2)e_p(ax_1^*x_2^*) \right| \lesssim p^{\frac{1}{7}} N_1^{\frac{2}{7}} N_2^{\frac{2}{7}} (\frac{N_1^3}{p} + 1)^{\frac{1}{10}} (\frac{N_2^3}{p} + 1)^{\frac{1}{10}}.
\]
Analogs of Theorem 9 for intervals starting at the origin can be found in [7], [11], [12].

**Theorem 10.** Let \( k_1, k_2 \) be positive integer constants, and \( I_1, I_2 \subset \mathbb{F}_p \) arbitrary intervals of sizes \( N_1, N_2 \) respectively with
\[
N_1 < p^{\frac{k_1+1}{2k_1}}, \quad N_2 < p^{\frac{k_2+1}{2k_2}}.
\]
Then we have
\[
\max_{(a, p) = 1} \left| \sum_{x_1 \in I_1} \sum_{x_2 \in I_2} \alpha_1(x_1) \alpha_2(x_2) e_p(ax_1^*x_2^*) \right| < \left( p^{\frac{1}{2k_1} N_1 - \frac{1}{k_2(k_1+1)}} N_2^{-\frac{1}{k_2(k_2+1)}} \right) (N_1N_2)^{1+o(1)}.
\]

We now consider multilinear Kloosterman sums.

**Theorem 11.** Suppose that \( n \geq 7 \) and \( N^n > p^{\frac{3}{2}+\varepsilon} \). Then for all intervals \( I_1, \ldots, I_n \) of length \( N \) we have
\[
\max_{(a, p) = 1} \left| \sum_{x_1 \in I_1} \cdots \sum_{x_n \in I_n} \alpha_1(x_1) \cdots \alpha_n(x_n) e_p(ax_1^* \cdots x_n^*) \right| < p^{-\delta} N^n
\]
for some \( \delta = \delta(\varepsilon, n) > 0 \).

**Theorem 12.** There is an absolute constant \( C > 0 \) such that for every positive integer \( n \) and all intervals \( I_1, \ldots, I_n \) of length \( N > p^{\frac{C}{n^2}} \) we have
\[
\max_{(a, p) = 1} \left| \sum_{x_1 \in I_1} \cdots \sum_{x_n \in I_n} \alpha_1(x_1) \cdots \alpha_n(x_n) e_p(ax_1^* \cdots x_n^*) \right| < p^{-\delta} N^n
\]
for some \( \delta = \delta(n) > 0 \).

**Remark 3.** One can show that Theorem 12 holds with \( C = 4 \). This can be done using the geometry of numbers in the style of [13] to get a suitable version of our Theorem 4.

**Theorem 13.** Let \( I_1, \ldots, I_n \) be intervals in \([1, p-1]\) such that
\[
|I_1| \cdots |I_n| > p^{\frac{3}{2}+\varepsilon}.
\]
Then for all integers \( a, a_1, \ldots, a_n \) with \((a, p) = 1\) and some \( \delta = \delta(\varepsilon, n) > 0 \) we have
\[
\left| \sum_{x_1 \in I_1} \cdots \sum_{x_n \in I_n} e_p(ax_1^* \cdots x_n^* + a_1 x_1 + \cdots + a_n x_n) \right| < p^{-\delta} |I_1| \cdots |I_n|.
\]
We have the following continuous analogue of Karatsuba’s estimate.

**Theorem 14.** Suppose that \( \xi \in \mathbb{R}, \ |\xi| > N_1 N_2 \) and \( k_1, k_2 \in \mathbb{Z}_+ \). Then

\[
\left| \sum_{n_1=N_1+1}^{2N_1} \sum_{n_2=N_2+1}^{2N_2} \alpha_1(n_1) \alpha_2(n_2) e^{i \frac{1}{n_1} \frac{1}{n_2} \xi} \right| < c(k_1, k_2, \varepsilon) \gamma(N_1 N_2)^{1+\varepsilon},
\]

where

\[
\gamma = \left\{ \left( \frac{|\xi|}{N_1 N_2} N_1^{-2k_1} + \frac{N_1 N_2}{|\xi|} N_2^{2(k_1-1)} \right) \left( \frac{|\xi|}{N_1 N_2} N_2^{-2k_2} + \frac{N_1 N_2}{|\xi|} N_2^{2(k_2-1)} \right) \right\}^{\frac{1}{4k_1 k_2}}.
\]

Given any \( |\xi| > N_1 N_2 \) we can choose \( k_1, k_2 \) such that

\[
N_i^{2(k_i-1)} \leq \frac{|\xi|}{N_1 N_2} < N_i^{2k_i}.
\]

Then each of the factors in the expression for \( \gamma \) in Theorem 14 is \( O(1) \).

Exponential sums of the form (4) appear, for example, in the proof of Theorem 13.8 in [14]:

\[
\pi(x) - \pi(x-y) \leq (2-\delta) \frac{y}{\log y}, \quad x^\theta < y < x,
\]

where, as usual, \( \pi(z) \) is the number of primes not exceeding \( z \) and \( \delta = \delta(\theta) > 0 \).

Here \( \theta > 0 \) may be small and \( x > x_0(\theta) \) sufficiently large. The proof of (5) in [14] is based on estimates of exponential sums of the form \( \sum_{n \sim N} e(\xi/n) \) using either Weyl’s method or Vinogradov’s method, when \( \theta \) is small. Theorem 14 enables us to get a better estimate.

**Theorem 15.** The estimate (5) holds for

\[
\delta < \frac{2(1-\theta)}{12(\theta^{-1} + 1)(\theta^{-1} + 0.5) + 1 - \theta} \sim \theta^2.
\]

We shall apply bounds for trilinear exponential sums in [3] (see Lemma 1 below) to linear Kloosterman sums and to a problem related to the Brun–Titchmarsh theorem.

**Theorem 16.** We have

\[
\max_{(a,p)=1} \left| \sum_{n \leq N} e_p(an^*) \right| \ll \frac{(\log \log p)^3 \log p}{(\log N)^{\frac{3}{2}}} N,
\]

where the constant in the sign \( \ll \) is absolute.

It follows from Theorem 16 that for \( N = p^\varepsilon \) with \( \varepsilon \) fixed, the saving is \( O((\log \log p)^3/(\log p)^{\frac{3}{2}}) \). The estimate in Theorem 16 is non-trivial if \( N > \exp((\log p)^{\frac{3}{2}}(\log \log p)^3) \). This improves some results of Korolev [4] in the case of prime moduli (see also [15] for various versions of the problem).

It is claimed in [16] that if \( \varepsilon > 0 \) is fixed and \( p^\varepsilon < N < p^4 \), then

\[
\left| \sum_{n=1}^{N} e_p(an^*) \right| < \frac{N}{(\log N)^{1-\varepsilon}},
\]
but the proof given there raises doubts. Our approach here relies heavily on the 
bounds for trilinear exponential sums in [3] (see also [17], Theorem 4.2).

For \((a, q) = 1\) we write \(\pi(x; q, a)\) for the number of primes \(p \leq x\) such that 
\(p \equiv a \pmod{q}\). We improve the result of Friedlander and Iwaniec [18] on \(\pi(x; q, a)\)
in the following form.

**Theorem 17.** Suppose that \(x^\theta \leq q \leq 2x^\theta\), where \(\theta < 1\) is close to 1. Then for 
some absolute constant \(c_1 > 0\) and all sufficiently large \(x > x_0(\theta)\) we have

\[
\pi(x; q, a) < \frac{cx}{\varphi(q) \log(x/q)},
\]

where \(c = 2 - c_1(1 - \theta)^2\).

The constants in Theorem 17 are effective and can be made explicit. We note 
that there are better bounds for small values of \(\theta\). In the region \(q < x^{\frac{1}{5}}\), recent 
work of Maynard [19] gives the bound

\[
\pi(x; q, a) < \frac{2x}{\varphi(q) \log x}.
\]

We also mention a result of Motohashi (see, for example, [20], (5.13)) which asserts 
that, for every fixed \(\varepsilon > 0\), if \(q < x^{\frac{9}{20} - \varepsilon}\), one has

\[
\pi(x; q, a) < \frac{(2 + o(1))x}{\varphi(q) \log(x/q^{\frac{3}{8}})}.
\]

For more details we refer the reader to [19], [20] and the references there.

§ 3. Preliminaries

Throughout the paper we will use the well-known connection between the number 
of solutions of a symmetric equation and the cardinality of the corresponding set. 
Let \(T\) be the number of solutions of the equation

\[x_1 + \cdots + x_n = y_1 + \cdots + y_n,\]

where for every \(i\) the variables \(x_i, y_i\) run through a set \(A_i\) independently of each 
other. Then for every subset \(\Omega \subset A_1 \times \cdots \times A_n\) one has

\[|\{x_1 + \cdots + x_n; (x_1, \ldots, x_n) \in \Omega\}| \geq \frac{|\Omega|^2}{T}.\]

This estimate follows from the observation that if \(T_n(\Omega; \lambda)\) is the number of solutions of the equation \(x_1 + \cdots + x_n = \lambda\), \((x_1, \ldots, x_n) \in \Omega\), and if \(X = \{x_1 + \cdots + x_n; (x_1, \ldots, x_n) \in \Omega\}\), then

\[T \geq \sum_{\lambda \in X} T_n(\Omega; \lambda)^2 \geq \frac{1}{|X|} \left|\sum_{\lambda \in X} T_n(\Omega; \lambda)\right|^2 = \frac{|\Omega|^2}{|X|}.\]
In particular,
\[ |A_1 + \cdots + A_n| = \#\{a_1 + \cdots + a_n; a_i \in A_i\} \geq \frac{|A_1|^2 \cdots |A_n|^2}{T}. \]

We note that if \( A_1, \ldots, A_{2n} \subset \mathbb{F}_p \) and \( T_{2n}(\lambda) \) is the number of solutions of the congruence
\[ x_1 + \cdots + x_{2n} \equiv \lambda \pmod{p}, \quad (x_1, \ldots, x_{2n}) \in A_1 \times \cdots \times A_{2n}, \]
then
\[ T_{2n}(\lambda) \leq (J_1 \cdots J_{2n})^{\frac{1}{2n}}, \]
where \( J_i \) is the number of solutions of the congruence
\[ y_1 + \cdots + y_n \equiv y_{n+1} + \cdots + y_{2n} \pmod{p}, \quad y_1, \ldots, y_{2n} \in A_i. \]

Indeed, we have
\[ T_{2n}(\lambda) = \frac{1}{p} \sum_{a=0}^{p-1} \sum_{x_{2n} \in A_{2n}} \cdots \sum_{x_1 \in A_1} e_p(ax_1) \cdots e_p(ax_{2n}) e_p(-a\lambda). \]

Using Hölder’s inequality, we get
\[ T_{2n}(\lambda) \leq \prod_{j=1}^{2n} \left( \frac{1}{p} \sum_{a=0}^{p-1} \left| \sum_{x_j \in A_j} e_p(ax_j) \right|^{\frac{2n}{\alpha_j}} \right)^{\frac{\alpha_j}{2n}} = (J_1 \cdots J_{2n})^{\frac{1}{2n}}. \]

The following observation will be used in the proofs of some of our results. If \( X, Y \subset \mathbb{F}_p \), then the number of solutions of the congruence
\[ \frac{1}{y + x_1} + \cdots + \frac{1}{y + x_n} = \frac{1}{y + x_{n+1}} + \cdots + \frac{1}{y + x_{2n}}, \quad x_i \in X, \ y \in Y, \]
is at most \( O(|X|^n|Y| + |X|^{2n}) \), where the constant implied in \( O \) may depend only on \( n \). Indeed, the contribution of those \( (x_1, \ldots, x_{2n}) \in X^{2n} \) for which the sequence \( x_1, \ldots, x_{2n} \) contains at most \( n \) distinct elements is \( O(|X|^n|Y|) \). On the other hand, when this sequence contains more than \( n \) distinct elements, we can assume that \( x_1 \not\in \{x_2, \ldots, x_{2n}\} \). For every such \( (x_1, \ldots, x_{2n}) \in X^{2n} \) the polynomial
\[ P(Z) = \prod_{i \neq 1} (Z + x_i) + \cdots + \prod_{i \neq n} (Z + x_i) - \prod_{i \neq n+1} (Z + x_i) - \cdots - \prod_{i \neq 2n} (Z + x_i) \]
is non-zero \( (P(-x_1) \neq 0) \) and, since \( P(y) = 0 \), we get at most \( 2n - 1 \) possibilities for \( y \) (see also [7], Lemmas 2, 3, for more general assertions).

\section*{4. Auxiliary facts}

The following lemma was proved by the first author [3]. The proof is based on results from additive combinatorics, in particular, on sum-product estimates. This lemma will be used to prove our results on Kloosterman sums.
Lemma 1. Let $\gamma_1(x_1), \ldots, \gamma_n(x_n)$ be non-negative real numbers such that

$$\|\gamma_i\|_1 = \sum_{x=0}^{p-1} |\gamma_i(x)| \leq 1,$$

$$\|\gamma_i\|_2 = \left( \sum_{x=0}^{p-1} |\gamma_i(x)|^2 \right)^{\frac{1}{2}} < p^{-\delta}.$$

Suppose that $\prod_{i=1}^{n} \|\gamma_i\|_2 < p^{-\frac{1}{2}} - \frac{\delta}{4}$, where $0 < \delta < 1/4$. Then we have

$$\left| \sum_{x_1=0}^{p-1} \cdots \sum_{x_n=0}^{p-1} \gamma_1(x_1) \cdots \gamma_n(x_n)e_p(x_1 \cdots x_n) \right| < p^{-\delta'}$$

for some $\delta' > (\delta/n)^Cn$.

We shall use the following resultant bound from [13].

Lemma 2. Suppose that $N \geq 1$, $\sigma, \vartheta \in \mathbb{R}$, and let $m, n \geq 2$ be fixed integers. Assume that one of the following conditions holds: (i) $\sigma \geq 0$; (ii) $\vartheta \geq 0$; (iii) $\sigma + \vartheta \geq -1$. Let $P_1(Z)$ and $P_2(Z)$ be non-constant polynomials with integer coefficients,

$$P_1(Z) = \sum_{i=0}^{m-1} a_i Z^{n-1-i}, \quad P_2(Z) = \sum_{i=0}^{n-1} b_i Z^{n-1-i},$$

such that

$$|a_i| < AN^{i+\sigma}, \quad i = 0, \ldots, m-1,$$

$$|b_i| < AN^{i+\vartheta}, \quad i = 0, \ldots, n-1,$$

for some $A$. Then

$$\text{Res}(P_1, P_2) \ll N^{(m-1+\sigma)(n-1+\vartheta) - \sigma \vartheta},$$

where the constant implicit in $\ll$ depends only on $A$, $m$ and $n$.

We shall use 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 symmetric (with respect to 0) convex compact body $D \subset \mathbb{R}^n$. Given a lattice $\Gamma \subset \mathbb{R}^n$ and any $i = 1, \ldots, n$, we write $\lambda_i(D, \Gamma)$ for the $i$th successive minimum of $D$ with respect to $\Gamma$. Recall that $\lambda_i(D, \Gamma)$ is defined as the minimal number $\lambda$ such that the set $\lambda D$ contains $i$ linearly independent vectors of $\Gamma$. Clearly, $\lambda_1(D, \Gamma) \leq \cdots \leq \lambda_n(D, \Gamma)$. We shall use the following result from [21], Proposition 2.1 (see also [22], Exercise 3.5.6, for a simplified form which still suffices for our purposes).

Lemma 3. We have

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

Writing, as usual, $(2n+1)!!$ for the product of all odd positive integers not exceeding $2n+1$, we get the following corollary.

Corollary 3. We have

$$\prod_{i=1}^{n} \min\{\lambda_i(D, \Gamma), 1\} \leq \frac{(2n+1)!!}{|D \cap \Gamma|}.$$
§ 5. Equations in many variables

The following lemma is due to Karatsuba [6].

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

The following elementary assertion will be used to exclude some degenerate cases in the proof of Lemma 6. An argument similar to our proof was first used by Linnik [23], Lemma 4.

**Lemma 5.** Suppose that \( c \in \mathbb{C}, c_1, \ldots, c_r \in \mathbb{C}^*, \) and \( S \) is a finite subset of \( \mathbb{C} \). Let \( T_r \) be the number of solutions of the equation
\[
c_1 x_1 + \cdots + c_r x_r = c, \quad x_1, \ldots, x_r \in S,
\]
and \( J_{2s} \) the number of solutions of the equation
\[
x_1 + \cdots + x_s = x_{s+1} + \cdots + x_{2s}, \quad x_1, \ldots, x_{2s} \in S.
\]
If \( r = 2k \) for some integer \( k \), then \( T_{2k} \leq J_{2k} \). If \( r = 2k - 1 \) for some integer \( k \), then \( T_{2k-1}^2 \leq J_{2k-2} J_{2k} \).

**Proof.** Suppose that \( r = 2k \). Among all \((2k+1)\)-tuples \((l_1, \ldots, l_{2k}, l)\) with \( l_i \in \{\pm c_1, \ldots, \pm c_{2k}\}, \quad l \in \{0, c\}, \)
we consider a tuple for which the number of solutions of the equation
\[
l_1 x_1 + \cdots + l_{2k} x_{2k} = l, \quad x_1, \ldots, x_{2k} \in S,
\]
is maximal. If there are several such tuples, we choose the one for which the sequence \( l_1, \ldots, l_{2k} \) contains the maximal number of elements of \( \{-l_1, l_1\} \). We fix such a tuple \((l_1, \ldots, l_{2k}, l)\) with \( l_i \in \{-l_1, l_1\}, \quad i = 1, \ldots, s, \) where either \( s = 2k \) or \( l_t \not\in \{-l_1, l_1\} \) for \( t > s \). Let \( L_{2k} \) be the number of solutions of equation (6). We rewrite this equation in the form
\[
l_1 x_1 + \cdots + l_k x_k = l - (l_{k+1} x_{k+1} + \cdots + l_{2k} x_{2k}), \quad x_1, \ldots, x_{2k} \in S.
\]
Note that
\[
L_{2k} = \sum_{\lambda} I_1(\lambda) I_2(\lambda),
\]
where \( I_1(\lambda) \) is the number of solutions of the equation \( l_1 x_1 + \cdots + l_k x_k = \lambda, \quad x_1, \ldots, x_k \in S, \) and \( I_2(\lambda) \) is the number of solutions of the equation \( l-(l_{k+1} x_{k+1} + \cdots + l_{2k} x_{2k}) = \lambda, \quad x_{k+1}, \ldots, x_{2k} \in S. \)

Using the Cauchy–Schwarz inequality, we obtain
\[
L_{2k}^2 \leq \left( \sum_{\lambda} I_1^2(\lambda) \right) \left( \sum_{\lambda} I_2^2(\lambda) \right).
\]
The quantity in the second parenthesis is equal to the number of solutions of the equation

\[ l_{k+1}x_1 + \cdots + l_{2k}x_k = l_{k+1}x_{k+1} + \cdots + l_{2k}x_{2k}, \quad x_1, \ldots, x_{2k} \in S. \]

Hence, by the maximality of \( L_{2k} \) we have

\[ L_{2k} \leq \sum_{\lambda} I_1^2(\lambda). \]

The right-hand side is the number of solutions of the equation

\[ l_1x_1 + \cdots + l_kx_k = l_1x_{k+1} + \cdots + l_kx_{2k}, \quad x_1, \ldots, x_{2k} \in S. \tag{7} \]

Clearly, the sequence \( l_1, \ldots, l_k, l_1, \ldots, l_k \) contains \( \min\{2s, 2k\} \) elements of \( \{ -l_1, l_1 \} \). Since \( s \) is maximal, it follows that \( s = 2k \). Therefore we have \( l_i \in \{ -l_1, l_1 \} \) for all \( i \), whence the number of solutions of (7) is equal to \( J_{2k} \). Thus \( L_{2k} \leq J_{2k} \) and, therefore, \( T_{2k} \leq J_{2k} \). This proves the first part of the lemma.

To prove the second part, we consider the equation corresponding to \( T_{2k-1} \). Writing it in the form

\[ c_1x_1 + \cdots + c_kx_k = l - (c_{k+1}x_{k+1} + \cdots + c_{2k-1}x_{2k-1}) \]

and using the Cauchy–Schwarz inequality as above, we get

\[ T_{2k-1}^2 \leq \left( \sum_{\lambda} I_1^2(\lambda) \right) \left( \sum_{\lambda} I_2^2(\lambda) \right), \]

where \( I_{11}(\lambda) \) is the number of solutions of the equation \( c_1x_1 + \cdots + c_kx_k = \lambda, \ x_1, \ldots, x_k \in S \), and \( I_{22}(\lambda) \) is the number of solutions of the equation \(- (c_{k+1}x_{k+1} + \cdots + c_{2k-1}x_{2k-1}) = \lambda, \ x_{k+1}, \ldots, x_{2k-1} \in S \).

Using the first part of the lemma, we obtain that

\[ \sum_{\lambda} I_{11}^2(\lambda) \leq J_{2k}, \quad \sum_{\lambda} I_{22}^2(\lambda) \leq J_{2k-2}. \]

Let \( \xi \) be an algebraic integer of degree \( d \), and let \( O_\mathbb{K} \) be the ring of integers in the field \( \mathbb{K} = \mathbb{Q}(\xi) \). Our proof of Lemma 6 below uses the language of ideals in the Dedekind domain \( O_\mathbb{K} \) (for background see [24], Ch. 3, [25], Ch. 12). All the ideals considered below are integral. In particular, we say that an ideal \( I_2 \) divides \( I_1 \) if \( I_1 = I_2I_3 \) for some ideal \( I_3 \).

We shall use well-known properties of ideals. For example, if \( I_1 \) and \( I_2 \) are ideals and \( I_1 \subset I_2 \), then \( I_2 \) divides \( I_1 \) (see, for example, [25], Proposition 12.2.7).

It follows from the uniqueness of factorization into prime ideals that if \( I_1, I_2, I_3 \) are ideals in \( O_\mathbb{K} \) and \( I_3 \) divides \( I_1I_2 \), then \( I_3 = J_1J_2 \) for some ideals \( J_1 \) and \( J_2 \) that divide \( I_1 \) and \( I_2 \) respectively.

We shall use the fact that the number of integral ideals of norm \( n \) in \( O_\mathbb{K} \) does not exceed \( \tau(n)^d \), where \( \tau(n) \) is the number of divisors of \( n \). In particular, for a fixed constant \( d \) and large \( n \) this is a quantity of order \( n^{\Theta(1)} \). Note that the number
of positive integers not exceeding \( m^{O(1)} \) all of whose prime divisors divide \( m \) is bounded above by \( m^{o(1)} \) (this follows, for example, from basic properties of smooth numbers and the distribution of the primes).

We recall that the \textit{logarithmic height of a polynomial} \( P \in \mathbb{Z}[Z] \) is defined as the logarithm of the maximal absolute value of the coefficients of \( P \). The \textit{logarithmic height of an algebraic number} \( \alpha \) is defined as the logarithmic height of its minimal polynomial. It is a well-known consequence of the basic properties of Mahler’s measure that if \( P, Q \in \mathbb{Z}[Z] \) are non-zero polynomials in one variable with \( Q | P \) and the logarithmic height of \( P \) does not exceed \( H \), then the logarithmic height of \( Q \) does not exceed \( H + O(1) \), where the constant implied in \( O(1) \) depends only on \( \deg P \) (see, for example, [26], Theorem 4.2.2).

In particular, if \( P \in \mathbb{Z}[Z] \) is non-constant and the absolute values of its coefficients do not exceed \( M \), then every root \( \sigma \) of \( P(Z) \) can be written in the form \( \xi/q \), where \( \xi \) is an algebraic integer of logarithmic height \( O(\log M) \) and \( q \) is a positive integer with \( q < M^{O(1)} \), where the constant implied in \( O(1) \) depends only on \( \deg P \).

\textbf{Lemma 6.} For every fixed positive integer constant \( r \) and all values of \( \sigma \in \mathbb{C} \), the number \( T_r(\sigma, N) \) of solutions of the equation

\[
\frac{1}{\sigma + x_1} + \cdots + \frac{1}{\sigma + x_r} = \frac{1}{\sigma + x_{r+1}} + \cdots + \frac{1}{\sigma + x_{2r}} \tag{8}
\]

in positive integers \( x_1, \ldots, x_{2r} \leq N \) satisfies

\[ T_r(a, N) < N^r + o(1). \]

\textbf{Proof.} For brevity we put \( T_r = T_r(a, N) \). The proof is by induction on \( r \). For \( r = 1 \) the assertion is trivial. Suppose that \( r \geq 2 \).

It follows from Lemma 5 that the number of solutions satisfying \( x_i = x_j \) for some \( i \neq j \) contributes to \( T_r \) a quantity of order \( O(\sqrt{T_{r-1}T_r}) \). Hence, by the inductive hypothesis, it suffices to show that

\[ T'_r < N^r + o(1), \]

where \( T'_r \) is the number of solutions of (8) such that \( x_i \neq x_j \) for all \( i \neq j \). We can also assume that \( T'_r > N^r \) (otherwise there is nothing to prove). Rewrite (8) in the form

\[
\prod_{i \neq 1} (\sigma + x_i) + \cdots + \prod_{i \neq r} (\sigma + x_i) = \prod_{i \neq r+1} (\sigma + x_i) + \cdots + \prod_{i \neq 2r} (\sigma + x_i)
\]

and consider the polynomial

\[
P(Z) = \prod_{i \neq 1} (Z + x_i) + \cdots + \prod_{i \neq r} (Z + x_i) - \prod_{i \neq r+1} (Z + x_i) - \cdots - \prod_{i \neq 2r} (Z + x_i).
\]

Clearly, \( \deg P \leq 2r - 1 \). Note also that \( P(-x_1) \neq 0 \). Hence \( P(Z) \) is not identically zero. Moreover, since \( P(\sigma) = 0 \), it follows that \( P(Z) \) is non-constant. Therefore we may assume that \( \sigma \) is an algebraic number of degree \( d \) with \( 1 \leq d \leq 2r - 1 \) and
of logarithmic height $O(\log N)$. We can write $\sigma$ in the form $\sigma = \xi/q$, where $\xi$ is an algebraic integer of height $O(\log N)$ and $q$ is an integer with $q = N^{O(1)}$. Then equation (8) takes the form

$$\prod_{i \neq 1} (\xi + qx_i) + \cdots + \prod_{i \neq r} (\xi + qx_i) = \prod_{i \neq r+1} (\xi + qx_i) + \cdots + \prod_{i \neq 2r} (\xi + qx_i). \quad (9)$$

Let $O_\mathbb{K}$ be the ring of integers in $\mathbb{K} = \mathbb{Q}(\xi)$. The idea is to use the observation that for all $i = 1, \ldots, 2r$ we have

$$\xi + qx_i \mid q^{2r-1} \prod_{j \neq i} (x_j - x_i). \quad (10)$$

The strategy for estimating the number of solutions of (9) is successively to introduce the variables $x_1, x_2, \ldots$, taking into account the congruences that arise from fixing the previous variables.

We denote the norm of an ideal $I$ by $\nu(I)$. The principal ideal $(\xi + qx_1)$ factorizes as

$$(\xi + qx_1) = I_1 J_1,$$

where the prime factors of $I_1$ divide $q$ and $J_1$ is coprime to $q$. By (10), the norm $\nu(J_1)$ divides $\prod_{j \geq 2} (x_j - x_1)^d$. Hence,

$$x_j \equiv x_1 \pmod{r_j}, \quad 2 \leq j \leq 2r, \quad (11)$$

for some $r_j \in \mathbb{Z}_+$ such that $\nu(J_1) \mid \nu_1^d$ with $\nu_1 = \prod_{j \geq 2} r_j$ and $\nu_1 \mid \nu(J_1)$. We restrict $\nu_1$ to dyadic intervals: there is a fixed number $\mu_1 \geq 1$ such that if we restrict $\nu_1$ to the interval

$$\mu_1 \leq \nu_1 \leq 2\mu_1, \quad (12)$$

then the number of solutions of (9) with this restriction changes by a factor no bigger than $N^{o(1)}$.

For every $x_1$ we consider at most $N^{o(1)}$ different cases and, according to (11), prescribe $x_j$, $j \geq 2$, to lie in the arithmetic progressions $L_{2,j} \in [1, N]$, where we thus have

$$\prod_{j \geq 2} |L_{2,j}| < \frac{N^{2r-1+o(1)}}{\mu_1}. \quad (13)$$

At the next step, for every $x_2 \in L_{2,2}$ we factorize $(\xi + qx_2)$ as

$$(\xi + qx_2) = I_2 J_2,$$

where the prime factors of $I_2$ divide $q$ or $\nu(\xi + qx_1)$ and $J_2$ is coprime to $q$ and $\nu(\xi + qx_1)$. Therefore $J_2$ is coprime to $(x_2 - x_1)$ and, again by (10), $\nu(J_2)$ divides $\prod_{j \geq 3} (x_j - x_2)^d$. Arguing as above, we find a $\nu_2$ such that $\nu(J_2) \mid \nu_2^d$ and $\nu_2 \mid \nu(J_2)$. As above, we can restrict $\nu_2$ to a dyadic interval: there is a fixed number $\mu_2 \geq 1$ (independent of the $x_i$) such that if we restrict $\nu_2$ to the interval

$$\mu_2 \leq \nu_2 \leq 2\mu_2, \quad (14)$$

we can successively introduce the variables $x_1, x_2, \ldots$.
then the number of solutions of (9) with this restriction is changed by a factor no bigger than $N^{o(1)}$. For every $x_2 \in L_{2,2}$ we consider $N^{o(1)}$ possibilities and prescribe $x_j$, $j \geq 3$, to lie in the arithmetic progressions $L_{3,j} \subset L_{2,j}$, where

$$\prod_{j \geq 3} |L_{3,j}| \leq \frac{1}{\mu_2} \prod_{j \geq 3} |L_{2,j}|, \quad \nu(J_2) | \nu_2^d.$$  \hspace{1cm} (15)

Note that the progressions $L_{2,j}$ are determined by some moduli $r_j | \nu_1$ and, since $\nu(J_1)$ and $\nu(J_2)$ are coprime, $r_j$ and $\nu(J_2)$ are also coprime.

At the next step, for every $x_3 \in L_{3,3}$ we factorize $(\xi + qx_3)$ as

$$(\xi + qx_3) = I_3 J_3,$$

where the prime factors of $I_3$ divide $(q)$, $\nu(\xi + qx_1)$ or $\nu(\xi + qx_2)$, and $J_3$ is coprime to $(q)$, $\nu(\xi + qx_1)$ and $\nu(\xi + qx_2)$. As in the previous cases, we can find a $\nu_3$ in a dyadic interval $\mu_3 \leq \nu_3 \leq 2\mu_3$, where $\mu_3$ is independent of the variables.

The continuation of the process is clear. We now successively fix $x_1 \leq N$, $x_2 \in L_{2,2}$, $\ldots$, $x_{2r} \in L_{2r,2r}$. More precisely, we fix $x_1$ and, considering the $N^{o(1)}$ possibilities for the arithmetic progressions $L_{2,j}$, $j \geq 3$, fix $x_2 \in L_{2,2}$. We then consider the $N^{o(1)}$ possibilities for the arithmetic progressions $L_{3,j}$, $j \geq 3$, fix $x_3 \in L_{3,3}$ and repeat this process until we fix $x_{2r} \in L_{2r,2r}$. Hence we estimate the number of solutions of (9) as $N^{o(1)}$ contributions of size

$$N|L_{2,2}| |L_{3,3}| \cdots |L_{2r,2r}|.$$

It follows from (13), (15) and the iteration process that

$$N^{2r-1} \gtrsim \mu_1 |L_{2,2}| \prod_{j \geq 3} |L_{2,j}| \gtrsim \mu_1 \mu_2 |L_{2,2}| |L_{3,3}| \prod_{j \geq 4} |L_{3,j}| \gtrsim \cdots$$

$$\cdots \gtrsim \mu_1 \cdots \mu_{2r-1} |L_{2,2}| \cdots |L_{2r,2r}|.$$

Here $A \gtrsim B$ means that $A > BN^{o(1)}$. Thus the number of solutions of (9) is bounded by

$$\frac{N^{2r+o(1)}}{\mu_1 \cdots \mu_{2r-1}}.$$ \hspace{1cm} (16)

Furthermore, it is clear from our construction that $\nu(I_1) = N^{O(1)}$. Since the prime factors of $I_1$ divide $q$, it follows that the number of possibilities for $I_1$ does not exceed $N^{o(1)}$. Fixing $I_1$ and denoting the conjugates of $\xi$ by $\xi_1 = \xi, \xi_2, \ldots, \xi_d$, we have

$$\prod_{s=1}^d (\xi_s + qx_1) = \nu(I_1) \nu(J_1).$$

Since $\nu(J_1) | \nu_1^d$, there are at most $N^{o(1)}$ possibilities for $\nu(J_1)$ with a fixed $\nu_1$. Hence, given $\nu_1$, we have at most $N^{o(1)}$ possible values for $x_1$. It follows that the number of possibilities for $x_1$ subject to (12) is at most $N^{o(1)} \mu_1$. Next, for a fixed $x_1$ there are at most $N^{o(1)}$ possibilities for the ideal $I_2$ and, similarly, at most $N^{o(1)} \mu_2$ possibilities for $x_2$. Arguing in this way, we see that the number of possibilities
for \(x_1, x_2, \ldots, x_{2r-1}\) is at most \(\mu_1 \mu_2 \cdots \mu_{2r-1} N^{o(1)}\). Thus the number of solutions of (9) is bounded by \(\mu_1 \mu_2 \cdots \mu_{2r-1} N^{o(1)}\). Since the number of solutions of (9) is also bounded by (16), we get the desired result. □

**Lemma 7.** Let \(x, y, z, a_1, a_2, b_1, b_2\) be complex numbers such that

\[
xyz = a_1(x + y + z) + b_1, \\
xy + yz + zx = a_2(x + y + z) + b_2.
\]

Then

\[
(x^2 - a_2x + a_1)(y^2 - a_2y + a_1)(z^2 - a_2z + a_1) = (b_1 - \alpha_1 \alpha_2 - \alpha_1^3)(b_1 - \alpha_2 \alpha_2 - \alpha_2^3),
\]

where

\[
\alpha_1 = \frac{a_2 + \sqrt{a_2^2 - 4a_1}}{2}, \quad \alpha_2 = \frac{a_2 - \sqrt{a_2^2 - 4a_1}}{2}.
\]

**Proof.** Since \(\alpha_i^2 - a_2 \alpha_i + a_1 = 0\), we have

\[
(x - \alpha_i)(y - \alpha_i)(z - \alpha_i) = b_1 - \alpha_i \alpha_2 - \alpha_i^3, \quad i = 1, 2.
\]

Multiplying these equalities, we get the result. □

**Lemma 8.** Let \(A, B\) be integers with \(AB \neq 0\) and \(|A|, |B| < N^{O(1)}\). Then the Diophantine equation

\[
Axy + Bx + By = 0 \tag{17}
\]

has at most \(N^{o(1)}\) solutions in integers \(x, y\) with \(|x|, |y| \leq N^{O(1)}\).

**Proof.** We have

\[
(Ax + B)(Ay + B) = B^2,
\]

and the assertion follows from the well-known bound for the number of divisors. □

**Lemma 9.** Let \(a_0, b_0, u_0, v_0\) be integers with \(b_0 u_0 v_0 \neq 0\) and

\[
|a_0|, |b_0|, |u_0|, |v_0| < N^{O(1)}.
\]

Assume that

\[
\frac{u_0}{v_0} \not\in \left\{ \frac{b_0}{a_0 + bx}; 1 \leq x \leq N \right\}.
\]

Then the number \(J\) of solutions of the Diophantine equation

\[
u_0(a_0 + b_0 x_1)(a_0 + b_0 x_2)(a_0 + b_0 x_3) = v_0 b_0
\]

\[
\times \left( (a_0 + b_0 x_1)(a_0 + b_0 x_2) + (a_0 + b_0 x_2)(a_0 + b_0 x_3) + (a_0 + b_0 x_3)(a_0 + b_0 x_1) \right)
\]

in integers \(x_1, x_2, x_3\) with \(1 \leq x_i \leq N\) and \(a_0 + b_0 x_i \neq 0\) satisfies the estimate

\[
J < N^{\frac{3}{2} + o(1)}.
\]
Proof. We can assume that $b_0 > 0$, $v_0 > 0$, $(a_0, b_0) = 1$. Observe that if one of
the variables $x_1, x_2, x_3$ is determined, then there are at most $N^{o(1)}$ possibilities
for the other two. Indeed, let $x_1$ be fixed. Then, writing
\[ X_i = a_0 + b_0x_i, \quad A = u_0X_1 - v_0b_0, \quad B = -v_0b_0X_1, \]
we get
\[ AX_2X_3 + BX_2 + BX_3 = 0. \]
By hypothesis, $AB \neq 0$ and $|A|, |B| < N^{O(1)}$. Hence, by Lemma 8 there are at most
$N^{o(1)}$ possible values for $x_2, x_3$ (and thus also for $x_2, x_3$).
Put
\[ u'_0 = \frac{u_0}{(u_0, b_0v_0)}, \quad \frac{b_0v_0}{(u_0, b_0v_0)} = w_0 \geq 1. \]
We have
\[ u'_0(a_0 + b_0x_1)(a_0 + b_0x_2)(a_0 + b_0x_3) \]
\[ = w_0((a_0 + b_0x_1)(a_0 + b_0x_2) + (a_0 + b_0x_2)(a_0 + b_0x_3) + (a_0 + b_0x_3)(a_0 + b_0x_1)). \]
Since $(u'_0, w_0) = 1$, there is a representation
\[ w_0 = w_1w_2w_3 \tag{18} \]
such that
\[ a_0 + b_0x_i = w_iy_i, \quad i = 1, 2, 3, \tag{19} \]
for some non-zero integers $y_1, y_2, y_3$. In particular,
\[ u'_0y_1y_2y_3 = w_1w_2y_1y_2 + w_2w_3y_2y_3 + w_3w_1y_3y_1. \tag{20} \]
We can assume that $w_1 \geq w_2 \geq w_3 \geq 1$. By (18) and the bound for the number
of divisors, there are at most $N^{o(1)}$ possible values for $w_1, w_2, w_3$. We fix such
a representation. Then the condition $(a_0, b_0) = 1$ and the equality
\[ a_0 + b_0x_1 = w_1y_1 \tag{21} \]
implies that $(b_0, w_1) = 1$. Hence (21) uniquely determines $x_1 \pmod{w_1}$. It follows
that there are at most $N^{1+o(1)}w_1^{-1} + 1$ possible values for $x_1$. We can then recover
$x_2, x_3$ and get the bound
\[ J < N^{1+o(1)}w_1^{-1} + N^{o(1)}. \tag{22} \]
Furthermore, by (20) and the fact that $w_1 \geq w_2 \geq w_3 \geq 1$ we have
\[ |u'_0| \min\{|y_1|, |y_2|, |y_3|\} \leq 3w_1^2. \]
Thus,
\[ \min\{|y_1|, |y_2|, |y_3|\} \leq 3w_1^2. \]
Hence there are $O(w_1^2)$ possible ways to determine one of the variables $y_1, y_2, y_3$. By (19) we can then determine one of the variables $x_1, x_2, x_3$ and thus obtain that
\[ J < w_1^2N^{o(1)}. \]
Comparing this with (22), we conclude that $J < N^{\frac{5}{2}+o(1)}$. □
§ 6. Congruences

In what follows $N$ is a large parameter, $N < p$. We start with the following result from [2], whose proof is based on ideas of Heath–Brown [27].

**Lemma 10.** Suppose that $\lambda \not\equiv 0 \pmod{p}$. Then the number $J$ of solutions of the congruence

$$xy \equiv \lambda \pmod{p}, \quad L + 1 \leq x, y \leq L + N,$$

satisfies

$$J < \frac{N^{3/2 + o(1)}}{p^{3/2}} + N^{o(1)}.$$

In particular, if $N < p^{1/3}$, then one has $J < N^{o(1)}$.

**Corollary 4.** Suppose that $\lambda \not\equiv 0 \pmod{p}$. Then the number $J$ of solutions of the congruence

$$\frac{1}{x} + \frac{1}{y} \equiv \lambda \pmod{p}, \quad L + 1 \leq x, y \leq L + N,$$

satisfies

$$J < \frac{N^{3/2 + o(1)}}{p^{3/2}} + N^{o(1)}.$$

In particular, if $N < p^{1/3}$, then one has $J < N^{o(1)}$.

**Proof.** Indeed, we have

$$(x - \lambda^{-1})(y - \lambda^{-1}) \equiv \lambda^{-2} \pmod{p},$$

and the claim follows from Lemma 10. \(\Box\)

The following result was proved in [2] (see also [28] for an extension to the case of many variables).

**Lemma 11.** Suppose that $\lambda \not\equiv 0 \pmod{p}$ and $N < p^{1/3}$. Then the number $J$ of solutions of the congruence

$$xyz \equiv \lambda \pmod{p}, \quad L + 1 \leq x, y \leq L + N,$$

satisfies

$$J < N^{o(1)}.$$

The following lemma follows from [29] (and from Lemma 10 when $|I_1||I_2|$ is very small). Note that this lemma will be used only in the case when one of the intervals starts at the origin (this particular case was established in [30]).

**Lemma 12.** Let $I_1, I_2$ be intervals in $\mathbb{F}_p^*$ with $|I_1||I_2| < p$. Then the congruence

$$xy = zt, \quad (x, z) \in I_1 \times I_1, \quad (y, t) \in I_2 \times I_2,$$

has at most $(|I_1||I_2|)^{1+o(1)}$ solutions.
The following lemma will be used in the proofs of Theorems 2, 3. We state it with explicit constants to make the assertion more transparent (these constants should not be taken too seriously).

**Lemma 13.** Suppose that \( I = \{a + 1, \ldots, a + N\} \) and \( \lambda \not\equiv 0 \pmod{p} \), \( \lambda \not\in \{x^{-1} \pmod{p} : x \in I\} \). Assume that

\[
|I| = N < 0.1 p^{\frac{1}{17}} J^{\frac{2}{9}}
\]

where \( J \) is the number of solutions of the congruence

\[
x^{-1} + y^{-1} + z^{-1} \equiv \lambda \pmod{p}, \quad x, y, z \in I.
\]

Assume also that \( J > N^\varepsilon \) for some fixed small constant \( \varepsilon > 0 \) and let \( N \) be sufficiently large. Then there are integers \( \Delta'_4 \), \( \Delta''_4 \), \( \Delta_3 \) with

\[
|\Delta'_4| < \frac{10^5 N^4}{J}, \quad |\Delta''_4| < \frac{10^5 N^4}{J}, \quad |\Delta_3| < \frac{10^5 N^3}{J}
\]

such that

\[
a \equiv \frac{\Delta'_4}{\Delta_3} \pmod{p}, \quad \lambda^{-1} \equiv \frac{\Delta''_4}{\Delta_3} \pmod{p}.
\]

**Proof.** It follows from the hypotheses that \( J \) is equal to the number of solutions of the congruence

\[
\lambda(a + x)(a + y)(a + z) \equiv (a + x)(a + y) + (a + y)(a + z) + (a + z)(a + x) \pmod{p} \quad (23)
\]

in positive integers \( x, y, z \leq N \) with \( (a + x)(a + y)(a + z) \not\equiv 0 \pmod{p} \).

Note that by Corollary 4 we have \( J < N^{1 + o(1)} \), whence \( N < p^{\frac{1}{17}} \). Rewrite (23) in the form

\[
xyz + (a - \lambda^{-1})(xy + yz + zx) + (a^2 - 2a\lambda^{-1})(x + y + z) + (a^3 - 3a^2\lambda^{-1}) \equiv 0 \pmod{p}. \quad (24)
\]

We fix a solution \( (x_0, y_0, z_0) \) and get

\[
(a^2 - 2a\lambda^{-1})(x + y + z - A_0) + (a - \lambda^{-1})(xy + yz + zx - B_0) + (xyz - C_0) \equiv 0 \pmod{p}, \quad (25)
\]

where

\[
A_0 = x_0 + y_0 + z_0, \quad B_0 = x_0y_0 + y_0z_0 + z_0x_0, \quad C_0 = x_0y_0z_0.
\]

We use some ideas from [13]. Define a lattice

\[
\Gamma = \{(u, v, w) \in \mathbb{Z}^3 : (a^2 - 2a\lambda^{-1})u + (a - \lambda^{-1})v + w \equiv 0 \pmod{p}\}
\]

and a body

\[
D = \{(u, v, w) \in \mathbb{R}^3 : |u| \leq 3N, |v| \leq 3N^2, |w| \leq N^3\}.
\]
Since every fixed vector
\[(x + y + z - A_0, xy + yz + zx - B_0, xyz - C_0)\]
determines the values of \(x, y, z\) with at most 6 possibilities, we have
\[|D \cap \Gamma| \geq \frac{J}{6}.
\]
Therefore, by Corollary 3, the successive minima \(\lambda_i = \lambda_i(D, \Gamma), \ i = 1, 2, 3,\) satisfy the inequality
\[
\prod_{i=1}^{3} \min\{1, \lambda_i\} < 1000J^{-1}.
\]
In particular, \(\lambda_1 \leq 1\). By the definition of \(\lambda_i\) there are linearly independent vectors
\[(u_i, v_i, w_i) \in \lambda_i D \cap \Gamma, \ i = 1, 2, 3.
\]
We consider the following three cases separately.
Case 1: \(\lambda_3 \leq 1\). Then \(\lambda_1 \lambda_2 \lambda_3 < 1000J^{-1}\). Consider the determinant
\[
\Delta = \det \begin{pmatrix} u_1 & v_1 & w_1 \\ u_2 & v_2 & w_2 \\ u_3 & v_3 & w_3 \end{pmatrix}.
\]
Clearly, \(|\Delta| < 6N^6 \lambda_1 \lambda_2 \lambda_3 < 6000N^6/J < p\). Thus \(|\Delta| < p\). On the other hand, the congruence
\[(a^2 - 2a\lambda^{-1})u_i + (a - \lambda^{-1})v_i + w_i \equiv 0 \pmod{p}, \quad i = 1, 2, 3,
\]
yields that \(\Delta\) is divisible by \(p\). Therefore \(\Delta = 0\) contrary to the linear independence of the vectors \((u_i, v_i, w_i), \ i = 1, 2, 3\). Thus this case is impossible.

Case 2: \(\lambda_1 \leq 1, \ \lambda_2 > 1\). Since \(\lambda_2 > 1\), the vectors \((x + y + z - A_0, xy + yz + zx - B_0, xyz - C_0)\) and \((u_1, v_1, w_1)\) are linearly dependent. Therefore one of the following conditions holds:
(i) \(x + y + z - A_0 = 0\);
(ii) \(xyz = \frac{w_1}{u_1}(x + y + z) + C_0 - \frac{w_1}{u_1}A_0, xy + yz + zx = \frac{w_1}{u_1}(x + y + z) + B_0 - \frac{w_1}{u_1}A_0\).

If a solution \((x, y, z)\) satisfies (i), then the congruence (24) may be written in the form
\[
\left(x + a - \frac{1}{\lambda}\right)\left(y + a - \frac{1}{\lambda}\right)\left(z + a - \frac{1}{\lambda}\right) \equiv \lambda' \pmod{p}.
\]
Since \(\lambda \notin I^{-1} \pmod{p}\), we have \(\lambda' \not\equiv 0 \pmod{p}\). Hence, by Lemma 11, the solutions satisfying (i) contribute at most \(N^{o(1)}\) to \(J\).

If a solution \((x, y, z)\) satisfies (ii), then Lemma 7 and the bound for the number of divisors imply that one of the variables \(x, y, z\) is determined up to at most \(N^{o(1)}\) possibilities. By Corollary 4 it follows that the solutions satisfying (ii) also contribute at most \(N^{o(1)}\) to \(J\).

Thus we obtain that \(J < N^{o(1)}\). This contradicts our assumption that \(J > N^\varepsilon\). Hence this case is impossible.
Case 3: $\lambda_1 \leq 1$, $\lambda_2 \leq 1$, $\lambda_3 > 1$. Then $\lambda_1 \lambda_2 < 1000J^{-1}$. Furthermore,

$$\begin{pmatrix} u_1 & v_1 \\ u_2 & v_2 \end{pmatrix} \begin{pmatrix} a^2 - 2a\lambda^{-1} \\ a - \lambda^{-1} \end{pmatrix} \equiv \begin{pmatrix} -w_1 \\ -w_2 \end{pmatrix} \pmod{p}. \quad (26)$$

Put

$$\Delta_3 = \det \begin{pmatrix} u_1 & v_1 \\ u_2 & v_2 \end{pmatrix}, \quad \Delta_5 = \det \begin{pmatrix} -w_1 & v_1 \\ -w_2 & v_2 \end{pmatrix}, \quad \Delta_4 = \det \begin{pmatrix} u_1 & -w_1 \\ u_2 & -w_2 \end{pmatrix}.$$ 

We have

$$|\Delta_3| < \frac{2000N^3}{J}, \quad |\Delta_5| < \frac{2000N^5}{J}, \quad |\Delta_4| < \frac{2000N^4}{J}. \quad (27)$$

Note that

$$\Delta_3 \not\equiv 0 \pmod{p}. \quad (28)$$

Indeed, assume the opposite. By (26) we get

$$\Delta_3 \equiv \Delta_5 \equiv \Delta_4 \equiv 0 \pmod{p}.$$ 

Taking (27) into account, we see that $\Delta_3 = \Delta_5 = \Delta_4 = 0$. But then the rank of the matrix

$$\begin{pmatrix} u_1 & v_1 & w_1 \\ u_2 & v_2 & w_2 \end{pmatrix}$$

is strictly less than 2. This contradicts the linear independence of the vectors $(u_i, v_i, w_i), \ i = 1, 2$. Therefore condition (28) holds. Hence,

$$a^2 - 2a\lambda^{-1} \equiv \frac{\Delta_5}{\Delta_3} \pmod{p}, \quad a - \lambda^{-1} \equiv \frac{\Delta_4}{\Delta_3} \pmod{p}. \quad (29)$$

Using (24), we also have

$$a^3 - 3a^2\lambda^{-1} \equiv \frac{\Delta_6}{\Delta_3} \pmod{p} \quad (30)$$

for some integer $\Delta_6$ with $|\Delta_6| < 6000N^6/J$. We have

$$\lambda^{-2} \equiv \frac{\Delta_4^2}{\Delta_3^2} - \frac{\Delta_5}{\Delta_3} \equiv \frac{\Delta_4^2 - \Delta_5 \Delta_3}{\Delta_3^2} \pmod{p}. \quad (31)$$

Furthermore, substituting $\lambda^{-1} \equiv a - (\Delta_4/\Delta_3) \pmod{p}$ in the first congruence in (29) and in (30), we get

$$\Delta_3 a^2 - 2\Delta_4 a + \Delta_5 \equiv 0 \pmod{p}, \quad 2\Delta_3 a^3 - 3\Delta_4 a^2 + \Delta_6 \equiv 0 \pmod{p}.$$ 

It follows that

$$\Delta_4 a^2 - 2\Delta_5 a + \Delta_6 \equiv 0 \pmod{p}.$$ 

Consider the polynomials

$$P(Z) = \Delta_4 Z^2 - 2\Delta_5 Z + \Delta_6, \quad Q(Z) = \Delta_3 Z^2 - 2\Delta_4 Z + \Delta_5.$$
Since $P(a) \equiv Q(a) \equiv 0 \pmod{p}$, we have $\text{Res}(P, Q) \equiv 0 \pmod{p}$. On the other hand,

$$|\text{Res}(P, Q)| < \frac{10^{18}N^{18}}{J^4} < p.$$ 

Thus,

$$\text{Res}(P, Q) = 0.$$ 

Then the polynomials $P(Z)$ and $Q(Z)$ have a common root. If $Q(Z)$ is irreducible in $\mathbb{Q}[Z]$, then $Q(Z)$ and $P(Z)$ are linearly dependent. It follows that

$$\Delta_2^2 = \Delta_5 \Delta_3.$$ 

This is impossible in view of (31). Hence $Q(Z)$ is reducible in $\mathbb{Q}[Z]$ and its discriminant is the square of an integer. Thus,

$$\Delta_4^2 - \Delta_5 \Delta_3 = m^2, \quad m \in \mathbb{Z}_+.$$ 

It follows that $m < 10^4N^4/J$. Furthermore,

$$\lambda^{-2} \equiv \frac{m^2}{\Delta_3} \pmod{p}.$$ 

Hence,

$$\lambda^{-1} \equiv \frac{\Delta_4''}{\Delta_3} \pmod{p}, \quad |\Delta_4''| = m < \frac{10^4N^4}{J}.$$ 

Therefore we also have

$$a \equiv \frac{\Delta_4}{\Delta_3} + \lambda^{-1} \equiv \frac{\Delta_4'}{\Delta_3} \pmod{p}, \quad |\Delta_4'| < \frac{10^5N^4}{J}. \quad \square$$

§ 7. Proof of Theorems 1–6

Proof of Theorem 1. Suppose that $I = [a + 1, a + N]$. We first consider the case when $N < p^{\frac{k+1}{2k}}$. Our aim in this case is to prove the bound

$$J_{2k} < \frac{N^{2k^2}}{p^{k+1}} + o(1).$$ 

Put

$$V = [N^{\frac{k+1}{2}}, \quad Y = [N^{\frac{2}{k+1}}], \quad I_1 = [a + 1, a + 2N].$$ 

We define a subset $\mathcal{V} \subset [0.5V, V]$ in the following way. For every $v \in [0.5V, V]$ we define a function $\eta_v: I_1 \to \mathbb{Z}_+$ by putting

$$\eta_v(u') = |\{(u_1', v_1) \in I_1 \times [0.5V, V]; \ u_1'v_1 \equiv u'v \pmod{p}\}|.$$ 

By Lemma 12 we have

$$\sum_{u' \in I_1} \sum_{v \in [0.5V, V]} \eta_v(u') < N^{1+o(1)}V.$$
Hence there is a subset $\mathcal{V} \subset [0.5V, V]$ with $|\mathcal{V}| \sim V$ such that
\[
\sum_{u' \in I_1} \eta_v(u') < N^{1+o(1)} \quad \forall v \in \mathcal{V}. \tag{32}
\]

For any fixed integers $y_i \in \mathcal{V} = [0.5Y, Y]$ and $v \in \mathcal{V}$, the quantity $J_{2k}$ does not exceed the number of solutions of the congruence
\[
\frac{1}{u'_1 - vy_1} + \cdots + \frac{1}{u'_k - vy_k} \equiv \frac{1}{u'_{k+1} - vy_{k+1}} + \cdots + \frac{1}{u'_{2k} - vy_{2k}} \pmod{p}
\]
in integers $u'_i \in I_1$. Summing over $y_i$ and $v \in \mathcal{V}$, we get
\[
Y^{2k} \mathcal{V} J_{2k} \ll \frac{1}{p} \sum_{n=0}^{p-1} \sum_{v \in \mathcal{V}} \left( \sum_{u' \in S_{v,B}} e_p(n(u' - vy)^{-1}) \right)^{2k}. \tag{33}
\]

For $v \in \mathcal{V}$ and any number $B$ of the form $B = 2^s < N$ we put
\[
S_{v,B} = \{u' \in I_1; 0.5B \leq \eta_v(u') < B\}.
\]
In particular, $I_1 = \bigcup_B S_{v,B}$. Since $v \in \mathcal{V}$, we obtain from (32) that
\[
|S_{v,B}| \sim \frac{N^{1+o(1)}}{B}. \tag{34}
\]
By (33) we have
\[
Y^{2k} \mathcal{V} J_{2k} \ll \frac{N^{o(1)}}{p} \sum_{n=0}^{p-1} \sum_{v \in \mathcal{V}} \left( \sum_{u' \in S_{v,B}} e_p(n(u' - vy)^{-1}) \right)^{2k}.
\]
Hence Hölder’s inequality and (34) yield the following estimate for some fixed $B$:
\[
Y^{2k} \mathcal{V} J_{2k} \ll \frac{N^{o(1)}}{p} \left( \frac{N}{B} \right)^{2k-1} \sum_{n=0}^{p-1} \sum_{v \in \mathcal{V}} \sum_{u' \in S_{v,B}} \sum_{y \in \mathcal{Y}} e_p(n(u' - vy)^{-1})^{2k}. \tag{35}
\]
The quantity
\[
\frac{1}{p} \sum_{n=0}^{p-1} \sum_{v \in \mathcal{V}} \sum_{u' \in S_{v,B}} \left( \sum_{y \in \mathcal{Y}} e_p(n(u' - vy)^{-1}) \right)^{2k}
\]
is bounded by the number of solutions of the congruence
\[
\frac{1}{u' - vy_1} + \cdots + \frac{1}{u' - vy_k} \equiv \frac{1}{u' - vy_{k+1}} + \cdots + \frac{1}{u' - vy_{2k}} \pmod{p}
\]
in the variables $v \in \mathcal{V}$, $u' \in S_{v,B}$, $y \in \mathcal{Y}$. Therefore we get
\[
\frac{1}{p} \sum_{n=0}^{p-1} \sum_{v \in \mathcal{V}} \sum_{u' \in S_{v,B}} \left( \sum_{y \in \mathcal{Y}} e_p(n(u' - vy)^{-1}) \right)^{2k} \ll Y^k \mathcal{V} \frac{N^{1+o(1)}}{B} + Y^{2k} B.
\]
Hence we obtain from (35) that

\[ Y^{2k}V J_{2k} \ll N^{2k-1+o(1)} B^{-2k+1} \left( Y^k V \frac{N^{1+o(1)}}{B} + Y^{2k} B \right) . \]

Thus,

\[ J_{2k} < N^{2k+o(1)} Y^{-k} + \frac{N^{2k-1+o(1)}}{V} < N^{\frac{2k^2}{k+1} + o(1)} . \]

This proves the desired result in the case when \( N < p^{\frac{k+1}{2k}} \).

Now suppose that \( N > p^{\frac{k+1}{2k}} \). Split the interval \( I = [a+1, a+N] \) into \( K \sim N p^{\frac{k+1}{2k}} \) subintervals of length at most \( N_1 = p^{\frac{k+1}{2k}} \). Then there are intervals \( I^{(1)}, \ldots, I^{(2k)} \) of lengths at most \( N_1 \) such that we have

\[ J_{2k} < K^{2k} R_{2k} \ll \left( \frac{N}{p^{\frac{k+1}{2k}}} \right)^{2k} R_{2k} , \]

where \( R_{2k} \) is the number of solutions of the congruence

\[ \frac{1}{x_1} + \cdots + \frac{1}{x_k} \equiv \frac{1}{x_{k+1}} + \cdots + \frac{1}{x_{2k}} \pmod{p}, \quad x_i \in I^{(i)}, \quad i = 1, \ldots, 2k. \]

Expressing \( R_{2k} \) in terms of exponential sums and using Hölder’s inequality, we get

\[ R_{2k} \leq \prod_{i=1}^{2k} (R_{2k}(i))^\frac{1}{2k} , \]

where \( R_{2k}(i) \) is the number of solutions of the congruence

\[ \frac{1}{x_1} + \cdots + \frac{1}{x_k} \equiv \frac{1}{x_{k+1}} + \cdots + \frac{1}{x_{2k}} \pmod{p}, \quad x_1, \ldots, x_{2k} \in I^{(i)}. \]

Thus, for some fixed \( i = i_0 \) we have

\[ R_{2k} \leq R_{2k}(i_0) . \]

Since \( |I^{(i_0)}| \leq N_1 = p^{\frac{k+1}{2k}} \), we know from what was proved above that

\[ R_{2k}(i_0) < N_1^{\frac{2k^2}{k+1} + o(1)} = p^k N^{o(1)} . \]

Hence,

\[ J_{2k} < \left( \frac{N}{p^{\frac{k+1}{2k}}} \right)^{2k} p^k N^{o(1)} = \frac{N^{2k+o(1)}}{p} . \]

This completes the proof of the theorem. \( \square \)

Proof of Theorem 2. Suppose that \( I = \{ a+1, \ldots, a+N \} \). We can assume that \( N \) is large and \( J > N^\frac{\delta}{2} \log N \) (otherwise there is nothing to prove). The hypotheses of Lemma 13 hold, whence there are integers \( \Delta_4', \Delta_4'', \Delta_3 \) with

\[ |\Delta_4'| < N^\frac{10}{3}, \quad |\Delta_4''| < N^\frac{10}{3}, \quad |\Delta_3| < N^\frac{7}{2} \quad (36) \]
such that
\[ a \equiv \frac{\Delta'_{4}}{\Delta_{3}} \pmod{p}, \quad \lambda^{-1} \equiv \frac{\Delta''_{4}}{\Delta_{3}} \pmod{p}. \] (37)

Substituting (36), (37) in the congruence
\[ \lambda(a + x)(a + y)(a + z) = (a + x)(a + y) + (a + y)(a + z) + (a + z)(a + x) \pmod{p}, \]
we obtain
\[ (\Delta'_{4} + \Delta_{3} x)(\Delta'_{4} + \Delta_{3} y)(\Delta'_{4} + \Delta_{3} z) \equiv \Delta''_{4} \{(\Delta'_{4} + \Delta_{3} x)(\Delta'_{4} + \Delta_{3} y)
\quad + (\Delta'_{4} + \Delta_{3} y)(\Delta'_{4} + \Delta_{3} z) + (\Delta'_{4} + \Delta_{3} z)(\Delta'_{4} + \Delta_{3} x) \} \pmod{p}. \]

Both sides of this congruence are of order \( O(N^{10}) = o(p) \). Hence the congruence becomes an equality
\[ (\Delta'_{4} + \Delta_{3} x)(\Delta'_{4} + \Delta_{3} y)(\Delta'_{4} + \Delta_{3} z) = \Delta''_{4} \{(\Delta'_{4} + \Delta_{3} x)(\Delta'_{4} + \Delta_{3} y)
\quad + (\Delta'_{4} + \Delta_{3} y)(\Delta'_{4} + \Delta_{3} z) + (\Delta'_{4} + \Delta_{3} z)(\Delta'_{4} + \Delta_{3} x) \}, \]
and the desired result follows from Lemma 9. \( \square \)

**Proof of Theorem 3.** Suppose that \( I = \{a+1, \ldots, a+N\} \). The theorem is equivalent to the assertion that for every \( \varepsilon > 0 \) we have
\[ J_{6} \ll N^{3+\varepsilon}, \]
where the constant implied in \( \ll \) may depend only on \( \varepsilon \).

Note that for every \( j \in \mathbb{Z} \) there are \( u_{j}, v_{j} \in \mathbb{Z} \) such that
\[ \frac{u_{j}}{v_{j}} \equiv j \pmod{p}, \quad |u_{j}| \leq p^{\frac{1}{2}}, \quad 0 < |v_{j}| \leq p^{\frac{1}{2}}. \] (38)

Indeed, there are more than \( p \) numbers \( u + jv, \ 0 \leq u, v \leq \lfloor p^{\frac{1}{2}} \rfloor \), whence at least two of them must be congruent modulo \( p \). We also represent \( a \) in a similar form:
\[ a \equiv \frac{a_{0}}{b_{0}} \pmod{p}, \quad |a_{0}| \leq p^{\frac{1}{2}}, \quad 0 < |b_{0}| \leq p^{\frac{1}{2}}. \] (39)

Let \( T_{j} \) be the number of solutions of the congruence
\[ \frac{1}{a + x_{1}} + \frac{1}{a + x_{2}} + \frac{1}{a + x_{3}} \equiv j \pmod{p}, \quad 1 \leq x_{1}, x_{2}, x_{3} \leq N. \]

We have
\[ J_{6} = \sum_{j=0}^{p-1} T_{j}^{2}, \quad \sum_{j=0}^{p-1} T_{j} \leq N^{3}. \]

It follows from Corollary 4 that \( T_{j} < N^{1+o(1)} \). Hence the contribution to \( J_{6} \) of all \( j \in \{I^{-1} \cup 0\} \pmod{p} \) is
\[ \sum_{0 \leq j < p^{-1} \atop j \in I^{-1} \cup 0} T_{j}^{2} \leq (N + 1) \max_{j} T_{j}^{2} < N^{3+o(1)}. \]
Furthermore, the contribution to $J_6$ of all $j$ with $T_j < N^{0.1\varepsilon}$ is less than
\[ N^{0.1\varepsilon} \sum_{j=0}^{p-1} T_j \leq N^{3+0.1\varepsilon}. \]

Thus, if we write $\Omega$ for the set of all integers $j$ with
\[ 1 \leq j \leq p-1, \quad j \notin I^{-1} \pmod{p}, \quad |T_j| > N^{0.1\varepsilon}, \]
then
\[ J_6 < N^{3+0.2\varepsilon} + \sum_{j \in \Omega} T_j^2. \]  \hspace{1cm} (40)

For every $j$ we use Lemma 13 with $J$ replaced by $T_j$ and $\lambda$ replaced by $j$. Then there are numbers $\Delta'_{4j}, \Delta''_{4j}, \Delta_{3j}$ with
\[ \Delta'_{4j} \ll N^4, \quad \Delta''_{4j} \ll N^4, \quad \Delta_{3j} \ll N^3 \]
such that
\[ a \equiv \frac{\Delta'_{4j}}{\Delta_{3j}} \pmod{p}, \quad j^{-1} \equiv \frac{\Delta''_{4j}}{\Delta_{3j}} \pmod{p}. \]

Comparing this with (38) and (39), we have
\[ a \equiv a_0 b_0 \equiv \frac{\Delta'_{4j}}{\Delta_{3j}} \pmod{p}, \quad j^{-1} \equiv \frac{v_j}{u_j} \equiv \frac{\Delta''_{4j}}{\Delta_{3j}} \pmod{p}. \]  \hspace{1cm} (41)

Using the inequalities that hold for $N, a_0, b_0, u_j, v_j$, we see that
\[ \frac{a_0}{b_0} = \frac{\Delta'_{4j}}{\Delta_{3j}}, \quad \frac{v_j}{u_j} = \frac{\Delta''_{4j}}{\Delta_{3j}}. \]  \hspace{1cm} (42)

We now represent the congruence corresponding to $T_j$ in the form
\[
x_1x_2x_3 + (a - j^{-1})(x_1x_2 + x_2x_3 + x_3x_1)
+ (a^2 - 2aj^{-1})(x_1 + x_2 + x_3) + (a^3 - 3a^2j^{-1}) \equiv 0 \pmod{p}.
\]

Using (41), we substitute $a$ and $j^{-1}$ and obtain that
\[
x_1x_2x_3 + \left( \frac{\Delta'_{4j}}{\Delta_{3j}} - \frac{\Delta''_{4j}}{\Delta_{3j}} \right) (x_1x_2 + x_2x_3 + x_3x_1)
+ \left( \left( \frac{\Delta'_{4j}}{\Delta_{3j}} \right)^2 - 2 \frac{\Delta'_{4j}}{\Delta_{3j}} \frac{\Delta''_{4j}}{\Delta_{3j}} \right)(x_1 + x_2 + x_3)
+ \left( \left( \frac{\Delta'_{4j}}{\Delta_{3j}} \right)^3 - 3 \left( \frac{\Delta'_{4j}}{\Delta_{3j}} \right)^2 \frac{\Delta''_{4j}}{\Delta_{3j}} \right) \equiv 0 \pmod{p}.
\]
If we multiply this congruence by \( \Delta_{3j}^3 \), then the left-hand side becomes an integer of order \( O(N^{12}) = o(p) \). Hence the resulting congruence is an equality. Dividing by \( \Delta_{3j}^3 \), we get
\[
x_1x_2x_3 + \left( \frac{\Delta_{3j}'}{\Delta_{3j}} - \frac{\Delta_{3j}''}{\Delta_{3j}} \right) (x_1x_2 + x_2x_3 + x_3x_1)
+ \left( \left( \frac{\Delta_{3j}'}{\Delta_{3j}} \right)^2 - 2 \frac{\Delta_{3j}'}{\Delta_{3j}} \frac{\Delta_{3j}''}{\Delta_{3j}} \right) (x_1 + x_2 + x_3)
+ \left( \left( \frac{\Delta_{3j}'}{\Delta_{3j}} \right)^3 - 3 \left( \frac{\Delta_{3j}'}{\Delta_{3j}} \right)^2 \frac{\Delta_{3j}''}{\Delta_{3j}} \right) = 0.
\]
Using (42), we rewrite this equality in the form
\[
x_1x_2x_3 + \left( \frac{a_0}{b_0} - \frac{v_j}{u_j} \right) (x_1x_2 + x_2x_3 + x_3x_1)
+ \left( \frac{a_0^2}{b_0^2} - 2 \frac{a_0}{b_0} \frac{v_j}{u_j} \right) (x_1 + x_2 + x_3)
+ \left( \frac{a_0^3}{b_0^3} - 3 \frac{a_0^2}{b_0^2} \frac{v_j}{u_j} \right) = 0.
\]
As a result, we get
\[
\frac{1}{(a_0/b_0) + x_1} + \frac{1}{(a_0/b_0) + x_2} + \frac{1}{(a_0/b_0) + x_3} = \frac{u_j}{v_j}.
\] (43)
Thus, for \( j \in \Omega \), the quantity \( T_j \) is equal to the number of solutions of the Diophantine equation (43) in positive integers \( x_1, x_2, x_3 \leq N \). Since the \( u_j/v_j \) are pairwise distinct, we see that \( \sum_{j \in \Omega} T_j^2 \) does not exceed the number of solutions of the equation
\[
\frac{1}{(a_0/b_0) + x_1} + \frac{1}{(a_0/b_0) + x_2} + \frac{1}{(a_0/b_0) + x_3}
= \frac{1}{(a_0/b_0) + x_4} + \frac{1}{(a_0/b_0) + x_5} + \frac{1}{(a_0/b_0) + x_6}
\]
in positive integers \( x_1, \ldots, x_6 \leq N \). Therefore it follows from Lemma 6 that
\[
\sum_{j \in \Omega} T_j^2 < N^{3+o(1)}.
\]
This together with (40) completes the proof of the theorem. \( \square \)

**Proof of Theorem 4.** Suppose that \( I = \{a+1, \ldots, a+N\} \). By a standard argument that uses induction and Hölder’s inequality, it suffices to prove that the contribution of the set of solutions with \( x_1, \ldots, x_{2k} \) pairwise distinct is bounded by \( N^{k+o(1)} \). Therefore in what follows we assume that \( x_1, \ldots, x_{2k} \) are pairwise distinct.

For every solution \( \bar{x} = (x_1, \ldots, x_{2k}) \) we consider the polynomial
\[
P_{\bar{x}}(Z) = \prod_{i \neq 1} (Z + x_i) + \cdots + \prod_{i \neq k} (Z + x_i) - \prod_{i \neq k+1} (Z + x_i) - \cdots - \prod_{i \neq 2k} (Z + x_i).
\]
Clearly, deg $P_\vec{x}(Z) \leq 2k - 2$. Note that $P_\vec{x}(-x_1) \neq 0$. In particular, $P_\vec{x}(Z)$ is not identically equal to zero. Since $P_\vec{x}(a) \equiv 0 \pmod{p}$, it is actually non-constant. Clearly, $P_\vec{x}(Z)$ is of the form

$$P_\vec{x}(Z) = \sum_{i=0}^{2k-2} a_i Z^{2k-2-i},$$

where $|a_i| \ll N^{i+1}$. We fix a solution

$$(x_1, \ldots, x_{2k}) = (c_1, \ldots, c_{2k})$$

and consider the polynomial $P_{\vec{c}}(Z)$ that corresponds to $\vec{c} = (c_1, \ldots, c_{2k})$. Since

$$P_\vec{x}(a) \equiv P_{\vec{c}}(a) \equiv 0 \pmod{p},$$

we have

$$\text{Res}(P_\vec{x}(Z), P_{\vec{c}}(Z)) \equiv 0 \pmod{p}.$$ 

On the other hand, the polynomials $P_\vec{x}(Z)$ and $P_{\vec{c}}(Z)$ satisfy the hypotheses of Lemma 2 with

$$\sigma = \theta = 1, \quad m = n = 2k - 1.$$ 

Hence

$$\text{Res}(P_\vec{x}(Z), P_{\vec{c}}(Z)) \ll N^{4k^2 - 4k}.$$ 

Therefore, assuming that $N < p^{\frac{1}{4k^2}}$, we get

$$|\text{Res}(P_\vec{x}(Z), P_{\vec{c}}(Z))| < p,$$

whence

$$\text{Res}(P_\vec{x}(Z), P_{\vec{c}}(Z)) = 0.$$ 

It follows that for every solution $\vec{x} = (x_1, \ldots, x_{2k})$ the polynomial $P_\vec{x}(Z)$ has a root in common with $P_{\vec{c}}(Z)$. Since the numbers $x_i$ are pairwise distinct, the condition $P_\vec{x}(\sigma) = 0$ implies that $x_i + \sigma \neq 0$. Then Lemma 6 yields that for every fixed root $\sigma$ of $P_\vec{c}(Z)$ the equation $P_\vec{x}(\sigma) = 0$ has at most $N^{k+o(1)}$ solutions in positive integers $x_i \leq N$. □

**Proof of Theorem 5.** It suffices to consider the case when $kN^{k-1} < p$ (otherwise the assertion is trivial). For $\lambda = 0, 1, \ldots, p - 1$ we put

$$J(\lambda) = \{(x_1, \ldots, x_k) \in I^k; \ x_1^* + \cdots + x_k^* \equiv \lambda \pmod{p}\}.$$ 

Let $\Omega = \{\lambda \in [1, p - 1]; \ |J(\lambda)| \geq 1\}$. Since $J(0) = 0$, we have

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

Consider the lattice

$$\Gamma_\lambda = \{(u, v) \in \mathbb{Z}^2; \ \lambda u \equiv v \pmod{p}\}$$

and the body

$$D = \{(u, v) \in \mathbb{R}^2; \ |u| \leq N^k, \ |v| \leq kN^{k-1}\}.$$
Writing $\mu_1, \mu_2$ for the successive minima of $D$ with respect to $\Gamma_\lambda$, we obtain from Corollary 3 that

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

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

$$\lambda x_1 \cdots x_k \equiv x_2 \cdots x_k + \cdots + x_1 \cdots x_{k-1} \pmod{p},$$

whence

$$(x_1 \cdots x_k, x_2 \cdots x_k + \cdots + x_1 \cdots x_{k-1}) \in \Gamma_\lambda \cap D.$$  

Thus we have $\mu_1 \leq 1$ for $\lambda \in \Omega$. Split $\Omega$ into subsets

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

We have

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

(44)

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

$$0 \neq \det \begin{pmatrix} u_1 & v_1 \\ u_2 & v_2 \end{pmatrix} \equiv 0 \pmod{p},$$

whence

$$\left| \det \begin{pmatrix} u_1 & v_1 \\ u_2 & v_2 \end{pmatrix} \right| \geq p.$$

Also,

$$\left| \det \begin{pmatrix} u_1 & v_1 \\ u_2 & v_2 \end{pmatrix} \right| \leq 2k \mu_1 \mu_2 N^{2k-1} \leq \frac{30kN^{2k-1}}{|\Gamma_\lambda \cap D|}.$$  

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

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

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

$$|\Gamma_\lambda \cap D| \leq \frac{30kN^{2k-1}}{p}. $$  

(45)

Writing $S(u, v)$ for the set of $k$-tuples $(x_1, \ldots, x_k)$ of positive integers $x_1, \ldots, x_k \leq N$ with

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

we thus obtain that

$$\sum_{\lambda \in \Omega'} |J(\lambda)|^2 = \sum_{\lambda \in \Omega'} \left( \sum_{(u,v) \in \Gamma_\lambda \cap D} \sum_{(x_1,\ldots,x_k) \in S(u,v)} 1 \right)^2.$$
By using the Cauchy–Schwarz inequality and taking (45) into account, we get
\[ \sum_{\lambda \in \Omega'} |J(\lambda)|^2 \leq \frac{30kN^{2k-1}}{p} \sum_{\lambda \in \Omega'} \sum_{(u,v) \in \Gamma_{\lambda} \cap D} \left( \sum_{(x_1, \ldots, x_k) \in S(u,v)} 1 \right)^2. \]

Clearly, the right-hand side is bounded by the number of solutions of the system of equations
\[
x_1 \cdots x_k = y_1 \cdots y_k, \\
x_1 \cdots x_{k-1} + \cdots + x_2 \cdots x_k = y_2 \cdots y_k + \cdots + y_1 \cdots y_{k-1}
\]
in positive integers \(x_i, y_j \leq N\). Hence it follows from Lemma 4 that
\[ \sum_{\lambda \in \Omega'} |J(\lambda)|^2 < 30k(2k)^{80k^3} N^{3k-1} \frac{N^{3k-1}}{p}. \] (46)

Case 2: \( \lambda \in \Omega'' \), that is, \( \mu_2 > 1 \). Then the vectors in \( \Gamma_{\lambda} \cap D \) are linearly dependent. In particular, there is a \( \hat{\lambda} \in \mathbb{Q} \) such that \( \hat{\lambda}x_1 \cdots x_k = x_2 \cdots x_k + \cdots + x_1 \cdots x_{k-1} \) for \((x_1, \ldots, x_k) \in J(\lambda)\). Thus we have
\[
\sum_{\lambda \in \Omega''} |J(\lambda)|^2 \leq \sum_{\lambda \in \mathbb{Q}} \left| \left\{ (x_1, \ldots, x_k) \in I^k; \frac{1}{x_1} + \cdots + \frac{1}{x_k} = \hat{\lambda} \right\} \right|^2 \\
= \left| \left\{ (x_1, \ldots, x_{2k}) \in [1, N]^{2k}; \frac{1}{x_1} + \cdots + \frac{1}{x_k} = \frac{1}{x_{k+1}} + \cdots + \frac{1}{x_{2k}} \right\} \right| \\
< (2k)^{80k^3} (\log N)^{4k^2} N^k.
\]

Substituting this and (46) in (44), we obtain that
\[ J_{2k} < (2k)^{90k^3} (\log N)^{4k^2} \left( \frac{N^{2k-1}}{p} + 1 \right) N^k. \quad \square \]

The proof of Theorem 6 follows the same lines. The only difference is that we replace Lemma 4 by the bound
\[
\left| \left\{ (x_1, \ldots, x_{2k}) \in ([1, N] \cap \mathcal{P})^{2k}; \frac{1}{x_1} + \cdots + \frac{1}{x_k} = \frac{1}{x_{k+1}} + \cdots + \frac{1}{x_{2k}} \right\} \right| \\
< (2k)^k \left( \frac{N}{\log N} \right)^k.
\]
\[ \square \]

§ 8. Proof of Theorems 7–14

**Proof of Theorem 7.** It suffices to consider the case when \( |I_1| = [p^{1+\varepsilon}], |I_2| = [p^{2+\varepsilon}] \) and \( 0 < \varepsilon < 0.1 \). Let
\[ W_2 = \sum_{x_1 \in I_1} \sum_{x_2 \in I_2} \alpha_1(x_1)\alpha_2(x_2)e_p(ax_1^*x_2^*). \]
We take \( k = \lceil 1/\varepsilon \rceil \) and use Hölder’s inequality:

\[
|W_2|^k \leq |I_1|^{k-1} \sum_{x_1 \in I_1} \left| \sum_{x_2 \in I_2} \alpha_2(x_2) e_p(ax_1^*x_2^*) \right|^k
\]

\[
= |I_1|^{k-1} \sum_{x_1 \in I_1} \left| \sum_{y_1, \ldots, y_k \in I_2} \alpha_2(y_1) \cdots \alpha_2(y_k) e_p(ax_1^*(y_1^* + \cdots + y_k^*)) \right|
\]

\[
= |I_1|^{k-1} \sum_{x_1 \in I_1} \theta(x_1) \left( \sum_{y_1, \ldots, y_k \in I_2} \alpha_2(y_1) \cdots \alpha_2(y_k) e_p(ax_1^*(y_1^* + \cdots + y_k^*)) \right)
\]

\[
\leq |I_1|^{k-1} \sum_{x_1 \in I_1} \left| \sum_{x_1 \in I_1} \theta(x_1) e_p(ax_1^*(y_1^* + \cdots + y_k^*)) \right|,
\]

where the \( \theta(x) \) are complex numbers with \( |\theta(x)| \leq 1 \). Again using Hölder’s inequality, we obtain that

\[
|W_2|^{3k} \leq |I_1|^{3k-3} |I_2|^{2k} \sum_{y_1, \ldots, y_k \in I_2} \left| \sum_{x_1 \in I_1} \theta(x_1) e_p(ax_1^*(y_1^* + \cdots + y_k^*)) \right|^3
\]

\[
= |I_1|^{3k-3} |I_2|^{2k} \sum_{\lambda=0}^{p-1} T(\lambda) \left| \sum_{x_1 \in I_1} \theta(x_1) e_p(ax_1^*\lambda) \right|^3,
\]

where \( T(\lambda) \) is the number of solutions of the congruence

\[
y_1^* + \cdots + y_k^* \equiv \lambda \pmod{p}, \quad y_i \in I_2.
\]

We now apply the Cauchy–Schwarz inequality and get

\[
|W_2|^{6k} \leq |I_1|^{6k-6} |I_2|^{4k} \left( \sum_{\lambda=0}^{p-1} T^2(\lambda) \right) \sum_{\lambda=0}^{p-1} \left| \sum_{x_1 \in I_1} \theta(x_1) e_p(ax_1^*\lambda) \right|^6.
\]

By Theorem 1 we have

\[
\sum_{\lambda=0}^{p-1} T^2(\lambda) < |I_2|^{2k-2+\varepsilon+o(1)} < |I_2|^{2k-2+\varepsilon}.
\]

Furthermore,

\[
\sum_{\lambda=0}^{p-1} \sum_{x_1 \in I_1} \theta(x_1) e_p(ax_1^*\lambda)^6 \leq p J_6,
\]

where \( J_6 \) is the number of solutions of the congruence

\[
y_1^* + y_2^* + y_3^* \equiv y_4^* + y_5^* + y_6^* \pmod{p}, \quad y_i \in I_1.
\]

By Theorem 3 we have \( J_6 = |I_1|^{3+o(1)} \). Thus,

\[
|W_2|^{6k} \leq p |I_1|^{6k-3+o(1)} |I_2|^{6k-2+\varepsilon}.
\]

Since \( p \ll |I_1|^3 |I_2|^2 p^{-2\varepsilon} \), this proves the theorem. \( \Box \)
Proof of Theorem 8. Let
\[ S = \sum_{x_1 \in I_1} \sum_{x_2 \in I_2} \alpha_1(x_1) \alpha_2(x_2)e_p(ax_1^* x_2^*). \]
Then, by Hölder’s inequality,
\[ |S|^{k_2} \leq N_1^{k_2 - 1} \sum_{x_1 \in I_1} \left| \sum_{x_2 \in I_2} \alpha_2(x_2)e_p(ax_1^* x_2^*) \right|^{k_2}. \]
Thus for some \( \sigma(x_1) \in \mathbb{C} \) with \( |\sigma(x_1)| = 1 \) we have
\[ |S|^{k_2} \leq N_1^{k_2 - 1} \sum_{y_1 \ldots y_{k_2} \in I_2} \left| \sum_{x_1 \in I_1} \sigma(x_1)e_p(ax_1^* (y_1^* + \cdots + y_{k_2}^*)) \right|^{k_2}. \]
Again by Hölder’s inequality,
\[ |S|^{k_1 k_2} \leq N_1^{k_1 k_2 - k_1} N_2^{k_1 k_2 - k_2} \sum_{\lambda = 0}^{p-1} J_{k_2}(\lambda; N_2) \left| \sum_{x_1 \in I_1} \sigma(x_1)e_p(ax_1^* \lambda) \right|^{k_1}, \]
where \( J_k(\lambda; N) \) is the number of solutions of the congruence
\[ x_1^* + \cdots + x_k^* \equiv \lambda \pmod{p}, \quad x_i \in [1, N]. \]
Then, applying the Cauchy–Schwarz inequality and using
\[ \sum_{\lambda = 0}^{p-1} J_{k_2}(\lambda; N_2)^2 = J_{2k_2}(N_2), \quad \sum_{\lambda = 0}^{p-1} \left| \sum_{x_1 \in I_1} \sigma(x_1)e_p(ax_1^*)^{2k_1} \right| \leq pJ_{2k_1}(N_1), \]
we get
\[ |S|^{2k_1 k_2} \leq pN_1^{2k_1 k_2 - 2k_1} N_2^{2k_1 k_2 - 2k_2} J_{2k_1}(N_1) J_{2k_2}(N_2). \] (47)
Here \( J_{2k}(N) \) stands for the number of solutions of the congruence
\[ x_1^{-1} + \cdots + x_k^{-1} \equiv x_{k+1}^{-1} + \cdots + x_{2k}^{-1} \pmod{p}, \quad x_i \in [1, N]. \]
Theorem 5 yields that
\[ |S|^{2k_1 k_2} \leq (2k_1)^{90k_1^3} (2k_2)^{90k_2^3} (\log N_1)^{4k_1^2} (\log N_2)^{4k_2^2} \]
\[ \times N_1^{2k_1 k_2} N_2^{2k_1 k_2} \left( \frac{N_1^{k_1 - 1}}{p^{\frac{1}{2}}} + \frac{p^{\frac{1}{2}}}{N_1^{k_1}} \right) \left( \frac{N_2^{k_2 - 1}}{p^{\frac{1}{2}}} + \frac{p^{\frac{1}{2}}}{N_2^{k_2}} \right). \]
Thus,
\[ |S| < (2k_1)^{45k_1^2} (2k_2)^{45k_2^2} (\log p)^{2(k_1 + k_2)} \]
\[ \times \left( \frac{N_1^{k_1 - 1}}{p^{\frac{1}{2}}} + \frac{p^{\frac{1}{2}}}{N_1^{k_1}} \right)^{\frac{1}{2}} \left( \frac{N_2^{k_2 - 1}}{p^{\frac{1}{2}}} + \frac{p^{\frac{1}{2}}}{N_2^{k_2}} \right)^{\frac{1}{2}} N_1 N_2. \]
Proof of Theorem 9. Note that if \(1 \leq N < p\), then Corollary 4 yields that the number of solutions of the congruence

\[
\frac{1}{x_1} + \frac{1}{x_2} \equiv \frac{1}{x_3} + \frac{1}{x_4} \pmod{p}, \quad L + 1 \leq x_1, x_2, x_3, x_4 \leq L + N,
\]

is bounded by \(N^{2+\alpha(1)}(N^{\frac{3}{2}}p^{-\frac{1}{2}} + 1)\). Following the proof of Theorem 8 for \(k_1 = k_2 = 2\) and using this bound for \([L + 1, L + N] = I_i\), we derive the theorem. □

Proof of Theorem 10. We use (47), where \(J_{2k}(N_i)\) is the number of solutions of the congruence

\[
x_1^{-1} + \cdots + x_k^{-1} \equiv x_{k+1}^{-1} + \cdots + x_{2k}^{-1} \pmod{p}, \quad (x_1, \ldots, x_{2k}) \in I_i^{2k}.
\]

Since

\[
N_1 < p^{\frac{k_1+1}{2k_1}}, \quad N_2 < p^{\frac{k_2+1}{2k_2}},
\]

we see from Theorem 1 that

\[
J_{2k_1}(N_1) < N_1^{\frac{2k_1^2}{2k_1+1}}, \quad J_{2k_2}(N_2) < N_2^{\frac{2k_2^2}{2k_2+1}}.
\]

Combining this with (47), we get the desired result. □

Proof of Theorem 11. We can assume that \(0 < \varepsilon < 0.01\) and \(N^n \sim p^{\frac{1}{2}+\varepsilon}\). Put

\[
W_n = \left| \sum_{x_1 \in I_1} \cdots \sum_{x_n \in I_n} \alpha_1(x_1) \cdots \alpha_n(x_n)e_p(ax_1^* \cdots x_n^*) \right|.
\]

Applying Hölder’s inequality \(n\) times and using the estimate

\[
\sum_u \left| \sum_v \alpha(v)e_p(auv) \right|^6 \leq \sum_{v_1, \ldots, v_6} \left| \sum_u e_p(a(v_1 + v_2 + v_3 - v_4 - v_5 - v_6)u) \right|,
\]

which holds for \(|\alpha(v)| \leq 1\), we obtain that

\[
W_n^{6^n} \leq N^{n6^n - 6n} \times \sum_{x_{11}, \ldots, x_{16} \in I_1} \cdots \sum_{x_{n1}, \ldots, x_{n6} \in I_n} e_p(a(x_{11}^* + \cdots - x_{16}^*) \cdots (x_{n1}^* + \cdots - x_{n6}^*)).
\]

We can fix \(x_{j4}, x_{j5}, x_{j6}\) in such a way that for some integers \(c_j\) we have

\[
W_n^{6^n} \leq N^{n6^n - 3n} \left| \sum_{x_{11}, x_{12}, x_{13} \in I_1} \cdots \sum_{x_{n1}, x_{n2}, x_{n3} \in I_n} \{ \cdots \} \right|,
\]

where \(\{ \cdots \}\) stands for the expression

\[
e_p(a(x_{11}^* + x_{12}^* + x_{13}^* - c_1) \cdots (x_{n1}^* + x_{n2}^* + x_{n3}^* - c_n)).
\]

Let \(T_j(\lambda), j = 1, \ldots, n\), be the number of solutions of the congruence

\[
x_1^* + x_2^* + x_3^* - c_j \equiv \lambda \pmod{p}, \quad x_1, x_2, x_3 \in I_j.
\]
Then we see that
\[ W_n^6 \leq N^{n^6 - 3n} \left| \sum_{\lambda_1=0}^{p-1} \cdots \sum_{\lambda_n=0}^{p-1} T_1(\lambda_1) \cdots T_n(\lambda_n) e_p(a\lambda_1 \cdots \lambda_n) \right|. \tag{48} \]

Observe that \( \sum_{\lambda=0}^{p-1} T_j(\lambda) \leq 1 \). By Theorem 3 we also have
\[ \sum_{\lambda} \left( \frac{T_j(\lambda)}{N^3} \right)^2 < N^{-3 + o(1)}. \]
Furthermore,
\[ \prod_{j=1}^{n} \left( \sum_{\lambda} \left( \frac{T_j(\lambda)}{N^3} \right)^2 \right)^{\frac{1}{2}} < N^{-\frac{3n}{2} + o(1)} < p^{-\frac{1}{2} - \delta} \]
for some \( \delta = \delta(\varepsilon, n) > 0 \). Thus we can use Lemma 1 with \( \gamma_j(x) = \frac{T_j(x)}{N^3} \). It follows that
\[ \left| \sum_{\lambda_1=0}^{p-1} \cdots \sum_{\lambda_n=0}^{p-1} T_1(\lambda_1) \cdots T_n(\lambda_n) e_p(a\lambda_1 \cdots \lambda_n) \right| < N^{3n} p^{-\delta}. \]
Substituting this into (48), we get the desired result. \( \square \)

**Proof of Theorem 12.** Take \( C = 9c^{-2} \), where \( c \leq \frac{1}{4} \) is the constant in Theorem 4. In particular, we can assume that \( n > 3c^{-1} \). Clearly, we can also assume that \( N = [p^\frac{9}{cn^2}] \). For \( k = [\frac{cn}{3}] \) we have
\[ p^\varepsilon \geq p^\frac{9}{cn^2} \geq N. \]
Thus, for every \( j \), the number of solutions of the congruence
\[ y_1^* + \cdots + y_k^* \equiv y_{k+1}^* + \cdots + y_{2k}^* \pmod{p}, \quad y_1, \ldots, y_{2k} \in I_j, \]
is bounded by \( N^{k+o(1)} \). Letting
\[ W_n = \left| \sum_{x_1 \in I_1} \cdots \sum_{x_n \in I_n} \alpha_1(x_1) \cdots \alpha_n(x_n) e_p(a x_1^* \cdots x_n^*) \right|, \]
we have
\[ W_n^{(2k)n} \leq N^{n(2k)^n - 2kn} \sum_{x_{11} \cdots x_{(2k)i} \in I_1} \cdots \sum_{x_{1n} \cdots x_{(2k)n} \in I_n} e_p(a\{\cdots\}), \]
where \( \{\cdots\} \) stands for the expression
\[ \prod_{j=1}^{n} (x_{1j}^* + \cdots + x_{kj}^* - x_{(k+1)j}^* - \cdots - x_{(2k)j}^*). \]
We can fix \( x_{(k+i)j} \) for all \( i = 1, \ldots, k \) and \( j = 1, \ldots, n \) in such a way that for some integers \( c_1, \ldots, c_n \) we have
\[ W_n^{(2k)n} \leq N^{n(2k)^n - kn} \left| \sum_{x_1 \cdots x_k \in I_1} \cdots \sum_{x_1 \cdots x_k \in I_n} e_p(a\{\cdots\}) \right|. \]
where \{\cdots\} stands for the expression
\[
(x_1^* + \cdots + x_{k_1}^* - c_1) \cdots (x_{1n}^* + \cdots + x_{kn}^* - c_n).
\]
Thus,
\[
W_n^{(2k)^n} \leq N^{n(2k)^n-kn}\left|\sum_{\lambda_1=0}^{p-1} \cdots \sum_{\lambda_n=0}^{p-1} T_1(\lambda_1) \cdots T_n(\lambda_n)e_p(a\lambda_1 \cdots \lambda_n)\right|,
\]  
(49)

where \(T_j(\lambda_j)\) is the number of solutions of the congruence
\[
y_1^* + \cdots + y_k^* - c_j \equiv \lambda_j \pmod{p}, \quad (y_1, \ldots, y_k) \in I_j.
\]
We have
\[
\sum_{\lambda_j=0}^{p-1} \frac{T_j(\lambda_j)}{N^k} \leq 1.
\]
Furthermore, by Theorem 4,
\[
\sum_{\lambda_j=0}^{p-1} \left(\frac{T_j(\lambda_j)}{N^k}\right)^2 < \frac{N^{k+o(1)}}{N^{2k}} < N^{-k+o(1)} < p^{-\delta}
\]
and
\[
\prod_{j=1}^{n} \left(\sum_{\lambda_j=0}^{p-1} \left(\frac{T_j(\lambda_j)}{N^k}\right)^2\right)^{\frac{1}{2}} < N^{-\frac{kn}{2}}p^{o(1)} < p^{-\frac{1}{2}-\delta}
\]
for some \(\delta = \delta(\varepsilon, n) > 0\). Here we take into account that \(N = \lfloor p^{\frac{9}{10\varepsilon^2}} \rfloor, N^{\frac{k\varepsilon}{2}} > N^{\frac{cn^2}{12}} \gg p^{\frac{3}{4}}\). Hence Lemma 1 is applicable. It yields that
\[
\sum_{\lambda_1=0}^{p-1} \cdots \sum_{\lambda_n=0}^{p-1} T_1(\lambda_1) \cdots T_n(\lambda_n)e_p(a\lambda_1 \cdots \lambda_n) < N^{kn}p^{-\delta'}
\]
for some \(\delta' = \delta'(\varepsilon, n) > 0\). Combining this with (49), we get the desired result. □

Proof of Theorem 13. Put \(N_j = |I_j|\). By removing the intervals \(I_j\) with \(N_j \leq p^{\frac{v}{2\varepsilon}}\) (if necessary), we reduce the problem to the case when \(N_j > p^{\frac{v}{2\varepsilon}}\) for all \(j\) and \(N_1 \cdots N_n \geq p^{\frac{1}{2}+\varepsilon}\). Note also that if \(N_j \geq p^{\frac{1}{2}+\frac{v}{10\varepsilon}}\) for some \(j\), then the desired result follows from Weil’s bound for incomplete Kloosterman sums. Thus we can also assume that \(N_j < p^{\frac{1}{2}+\frac{v}{10\varepsilon}}\) for all \(j\). Then we can divide the intervals \(I_j\) with \(N_j > p^{\frac{1}{2}}\) into subintervals of size \(\approx p^{\frac{1}{2}}\), which enables us to assume that \(p^{\frac{v}{10\varepsilon}} < N_j < p^{\frac{1}{2}}\) for all \(j\). Further dividing some of the intervals into subintervals, we can reduce the problem to the case when
\[
p^{\frac{1}{2}+\varepsilon} < N_1 \cdots N_n < 2p^{\frac{1}{2}+\varepsilon},
\]
\[
p^{\frac{v}{10\varepsilon}} < N_j < p^{\frac{1}{2}}, \quad j = 1, 2, \ldots, n.
\]
We write \( \alpha_j(x_j) = e_p(a_j x_j) \) and put
\[
W_n = \left| \sum_{x_1 \in I_1} \cdots \sum_{x_n \in I_n} \alpha_1(x_1) \cdots \alpha_n(x_n) e_p(a x_1^* \cdots x_n^*) \right|.
\]

By taking \( k = \lfloor \frac{2}{\varepsilon} \rfloor \) and applying Hölder’s inequality \( n \) times, we get
\[
W_n^{(2k)^n} \leq (N_1 \cdots N_n)^{(2k)^n - 2k} \sum_{\lambda_1 = 0}^{p-1} \cdots \sum_{\lambda_n = 0}^{p-1} T_1(\lambda_1) \cdots T_n(\lambda_n) e_p(a \lambda_1 \cdots \lambda_n), \quad (50)
\]
where \( T_j(\lambda_j) \) is the number of solutions of the congruence
\[
(y_1^* + \cdots + y_k^*) - (y_{k+1}^* + \cdots + y_{2k}^*) \equiv \lambda_j \pmod{p}, \quad (y_1, \ldots, y_{2k}) \in I_j^{2k}.
\]

Observe that
\[
\sum_{\lambda_j = 0}^{p-1} \frac{T_j(\lambda_j)}{N_j^{2k}} \leq 1.
\]

Furthermore, by Theorem 1,
\[
\sum_{\lambda_j = 0}^{p-1} \left( \frac{T_j(\lambda_j)}{N_j^{2k}} \right)^2 \frac{N_j^{4k-2+\frac{1}{2k+1}+o(1)}}{N_j^{4k}} \leq N_j^{-2+\frac{2}{2k+1}+o(1)} < p^{-\delta}
\]
and
\[
\prod_{j=1}^{n} \left( \sum_{\lambda_j = 0}^{p-1} \left( \frac{T_j(\lambda_j)}{N_j^{2k}} \right)^2 \right)^{\frac{1}{2}} \leq (N_1 \cdots N_n)^{-1} p^{0.5\varepsilon} < p^{-\frac{1}{2}-\delta}
\]
for some \( \delta = \delta(\varepsilon, n) > 0 \). Thus Lemma 1 is applicable and yields that
\[
\sum_{\lambda_1 = 0}^{p-1} \cdots \sum_{\lambda_n = 0}^{p-1} T_1(\lambda_1) \cdots T_n(\lambda_n) e_p(a \lambda_1 \cdots \lambda_n) < (N_1 \cdots N_n)^{2k} p^{-\delta'},
\]
where \( \delta' = \delta(\varepsilon, n) > 0 \). Combining this with (50), we get the desired result. \( \square \)

Proof of Theorem 14. We shall use the following corollary of Theorem 7 in [31]. Let \( \mu, \nu \) be positive probability measures on \( \mathbb{R} \) supported on \([-1,1]\), and let \( \alpha, \beta \) be complex-valued functions on \( \mathbb{R} \), \( |\alpha|, |\beta| \leq 1 \). Suppose that \( \xi \in \mathbb{R}, |\xi| > 1 \). Then
\[
\left| \int \int \alpha(x) \beta(y) e^{ixy} \mu(dx) \nu(dy) \right| \ll |\xi|^{-\frac{1}{2}} \| \mu \ast \varphi_\delta \|_2 \| \nu \ast \varphi_\delta \|_2, \quad (51)
\]
where \( \delta = (100|\xi|)^{-1} \) and
\[
\varphi_\delta(t) = \begin{cases} 
\delta^{-1} & \text{if } t \in [-\delta, \delta], \\
0 & \text{otherwise}.
\end{cases}
\]

Note that (51) is a simple fact. There are also multilinear versions in [31], but we do not need them here.
We give a direct proof of (51). For brevity put \( \varphi = \varphi_\delta \). Since

\[
\hat{\varphi}(\lambda) = \frac{2}{\delta \lambda} \sin \frac{\delta \lambda}{2},
\]

the following inequalities hold for \( |\lambda| < (10\delta)^{-1} = 10\xi \) and \( |y| \leq 1 \):

\[
\frac{1}{2} < \hat{\varphi}(\lambda) \leq 1, \quad \left| \frac{\beta(y)}{\hat{\varphi}(\xi y)} \right| \leq 2.
\]

For \( x, y \in [-1, 1] \) we write

\[
e^{i\xi xy} = \frac{1}{\hat{\varphi}(\xi y)} \int \varphi(s - x) e^{i\xi sy} \, ds.
\]

Then

\[
\left| \int \int \alpha(x) \beta(y) e^{i\xi y \xi} \mu(dx) \nu(dy) \right| \leq \int \int \left| \frac{\beta(y)}{\hat{\varphi}(\xi y)} e^{i\xi sy} \nu(dy) \right| \varphi(s - x) \mu(dx) \, ds
\]

\[
= \int |\hat{\nu}(\xi s)|(\mu * \varphi)(s) \, ds,
\]

(52)

where

\[
\frac{d\nu_1}{d\nu} = \frac{\beta(y)}{\hat{\varphi}(\xi y)}.
\]

Note that \( |\nu_1| \leq 2\nu \). Since \( \text{supp}(\mu * \varphi) \subset [-2, 2] \), it follows from (52) that

\[
\left| \int \int \alpha(x) \beta(y) e^{i\xi y \xi} \mu(dx) \nu(dy) \right| \leq \|\mu * \varphi\|_2 \|\hat{\nu}(\xi \cdot)\|_{L^2[-2,2]}.
\]

Furthermore, for \( |s| \leq 2 \) we have

\[
|\hat{\nu}_1(\xi s)| \leq 2|\hat{\nu}_1(\xi s)\hat{\varphi}(\xi s)| = 2| (\nu_1 * \varphi)(\xi s) |.
\]

Hence,

\[
\|\hat{\nu}_1(\xi \cdot)\|_{L^2[-2,2]} \leq 2|\xi|^{-\frac{1}{2}} \| (\nu_1 * \varphi) \|_2 = 2|\xi|^{-\frac{1}{2}} (2\pi)^{\frac{1}{2}} \|\nu_1 * \varphi\|_2
\]

\[
\leq 4(2\pi)^{\frac{1}{2}} |\xi|^{-\frac{1}{2}} \|\nu * \varphi\|_2,
\]

and (51) follows.

We write \( e(z) = e^{iz} \) and put

\[
S = \sum_{n_1 \sim N_1}^{n_{k_1}} \sum_{n_2 \sim N_2}^{n_{k_2}} \alpha_1(n_1) \alpha_2(n_2) e \left( \frac{1}{n_1} \frac{1}{n_2} \xi \right).
\]

By using Hölder’s inequality, we easily see that

\[
|S|^{k_1 k_2} \leq N_1^{k_1 k_2 - k_1} N_2^{k_1 k_2 - k_2}
\]

\[
\times \sum_{n_1, \ldots, n_{k_1} \sim N_1}^{n_{k_1}} \sum_{n_{k_1+1}, \ldots, n_{k_2} \sim N_2}^{n_{k_2}} \alpha_1 \beta_{k_2} e \left( \xi \left( \frac{1}{n_{k_1}} + \cdots + \frac{1}{n_{k_1}} \right) \left( \frac{1}{n_{k_2}} + \cdots + \frac{1}{n_{k_2}} \right) \right),
\]

\[
\leq 4(2\pi)^{\frac{1}{2}} |\xi|^{-\frac{1}{2}} \|\nu * \varphi\|_2.
\]
where \( \mathbf{n} = (n_{i1}, \ldots, n_{ik_i}) \) and the coefficients \( \alpha_{\mathbf{n}} \) and \( \beta_{\mathbf{n}} \) are complex numbers depending only on the sums
\[
\frac{1}{n_{11}} + \cdots + \frac{1}{n_{1k_1}}, \quad \frac{1}{n_{21}} + \cdots + \frac{1}{n_{2k_2}},
\]
respectively. Moreover, \( |\alpha_{\mathbf{n}}| = |\beta_{\mathbf{n}}| = 1 \). Thus there are complex numbers \( \alpha(x) \) and \( \beta(y) \) with \( |\alpha(x)| = |\beta(y)| = 1 \) such that
\[
|S|^{k_1 k_2} \leq (N_1 N_2)^{k_1 k_2} \left| \int \int \alpha(x) \beta(y) e \left( \frac{\xi}{N_1 N_2} xy \right) \mu(dx) \nu(dy) \right|,
\]
where \( \mu \) is the normalized measure of the image in \( \mathbb{R} \) of the map
\[
\{ n_i \sim N_1 \}^{k_1} \to \mathbb{R}: (n_{11}, \ldots, n_{1k_1}) \to N_1 \left( \frac{1}{n_{11}} + \cdots + \frac{1}{n_{1k_1}} \right)
\]
and \( \nu \) is defined in a similar way.

Put \( \delta = \frac{N_1 N_2}{100 |\xi|} \). It follows from (51) that
\[
|S|^{k_1 k_2} \leq (N_1 N_2)^{k_1 k_2} \delta^{\frac{1}{2}} \| \mu * \varphi_\delta \|_2 \| \nu * \varphi_\delta \|_2. \tag{53}
\]
We now estimate \( \| \mu * \varphi_\delta \|_2 \). Note that if \( \{ I_j \}_j \) is a partition of \( \mathbb{R} \) into \( \delta \)-intervals, then
\[
\sum_j \left| (n_1, \ldots, n_k); n_i \sim N, \frac{N}{n_1} + \cdots + \frac{N}{n_k} \in I_j \right|
\leq \left| (n_1, \ldots, n_{2k}); n_i \sim N, \left| \frac{1}{n_1} + \cdots + \frac{1}{n_k} - \frac{1}{n_{k+1}} - \cdots - \frac{1}{n_{2k}} \right| < \frac{\delta}{N} \right|.
\]
Therefore we have
\[
\| \mu * \varphi_\delta \|_2^2 \sim N_1^{-2k_1} \delta^{-1} T(N_1), \tag{54}
\]
where
\[
T(N) = \left| (n_1, \ldots, n_{2k}); n_i \sim N, \left| \frac{1}{n_1} + \cdots + \frac{1}{n_k} - \frac{1}{n_{k+1}} - \cdots - \frac{1}{n_{2k}} \right| < \frac{\delta}{N} \right|.
\]
We claim that
\[
T(N) < c(k)(\log N)^{4k^2} N^k (1 + \delta N^{2k-1}).
\]
Indeed, for \( \lambda \in \mathbb{Q} \) let \( J(\lambda) \) be the number of representations of \( \lambda \) in the form
\[
\lambda = \frac{1}{n_1} + \cdots + \frac{1}{n_k}, \quad n_i \sim N. \tag{55}
\]
By Lemma 4,
\[
\sum_\lambda J^2(\lambda) \leq c(k) N^k (\log N)^{4k^2}.
\]
Note that the distance between different $\lambda$ is of order at least $N^{-2k}$. Hence an interval $I \subset \mathbb{R}$ of length $\delta/N$ can contain at most $O(1 + N^{2k-1}\delta)$ numbers of the form (55). Therefore,
\[ T(N) \ll \sum_{n_1, \ldots, n_k \sim N} J\left(\frac{1}{n_1} + \cdots + \frac{1}{n_k}\right)(1 + N^{2k-1}\delta) \]
\[ \ll (1 + N^{2k-1}\delta) \sum_{\lambda} J^2(\lambda) < c(k)N^k(\log N)^{4k^2}(1 + N^{2k-1}\delta). \]
This yields the required bound for $T(N)$.
Thus we obtain from (54) that
\[ \|\mu \ast \varphi_\delta\|_2 \leq c(k_1)(\log N_1)^{2k_1}\delta^{-\frac{1}{2}}N_1^{-\frac{k_1}{2}}(1 + \delta N_1^{2k_1-1})^{\frac{1}{2}}. \]
Similarly,
\[ \|\nu \ast \varphi_\delta\|_2 \leq c(k_2)(\log N_2)^{2k_2}\delta^{-\frac{1}{2}}N_2^{-\frac{k_2}{2}}(1 + \delta N_2^{2k_2-1})^{\frac{1}{2}}. \]
Substituting these bounds into (53), we have
\[ |S|^{k_1 k_2} \leq c(k_1)c(k_2)(\log N_1)^{2k_1}(\log N_2)^{2k_2}(N_1 N_2)^{k_1 k_2} \]
\[ \times (\delta^{-\frac{1}{2}}N_1^{-k_1} + \delta^{\frac{1}{2}}N_2^{k_1-1})(\delta^{-\frac{1}{2}}N_2^{-k_2} + \delta^{\frac{1}{2}}N_2^{k_2-1})^{\frac{1}{2}}. \]
Since $\delta = \frac{N_1 N_2}{100|\xi|}$, this completes the proof.  

\section{Some applications}

In this section we use Theorem 14 to prove Theorem 15 on $\pi(x) - \pi(x - y)$. We also use bounds for trilinear exponential sums to prove Theorem 16 on linear Kloosterman sums and Theorem 17 on the Brun–Titchmarsh theorem.

\textbf{Proof of Theorem 15.} If $y \geq x^{\frac{7}{12}+}$, then the assertion follows from a result of Huxley [32]. Therefore we can assume that $x^\theta \leq y < x^{\frac{7}{12}+}$. Since the function
\[ f(\nu) = \frac{2(1 - \nu)}{12(\nu^{-1} + 1)(\nu^{-1} + 0.5) + 1 - \nu} \]
is increasing for $\nu \in (0, \frac{7}{12}+]$, it suffices to consider the case when $y = x^\theta$, where $\theta \in (0, \frac{7}{12}+)$. Using an argument in [14], p. 269, and the estimate (13.56) in [14], we see that $R(M, N)$ is bounded above by a quantity of the form
\[ \frac{Hy}{MN} \left| \sum_{m \sim M} \alpha_m \beta_n e\left(\frac{hu}{mn}\right) \right|, \]
where $u \sim x$ and $1 \leq h \leq H = MNy^{-1}x^\varepsilon$. Here $M$, $N$ can be chosen arbitrarily provided that $MN = D > y$ (see [14], Theorem 12.21), and we must guarantee that $R(M, N) < yx^{-\varepsilon}$. We can then obtain an upper bound
\[ \pi(x) - \pi(x - y) < \frac{2y}{\log D}. \]
Thus we have
\[
\frac{Hy}{MN} \sum_{m \sim M \atop n \sim N} \alpha_m \beta_n e \left( \frac{hu}{mn} \right) \leq x^\varepsilon \left| \sum_{m \sim M \atop n \sim N} \alpha_m \beta_n e \left( \frac{\xi}{mn} \right) \right|,
\]
where
\[D < x \leq \xi < \frac{D}{y} x^{1+\varepsilon}.
\]

Take an integer \( k \) such that \( k - \frac{1}{2} < \frac{1}{\theta} < k + \frac{1}{2} \), and define \( M \) by the formula
\[
\frac{x}{D} = M^{2k-1}.
\]

Put \( N = D/M \) and choose an integer \( l \) such that
\[N^{2(l-1)} \leq \frac{\xi}{D} < N^{2l}.
\]

Then
\[
\log N = \log D - \frac{\log \left( \frac{x}{D} \right)}{2k-1} \geq \log y - \frac{\log \frac{\xi}{y}}{2k-1} = \left( \theta - \frac{1}{2k-1} \right) \log x > \frac{\theta}{2} \log x,
\]
and \( l \leq \theta^{-1} + 1 \). The estimation of (56) using Theorem 14 yields that
\[
x^\varepsilon D \left( \frac{\xi}{D} M^{-2k} + \frac{D}{\xi} M^{2(k-1)} \right)^{\frac{1}{4k-1}} \leq x^\varepsilon D \left( \frac{D}{y} \frac{x}{M-1} + 1 \right)^{\frac{1}{4k-1}} < x^{2\varepsilon} \left( \frac{D}{y} \right)^{\frac{5}{4}} \left( \frac{x}{D} \right)^{-\frac{1}{4k(2k-1)}} y < x^{2\varepsilon} \left( \frac{D}{y} \right)^{\frac{3}{2}} x^{-\frac{(1-\theta)\theta}{8(\theta-1+1)(\theta-1+0.5)}} y.
\]
Hence we can take
\[D = y^{1+\frac{1-\theta}{12(\theta-1+1)(\theta-1+0.5)}} - \varepsilon'. \quad \square
\]

**Proof of Theorem 16.** Put \( \varepsilon = \frac{\log N}{\log p} \). By Weil’s bound for incomplete Kloosterman sums, we may assume that \( \varepsilon < \frac{4}{7} \). Let
\[
\mathcal{G} = \{ x < N : p_1 \geq N^\alpha, p_3 \geq N^\beta, p_1 p_2 p_3 < N^{1-\beta} \},
\]
where \( p_1 \geq p_2 \geq p_3 \) are the largest prime divisors of \( x \), and \( \alpha, \beta \) are parameters to be specified below. For the moment we assume that
\[0.1 > \alpha > \beta > \frac{1}{\log N}.
\]
We also introduce parameters \( \beta, \beta_1 \) with \( 0.1 > \beta_1 > \beta \). Note that
\[
\sum_{x < N \atop p_1 p_2 > N^{1-\beta_1}} 1 \leq \sum_{y < N^{\beta_1}} \sum_{p_1, p_2 \leq N/y} 1 \leq \sum_{y < N^{\beta_1}} \sum_{p_2 y \log N} \frac{3N}{p_2 y \log N} \leq 4\beta_1 (\log \log N) N.
\]
Similarly,
\[
\sum_{x < N, \ p_1 p_2 p_3 \geq N^{1-\beta}} 1 < \sum_{y \leq N^\beta, \ p_2 p_3 < N} \frac{4N}{y p_2 p_3 \log N} < 5\beta (\log \log N)^2 N.
\]

We also note that the number of positive integers that do not exceed \(N\) and are products of at most two primes is less than
\[
\frac{2N \log \log N}{\log N} < 2\beta N \log \log N.
\]
Hence,
\[
N - |G| \leq \frac{2N \log \log N}{\log N} \\
+ \sum_{x < N, \ p_1 < N^{\alpha}} 1 + \sum_{x < N, \ p_1 p_2 \leq N^{1-\beta_1}} 1 + \sum_{x < N, \ p_1 p_2 p_3 < N^{1-\beta}} 1
\]
\[
\leq \frac{2N \log \log N}{\log N} + \Psi(N, N^\alpha) + 4\beta_1 N \log \log N \\
+ \sum_{p_1 p_2 \leq N^{1-\beta_1}} \Psi \left( \frac{N}{p_1 p_2}, N^\beta \right) + 5\beta N (\log \log N)^2.
\]
Here, as usual, \(\Psi(x, y)\) stands for the number of positive integers not exceeding \(x\) and having no prime divisors greater than \(y\). By a classical result of de Bruijn [33], if \(y > (\log x)^{1+\delta}\), where \(\delta > 0\) is a fixed constant, then
\[
\Psi(x, y) \leq x u^{-(1+o(1))} \quad \text{as} \quad u = \frac{\log x}{\log y} \to \infty.
\]
Thus, taking
\[
\alpha = \frac{1}{\log \log p}, \quad \beta_1 = \beta \log \log p, \quad \frac{2 \log \log N}{\log N} < \beta < \frac{1}{(\log \log p)^2},
\]
we have
\[
N - |G| < \alpha^{\frac{1}{\alpha}} N + \sum_{p_1 p_2 < N^{1-\beta_1}} \frac{N}{p_1 p_2} \left( \frac{\beta}{\beta_1} \right)^{\frac{\beta_1}{\beta}} + 11\beta N (\log \log p)^2
\]
\[
< \left( \alpha^{\frac{1}{\alpha}} + (\log \log N)^2 \left( \frac{\beta}{\beta_1} \right)^{\frac{\beta_1}{\beta}} + 11\beta (\log \log p)^2 \right) N
\]
\[
< 12\beta (\log \log p)^2 N.
\]
Therefore,
\[
\sum_{x < N} e_p(ax^*) \leq 12\beta (\log \log p)^2 N + \left| \sum_{x \in G} e_p(ax^*) \right|.
\]
We further assume that
\[ \varepsilon \beta > \frac{1}{\sqrt{\log p}}. \]

The sum \( \sum_{x \in \mathcal{G}} e_p(ax^*) \) can be bounded by
\[
\sum_{p_1} \sum_{p_2} \sum_{p_3} \sum_{y} e_p(ap_1^*p_2^*p_3^*y^*) \leq \sum_{p_1} \sum_{p_2} \sum_{p_3} \left| \sum_{y} e_p(ap_1^*p_2^*p_3^*y^*) \right|,
\]
where the summation is taken over all primes \( p_1, p_2, p_3 \) and integers \( y \) such that
\[
p_1 \geq p_2 \geq p_3, \quad p_1 \geq N^\alpha, \quad p_3 \geq N^\beta, \quad p_1p_2p_3 \leq N^{1-\beta},
\]
and
\[
y < \frac{N}{p_1p_2p_3}, \quad P(y) \leq p_3.
\]

Note that if \( t \) and \( T \) satisfy
\[
\left(1 - \frac{c}{\log p}\right)p_3 < t < p_3, \quad \left(1 - \frac{c}{\log p}\right)\frac{N}{p_1p_2p_3} < T < \frac{N}{p_1p_2p_3},
\]
where \( c > 0 \) is an arbitrary constant, then the condition on \( y \) may be replaced by the condition
\[
y < T, \quad P(y) \leq t.
\]

This results in adding to (57) a quantity of size at most
\[
N(\log \log p)^{O(1)} \frac{\log p}{\log p}.
\]

Thus for all \( t \) and \( T \) satisfying (59) we have
\[
\left| \sum_{x \in \mathcal{G}} e_p(ax^*) \right| < \frac{N(\log \log p)^{O(1)}}{\log p} + \sum_{p_1} \sum_{p_2} \sum_{p_3} \sum_{y} e_p(ap_1^*p_2^*p_3^*y^*) \leq \sum_{p_1} \sum_{p_2} \sum_{p_3} \left| \sum_{y} e_p(ap_1^*p_2^*p_3^*y^*) \right|,
\]
where the summation is taken over all primes \( p_1, p_2, p_3 \) and integers \( y \) satisfying (58) and (60).

We split the ranges for the primes \( p_1, p_2, p_3 \) into subintervals of the form \([L, L + L(\log p)^{-1}]\). By an appropriate choice of \( t \) and \( T \), we obtain that for some numbers \( M_1, M_2, M_3 \) with
\[
M_1 > 0.5M_2 > 0.2M_3, \quad M_1 > N^\alpha, \quad M_3 > N^\beta, \quad M_1M_2M_3 < N^{1-\beta}
\]
one has
\[
\left| \sum_{x \in \mathcal{G}} e_p(ax^*) \right| < \frac{N(\log \log p)^{O(1)}}{\log p} + (\log p)^{10} \sum_{p_1 \in I_1} \sum_{p_2 \in I_2} \sum_{p_3 \in I_3} \sum_{y \leq M} e_p(ap_1^*p_2^*p_3^*y^*) \leq \sum_{p_1 \in I_1} \sum_{p_2 \in I_2} \sum_{p_3 \in I_3} \left| \sum_{y \leq M} e_p(ap_1^*p_2^*p_3^*y^*) \right|,
\]
where
\[ I_j = \left[ M_j, M_j + \frac{M_j}{\log p} \right], \quad M = \frac{N}{M_1 M_2 M_3} \geq N^\beta. \]

Put
\[ W = \sum_{p_1 \in I_1} \sum_{p_2 \in I_2} \sum_{p_3 \in I_3} \left| \sum_{y \leq M} e_p(\sum_{I(y) \leq M_3} a p_1^* p_2^* p_3^* (y - z^*)) \right|. \]

Using the Cauchy–Schwarz inequality, we get
\[ W^2 \leq M_1 M_2 M_3 \sum_{y \leq M} \sum_{z \leq M} \left| \sum_{p_1 \in I_1} \sum_{p_2 \in I_2} \sum_{p_3 \in I_3} e_p(\sum_{I(y) \leq M_3} a p_1^* p_2^* p_3^*) (y - z^*) \right|. \]

Estimating the right-hand side for \( y = z \) and then appropriately fixing \( y, z \) for \( y \neq z \), we see that there is a \( b \neq 0 \ (\text{mod } p) \) such that
\[ W^2 \leq \frac{N^2}{M} + N M |S|, \quad (63) \]

where
\[ |S| = \left| \sum_{p_1 \in I_1} \sum_{p_2 \in I_2} \sum_{p_3 \in I_3} e_p(b p_1^* p_2^* p_3^*) \right|. \]

Let \( k_1, k_2, k_3 \) be integers satisfying
\[ p^{\frac{1}{k_j}} \leq M_j < p^{\frac{1}{2(k_j - 1)}}, \quad j = 1, 2, 3. \]

In particular, it follows from (61) and the choice of \( \alpha \) and \( \beta \) that
\[ k_1 < \frac{1}{\varepsilon \alpha} < (\log p)^{\frac{1}{2}}, \quad k_2, k_3 < \frac{1}{\varepsilon \beta} < (\log p)^{\frac{1}{2}}. \]

We also take even integers \( l_j \in\{k_j, k_j + 1\}, \quad j = 1, 2, 3, \) and put
\[ \eta_j(\lambda) = \left| \{(x_1, \ldots, x_{l_j}) \in (I_j \cap \mathcal{P})^{l_j} : x_1^* - x_2^* + \cdots - x_{l_j}^* \equiv \lambda \ (\text{mod } p) \} \right|. \]

We have
\[ \sum_{\lambda = 0}^{p-1} \eta_j(\lambda) < M_j^{l_j}, \quad (65) \]

and Theorem 6 yields that
\[ \sum_{\lambda = 0}^{p-1} \eta_j^2(\lambda) < M_j^{2(l_j - k_j)} (2M_j)^{k_j} (2k_j)^{k_j} \left( \frac{(2M_j)^{2k_j - 1}}{p} + 1 \right) \]
\[ < (20k_j)^{k_j} M_j^{2l_j} p^{-\frac{1}{2}}. \]

(66)

Successively applying Hölder’s inequality, we obtain that
\[ |S|^{l_1} < (M_2 M_3)^{l_1 - 1} \sum_{p_1 \in I_1} \sum_{p_2 \in I_2} \sum_{p_3 \in I_3} e_p(b p_1^* p_2^* p_3^*)^{l_1}. \]
Since the numbers $l_j$ are even, we further get

$$|S|^{l_1} < (M_2 M_3)^{l_1 - 1} \sum_{\lambda_1 = 0}^{p - 1} \eta_1(\lambda_1) \left[ \sum_{p_2 \in I_2} \sum_{p_3 \in I_3} e_p(b \lambda_1 p_2^* p_3^*) \right]$$

$$< (M_2 M_3)^{l_1 - 1} \sum_{\lambda_1 = 0}^{p - 1} \eta_1(\lambda_1) \left| \sum_{p_2 \in I_2} \sum_{p_3 \in I_3} e_p(b \lambda_1 p_2^* p_3^*) \right|.$$ 

Using Hölder’s inequality and (65), we get

$$|S|^{l_1 l_2} < (M_2 M_3)^{(l_1 - 1) l_2} M_1^{l_2 - 1} \sum_{\lambda_1 = 0}^{p - 1} \eta_1(\lambda_1) \sum_{p_3 \in I_3} e_p(b \lambda_1 M_2 p_3^*)$$

$$= M_1^{l_1 l_2} M_2^{l_2 l_1 - 1} M_3^{l_1} \sum_{\lambda_1 = 0}^{p - 1} \sum_{\lambda_2 = 0}^{p - 1} \eta_1(\lambda_1) \eta_2(\lambda_2) \sum_{p_3 \in I_3} e_p(b \lambda_1 \lambda_2 \lambda_3).$$ 

We again apply Hölder’s inequality and use (65):

$$|S|^{l_1 l_2 l_3} < M_1^{l_1 l_2 l_3} M_2^{l_2 l_1 l_3} M_3^{l_1 l_2 l_1 - 1} (M_1 M_2 M_3)^{l_2 - 1}$$

$$\times \left| \sum_{\lambda_1 = 0}^{p - 1} \sum_{\lambda_2 = 0}^{p - 1} \sum_{\lambda_3 = 0}^{p - 1} \eta_1(\lambda_1) \eta_2(\lambda_2) \eta_3(\lambda_3) e_p(b \lambda_1 \lambda_2 \lambda_3) \right|$$

$$= M_1^{l_1 l_2 l_3 - l_1} M_2^{l_2 l_1 l_3 - l_2} M_3^{l_1 l_2 l_3 - l_3} |S_1|,$$

where

$$|S_1| = \left| \sum_{\lambda_1 = 0}^{p - 1} \sum_{\lambda_2 = 0}^{p - 1} \sum_{\lambda_3 = 0}^{p - 1} \eta_1(\lambda_1) \eta_2(\lambda_2) \eta_3(\lambda_3) e_p(b \lambda_1 \lambda_2 \lambda_3) \right|.$$ 

We now use Lemma 1 with $n = 3$ and $\gamma_j(\lambda) = \eta_j(\lambda) M_j^{\lambda_j}$. It follows from (65) that

$$\|\gamma_i\|_1 = \sum_{\lambda = 0}^{p - 1} \frac{\eta_i(\lambda)}{M_i^{\lambda_i}} \leq 1.$$ 

By (66) and (64) we have

$$\|\gamma_i\|_2 = \left( \sum_{\lambda = 0}^{p - 1} \left( \frac{\eta_i(\lambda)}{M_i^{\lambda_i}} \right)^2 \right)^{\frac{1}{2}} < p^{-\frac{1}{2}}$$

and, in particular,

$$\prod_{i=1}^{n} \|\gamma_i\|_2 < p^{-\frac{1}{2} - \frac{1}{16}}.$$ 

Hence Lemma 1 is applicable and yields that

$$|S_1| < M_1 M_2 M_3 p^{-c}.$$
for some absolute constant $c > 0$. Therefore,
\[ |S| < M_1 M_2 M_3 p^{-c_1/2^k_3} < M_1 M_2 M_3 p^{-c_2 \varepsilon^3 \alpha \beta^2}. \]
Substituting this into (63) and taking into account that
\[ M > N^\beta = p^\varepsilon \beta > \exp(\sqrt{\log p}), \]
we get
\[ W < \frac{N}{\exp(0.5 \sqrt{\log p})} + N p^{-c_3 \varepsilon^3 \alpha \beta^2}. \]
Substituting this into (62), we get
\[ \left| \sum_{x \in G} e_p(ax^*) \right| < \frac{N(\log \log p)^O(1)}{\log p} + (\log p)^{10} N p^{-c_3 \varepsilon^3 \alpha \beta^2}. \]
Hence we have
\[ \left| \sum_{x < N} e_p(ax^*) \right| \leq \frac{N(\log \log p)^O(1)}{\log p} + 12 \beta (\log \log p)^2 N + (\log p)^{10} N p^{-c_3 \varepsilon^3 \alpha \beta^2}. \]
Thus, taking
\[ \beta = \frac{C \log \log p}{\varepsilon^{\frac{3}{2}} (\log p)^\frac{3}{2}}, \]
where $C$ is a sufficiently large constant, we get
\[ \left| \sum_{x < N} e_p(ax^*) \right| \ll \frac{(\log \log p)^3}{(\log p)^{\frac{3}{2}}} \varepsilon^{-\frac{3}{2}} N. \]

**Proof of Theorem 17.** We recall that here we consider only the case of prime $q$. The case of composite $q$ will be treated in a forthcoming paper.

We follow [18]. Put
\[ \mathcal{A} = \{n \leq x; n \equiv a \pmod{q}\}, \quad \mathcal{A}_d = \{n \in \mathcal{A}; n \equiv 0 \pmod{d}\}, \]
\[ S(\mathcal{A}, z) = |\{n \in \mathcal{A}; (n, p) = 1, p < z, (p, q) = 1\}|, \]
\[ D = \frac{x^{1-\varepsilon}}{q}. \]

Suppose that $D^{\frac{1}{3}} < w < y < z = (x/q)^{\frac{1}{3}}$, where $w$ and $y$ are to be specified later. Using Buchstab’s identity, we write
\[ S(\mathcal{A}, z) = S(\mathcal{A}, w) - \sum_{y \leq p < z} S(\mathcal{A}_p, z) - \sum_{w \leq p < y} S(\mathcal{A}_p, w) + \sum_{w \leq p_1 < p_2 < y} S(\mathcal{A}_{p_1 p_2}, p_2). \tag{67} \]
Using basic estimates of the linear sieve for each term in (67), we arrive at the estimate
\[ S(\mathcal{A}, z) < \frac{2x}{\varphi(q) \log D}. \tag{68} \]
(see the discussion in [18] and also [14], p. 265). In particular, it follows that

$$S(A_{p_1p_2}, p_2) < \frac{2x}{\varphi(q)p_1p_2 \log D_{12}}, \quad D_{12} = \frac{D}{p_1p_2}. \tag{69}$$

Here $D_{12}$ is the level of distribution for the sequence $A_{p_1p_2}$. The idea in [18] is to improve (69) in the mean over $p_1, p_2$ by increasing $D_{12}$ to some level $D'_{12}$.

More precisely, we define the remainders

$$R_{p_1,p_2,d} = |A_{dp_1p_2}| - \frac{x}{qdp_1p_2} \tag{70}$$

arising as error terms in the sieving process. Our strategy is to bound the total contribution of $R_{p_1,p_2,d}$ when performing the summation over $p_1, p_2$.

We subdivide $[w, y]$ into dyadic intervals and proceed to estimate

$$\sum_{p_1 \sim P_1 \atop p_2 \sim P_2} S(A_{p_1p_2}, p_2)$$

for fixed $P_1, P_2$. We introduce $D'_{12} = D'_{12}(P_1, P_2) > D_{12}$ in such a way that

$$\sum_{d < D'_{12}} \left| \sum_{p_1 \sim P_1 \atop p_2 \sim P_2} R_{p_1,p_2,d} \right| < \frac{x^{1-\varepsilon}}{q} P_1 P_2. \tag{71}$$

Taking $D'_{12}$ for the sieving limit improves the estimates (69) in the form

$$S(A_{p_1p_2}, p_2) < \frac{2x}{\varphi(q)p_1p_2 \log D'_{12}}$$

in the mean over $p_1 \sim P_1, p_2 \sim P_2$ provided that $p_2^3 > D'_{12}$. Then the gain in (68) is of order

$$\frac{x}{\varphi(q)} \sum_{w \leq p_1 < p_2 < y} \frac{1}{p_1p_2} \left( \frac{1}{\log D_{12}} - \frac{1}{\log D'_{12}} \right)$$

$$= \frac{x}{\varphi(q)} \sum_{w \leq p_1 < p_2 < y} \frac{1}{p_1p_2} \frac{\log D'_{12}}{(\log D_{12})(\log D'_{12})}. \tag{72}$$

We use the analysis in [18] to express (70) in terms of exponential sums. This shows that the left-hand side of (71) is bounded by

$$\sum_{d < D'_{12}} \sum_{0 \leq |h| < H} \left| \sum_{p_1 \sim P_1 \atop p_2 \sim P_2} (qdp_1p_2)^{-1} \hat{f} \left( \frac{h}{qdp_1p_2} \right) c_q(-ahd^*p_1^*p_2^*) \right| \tag{73}$$

up to an admissible error term. Here

$$H = qdP_1 P_2 x^{2\varepsilon-1}$$
and \( f \geq 0 \) is supported on \( x^{1-\varepsilon} < t < x + x^{1-\varepsilon} \) and satisfies \( \hat{f}(0) = x \) and \( t^j f^{(j)}(t) \ll x^{2\varepsilon j} \) for \( j \geq 0 \). Standard manipulations enable us to express (73) in terms of trilinear exponential sums \( (D_{12} \leq \tilde{D} < D'_{12}) \)

\[
\frac{x}{qDP_1P_2} H \left| \sum_{d \in I_0} \sum_{p_1 \in I_1, p_2 \in I_2} \alpha_d \beta_{p_1} \gamma_{p_2} e_q(-ahd^*p_1^*p_2^*) \right| < x^{1-c' \delta^3} \frac{1}{q} H < x^{2\varepsilon - c' \delta^3} D'_{12} P_1 P_2.
\]

where \( |\alpha_d|, |\beta_{p_1}|, |\gamma_{p_2}| \leq 1 \) and \( I_0, I_1, I_2 \) are intervals with

\[
I_0 \subset [\tilde{D}, 2\tilde{D}], \quad I_1 \subset [P_1, 2P_1], \quad I_2 \subset [P_2, 2P_2].
\]

Note that these intervals can always be enlarged to

\[
I_0 = [\tilde{D}, 2\tilde{D}], \quad I_1 = [P_1, 2P_1], \quad I_2 = [P_2, 2P_2].
\]

Take \( \delta = (1 - \theta)/5 \) and \( w = x^\delta, \ y = x^{2\delta} \). Note that

\[
\tilde{D} > D_{12} > \frac{D}{y^2} > x^{0.9\delta}.
\]

The Karatsuba amplification argument followed by an estimation of the trilinear exponential sums gives a saving of a factor \( x^{c' \delta^3} \). Hence,

\[
\frac{x}{qDP_1P_2} H \left| \sum_{d \in I_0} \sum_{p_1 \in I_1, p_2 \in I_2} \alpha_d \beta_{p_1} \gamma_{p_2} e_q(-ahd^*p_1^*p_2^*) \right| < x^{1-c' \delta^3} \frac{1}{q} H < x^{2\varepsilon - c' \delta^3} D'_{12} P_1 P_2.
\]

For

\[
D'_{12} = \frac{x^{1+c'' \delta^3}}{qP_1P_2} \sim D_{12} x^{c'' \delta^3}
\]

the right-hand side of (74) does not exceed \( x^{1-\varepsilon}q^{-1} \). The condition \( w^5 > D'_{12} \) holds. Returning to (72), we gain a quantity of order

\[
\frac{x}{\varphi(q)} \sum_{x^\delta < p_1 < p_2 < x^{2\delta}} \frac{1}{p_1p_2} \frac{\log(x^{c'' \delta^3})}{\delta^2(\log x)^2} \gg \frac{x\delta}{\varphi(q) \log x} \sim \frac{x\delta^2}{\varphi(q) \log \frac{x}{q}}.
\]

Since \( \varepsilon \) is small, the desired result follows. \( \square \)

\[\text{§ 10. Comments}\]

As mentioned in the introduction, if \( I \subset \mathbb{F}_p^* \) is an interval with \( |I| < p^{\frac{1}{2}} \), then

\[
|I^{-1} + I^{-1} + I^{-1}| > |I|^{1.55 + o(1)}.
\]

This is better than the estimate in Corollary 1 for \( k = 3 \). We now prove (75). We can assume that \( |I| = N > p^{\frac{1}{3}} \) because otherwise Corollary 4 yields a better bound

\[
|I^{-1} + I^{-1}| > |I|^{2 + o(1)}.
\]
Let \( J_6 \) be the number of solutions of the congruence
\[
\frac{1}{x_1} + \frac{1}{x_2} + \frac{1}{x_3} \equiv \frac{1}{x_4} + \frac{1}{x_5} + \frac{1}{x_6} \pmod{p}, \quad x_1, \ldots, x_6 \in I.
\]
We can bound \( J_6 \):
\[
J_6 \leq (J_4J_8)^{\frac{1}{2}}.
\]
It follows from Theorem 1 that \( J_8 < N^{\frac{32}{5}+o(1)} \). By Corollary 4 we have
\[
J_4 < \frac{N^{\frac{7}{2}+o(1)}}{p^2}.
\]
Thus,
\[
J_6 < \frac{N^{\frac{99}{10}+o(1)}}{p-\frac{1}{4}}.
\]
Using the relationship between the number of solutions of a congruence and the cardinality of the corresponding set, we conclude that
\[
|I^{-1} + I^{-1} + I^{-1}| \geq N^{\frac{64}{10}+o(1)}p^{\frac{1}{2}} > N^{1.55+o(1)}.
\]
Note that the arguments in the proof of Theorem 1 yield the following result.

**Proposition 1.** For any fixed positive integer constants \( r \) and \( k \), the number \( J_{2k}^{(r)} \) of solutions of the congruence
\[
\frac{1}{x_1^r} + \cdots + \frac{1}{x_k^r} \equiv \frac{1}{x_{k+1}^r} + \cdots + \frac{1}{x_{2k}^r} \pmod{p}, \quad x_1, \ldots, x_{2k} \in I,
\]
satisfies the bound
\[
J_{2k}^{(r)} < \left( |I|^{\frac{2k^2}{k+1}} + \frac{|I|^{2k}}{p} \right)|I|^{o(1)}.
\]

**Corollary 5.** Suppose that \( r_1, r_2, k_1, k_2 \) are fixed positive integer constants, \( I_1 = [a_1 + 1, a_1 + N_1] \), \( I_2 = [a_2 + 1, a_2 + N_2] \) and
\[
N_1 < p^{\frac{k_1+1}{2k_1}}, \quad N_2 < p^{\frac{k_2+1}{2k_2}}.
\]
Then for any complex coefficients \( \alpha_1(x_1), \alpha_2(x_2) \) with \( |\alpha_i(x_i)| \leq 1 \) one has
\[
\max_{(a,p)=1} \left| \sum_{x_1 \in I_1} \sum_{x_2 \in I_2} \alpha_1(x_1)\alpha_2(x_2)e_p(ax_1^{-r_1}x_2^{-r_2}) \right| < \left( p^{\frac{1}{2k_1k_2}} N_1^{-\frac{1}{k_2(k_1+1)}} N_2^{-\frac{1}{k_1(k_2+1)}} \right)(N_1N_2)^{1+o(1)}.
\]
Combining the bilinear sums in Corollary 5 with a formula of Vaughan [34], one can bound the corresponding sums over primes as in Theorems A1, A9 in [1] and Corollary 1.5 in [35].
Corollary 6. Suppose that $r \in \mathbb{Z}_+$ and $p > N > p^{\frac{1}{2} + \varepsilon}$ for some $\varepsilon > 0$. Then
\[
\max_{(a,p)=1} \left| \sum_{x < N \text{ prime}} e_p(ax-r) \right| < N^{1-\delta},
\]
where $\delta = \delta(\varepsilon; r) > 0$.

We further remark that a result in [12] yields the bound
\[
\max_{(a,p)=1} \left| \sum_{x < p \text{ prime}} e_p(ax-1) \right| < p^{\frac{15}{16} + o(1)}.
\]

Corollary 5 leads to the following assertion.

Corollary 7. For every fixed positive integer constant $r$ we have
\[
\max_{(a,p)=1} \left| \sum_{x < p \text{ prime}} e_p(ax-r) \right| < p^{\frac{44}{24} + o(1)}.
\]

Proof. It suffices to prove that
\[
\left| \sum_{n \leq p} \Lambda(n)e_p(an-r) \right| < p^{\frac{44}{24} + o(1)},
\]
which yields the desired result by partial summation. Here $\Lambda(n)$ is von Mangoldt’s function.

In what follows we write $A \lesssim B$ to indicate that $A < Bp^{o(1)}$. By Vaughan’s identity (see [36], Ch. 24) we have
\[
\sum_{n \leq p} \Lambda(n)e_p(an-r) \lesssim W_1 + W_2 + W_3 + W_4,
\]
where
\[
W_1 = \left| \sum_{n \leq U} \Lambda(n)e_p(an-r) \right|,
W_2 = \left| \sum_{n \leq UV} \sum_{m \leq p/n} e_p(an-rm-r) \right|,
W_3 = \left| \sum_{n \leq V} \sum_{m \leq p/n} (\log m)e_p(an-rm-r) \right|,
W_4 = \left| \sum_{U < n \leq p/V} \sum_{V < m \leq p/n} \beta_m e_p(an-rm-r) \right|.
\]

Here $U \geq 2$ and $V \geq 2$ are parameters with $UV \leq p$,
\[
\beta_m = \sum_{d|m} \mu(d).
\]

We shall use Weil’s bound in the form
\[
\left| \sum_{x=1}^{p-1} e_p(ax-r + bx) \right| \ll p^{\frac{1}{2}}.
\]
More precisely, we shall use the following corollary of this bound. For every interval $I \subset \mathbb{F}_p$ we have
\[
\left| \sum_{x \in I} e_p(ax^{-r}) \right| \lesssim p^{1/2}.
\]

Take $U = V = p^{1/3}$ and estimate $W_1$ trivially:
\[
W_1 \lesssim U = p^{1/3}.
\]

To estimate $W_2$, divide the range of summation over $n$ into dyadic intervals. Then, for some $L \leq p^{2/3}$ we have
\[
W_2 \lesssim \sum_{L \leq n \leq 2L} \left| \sum_{m \leq p/n} e_p(an^{-r}m^{-r}) \right|.
\]

If $L < p^{1/3}$, then we apply Weil’s bound for the sum over $m$ and get
\[
W_2 \lesssim L p^{1/2} \lesssim p^{5/6}.
\]

If $p^{1/3} < L < p^{2/3}$, then a standard smoothing argument enables us to extend the summation over $m$ to $m \leq p/L$ and apply Corollary 5 with $k_1 = k_2 = 2$. We get
\[
W_2 \lesssim p^{23/24}.
\]

To estimate $W_3$, we use partial summation over $m$ and Weil’s bound. We get
\[
W_3 \lesssim \sum_{n < p^{1/3}} p^{1/2} \lesssim p^{5/6}.
\]

To estimate $W_4$, we divide the range of summation over $n$ into dyadic intervals and obtain the following estimate for some $L$, $p^{1/3} < L \leq p^{2/3}$:
\[
W_4 \lesssim \sum_{L \leq n < 2L} \left| \sum_{p^{1/3} < m \leq p/n} \beta_m e_p(an^{-r}m^{-r}) \right|.
\]
A smoothing argument enables us to extend the range of summation over $m$ to $m < p/L$. Using Corollary 5 with $k_1 = k_2 = 2$, we get
\[
W_4 \lesssim p^{23/24}. \qed
\]

Bibliography

[1] J. Bourgain, “More on the sum-product phenomenon in prime fields and its applications”, Int. J. Number Theory 1:1 (2005), 1–32.

[2] J. Cilleruelo and M. Z. Garaev, “Concentration of points on two and three dimensional modular hyperbolas and applications”, Geom. Funct. Anal. 21:4 (2011), 892–904.
[3] J. Bourgain, “Multilinear exponential sums in prime fields under optimal entropy condition on the sources”, *Geom. Funct. Anal.* **18**:5 (2009), 1477–1502.

[4] M. A. Korolev, “Incomplete Kloosterman sums and their applications”, *Izv. Ross. Akad. Nauk Ser. Mat.* **64**:6 (2000), 41–64; English transl., *Izv. Math.* **64**:6 (2000), 1129–1152.

[5] A. A. Karatsuba, “Fractional parts of functions of a special form”, *Izv. Ross. Akad. Nauk Ser. Mat.* **59**:4 (1995), 61–80; English transl., *Izv. Math.* **59**:4 (1995), 721–740.

[6] A. A. Karatsuba, “Analogues of Kloosterman sums”, *Izv. Ross. Akad. Nauk Ser. Mat.* **59**:5 (1995), 93–102; English transl., *Izv. Math.* **59**:5 (1995), 971–981.

[7] R. C. Baker, “Kloosterman sums with prime variable”, *Acta Arith.* **156**:4 (2012), 351–372.

[8] Wenzhi Luo, “Bounds for incomplete hyper-Kloosterman sums”, *J. Number Theory* **75**:1 (1999), 41–46.

[9] I. E. Shparlinski, “Bounds of incomplete multiple Kloosterman sums”, *J. Number Theory* **126**:1 (2007), 68–73.

[10] M. Z. Garaev, “Estimation of Kloosterman sums with primes and its application”, *Mat. Zametki* **88**:3 (2010), 365–373; English transl., *Math. Notes* **88**:3 (2010), 330–337.

[11] J. Bourgain, M. Z. Garaev, S. V. Konyagin, and I. E. Shparlinski, “On congruences with products of variables from short intervals and applications”, *Orthogonal series, approximation theory and related topics*, Papers for the 60th birthday of Academician Boris Sergeevich Kashin, Tr. Mat. Inst. Steklova, vol. 280, MAIK, Moscow 2013, pp. 67–96; *Proc. Steklov Inst. Math.* **280**:1 (2013), 61–90.

[12] J. Friedlander and H. Iwaniec, *Opera de cribro*, Amer. Math. Soc. Colloq. Publ., vol. 57, Amer. Math. Soc., Providence, RI 2010.

[13] M. A. Korolev, “Short Kloosterman sums with weights”, *Mat. Zametki* **88**:3 (2010), 415–427; English transl., *Math. Notes* **88**:3 (2010), 374–385.

[14] A. A. Karatsuba, “New estimates of short Kloosterman sums”, *Mat. Zametki* **88**:3 (2010), 384–398; English transl., *Math. Notes* **88**:3 (2010), 347–359.

[15] M. Z. Garaev, “Sums and products of sets and estimates of rational trigonometric sums in fields of prime order”, *Uspekhi Mat. Nauk* **65**:4 (394) (2010), 5–66; English transl., *Russian Math. Surveys* **65**:4 (2010), 599–658.

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

[17] J. Maynard, “On the Brun–Titchmarsh theorem”, *Acta Arith.* **157**:3 (2013), 249–296.

[18] Y. Motohashi, “An extension of the Linnik phenomenon”, *Mathematics and informatics*, 1, For the 75th anniversary of Anatolii Alekseevich Karatsuba, Sovr. Probl. Mat., vol. 16, Steklov Math. Institute, RAS, Moscow 2012, pp. 66–75; Reprinted in *Proc. Steklov Inst. Math.* **280**: Suppl. 2 (2013), S56–S64.

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

[20] T. Tao and Van H. Vu, *Additive combinatorics*, Cambridge Stud. Adv. Math., vol. 105, Cambridge Univ. Press, Cambridge 2006.
[23] Yu. V. Linnik, “An elementary solution of Waring’s problem by Shnirel’man’s method”, Mat. Sb. 12 (54):2 (1943), 225–230. (Russian)
[24] Z. I. Borevich and I. R. Shafarevich, Number theory, Nauka, Moscow 1964; English transl., Pure and Applied Mathematics, vol. 20, Academic Press, New York–London 1966.
[25] K. Ireland and M. Rosen, A classical introduction to modern number theory, 2nd ed., Grad. Texts in Math., vol. 84, Springer-Verlag, New York 1990.
[26] V. V. Prasolov, Polynomials, 2nd ed., MCCME, Moscow 2001; English transl., Algorithms Comput. Math., vol. 11, Springer-Verlag, Berlin 2004.
[27] D. R. Heath-Brown, “Almost-primes in arithmetic progressions and short intervals”, Math. Proc. Cambridge Philos. Soc. 83:3 (1978), 357–375.
[28] J. Bourgain, M. Z. Garaev, S. V. Konyagin, and I. E. Shparlinski, “On the hidden shifted power problem”, SIAM J. Comput. 41:6 (2012), 1524–1557.
[29] A. Ayyad, T. Cochrane, and Z. Zheng, “The congruence $x_1x_2 \equiv x_3x_4 \pmod{p}$, the equation $x_1x_2 = x_3x_4$ and mean value of character sums”, J. Number Theory 59:2 (1996), 398–413.
[30] J. Friedlander and H. Iwaniec, “Estimates for character sums”, Proc. Amer. Math. Soc. 119:2 (1993), 365–372.
[31] J. Bourgain, “The discretized sum-product and projection theorems”, J. Anal. Math. 112:1 (2010), 193–236.
[32] M. N. Huxley, “On the difference between consecutive primes”, Invent. Math. 15:2 (1972), 164–170.
[33] N. G. de Bruijn, “On the number of positive integers $\leq x$ and free of prime factors $> y$. II”, Indag. Math. 28 (1966), 239–247.
[34] R. C. Vaughan, “Sommes trigonométriques sur les nombres premiers”, C. R. Acad. Sci. Paris Sér. A 285:16 (1977), 981–983.
[35] E. Fouvry and P. Michel, “Sur certaines sommes d’exponentielles sur les nombres premiers”, Ann. Sci. École Norm. Sup. (4) 31:1 (1998), 93–130.
[36] H. Davenport, Multiplicative number theory, 3rd ed., Grad. Texts in Math., vol. 74, Springer-Verlag, New York 2000.

Jean Bourgain
Institute for Advanced Study,
School of Mathematics, Princeton, NJ, USA
E-mail: bourgain@ias.edu

Moubariz Z. Garaev
National Autonomous University of Mexico,
Morelia Campus, Center of Mathematical Sciences, Mexico
E-mail: garaev@matmor.unam.mx

Received 20/NOV/12
Translated by THE AUTHORS
22/JUL/13