*Bull. Aust. Math. Soc.* **112** (2025), 237–247
doi:10.1017/S0004972725000152

# BINARY AND TERNARY CONGRUENCES INVOLVING INTERVALS AND SETS MODULO A PRIME

**MOUBARIZ Z. GARAEV, JULIO C. PARDO and IGOR E. SHPARLINSKI**

(Received 19 October 2024; accepted 20 December 2024; first published online 18 March 2025)

**Abstract**

Let $s$ be a fixed positive integer constant and let $\varepsilon$ be a fixed small positive number. Then, provided that a prime $p$ is large enough, we prove that, for any set $\mathcal{M} \subseteq \mathbb{F}_p^*$ of size $|\mathcal{M}| = \lfloor p^{14/29} \rfloor$ and integer $H = \lfloor p^{14/29+\varepsilon} \rfloor$, any integer $\lambda$ can be represented in the form

$$\frac{m_1}{x_1^s} + \frac{m_2}{x_2^s} + \frac{m_3}{x_3^s} \equiv \lambda \bmod p \quad \text{with } m_i \in \mathcal{M} \text{ and } 1 \leqslant x_i \leqslant H,\ i = 1, 2, 3.$$

When $s = 1$, we show that, for almost all primes $p$, if $|\mathcal{M}| = \lfloor p^{1/2} \rfloor$ and $H = \lfloor p^{1/2} (\log p)^{6+\varepsilon} \rfloor$, then any integer $\lambda$ can be represented in the form

$$\frac{m_1}{x_1} + \frac{m_2}{x_2} \equiv \lambda \bmod p \quad \text{with } m_i \in \mathcal{M} \text{ and } 1 \leqslant x_i \leqslant H,\ i = 1, 2.$$

2020 *Mathematics subject classification*: primary 11D79; secondary 11L07, 11L26.

*Keywords and phrases*: products of intervals and sets, congruences, exponential sums, character sums.

## 1. Introduction

**1.1. Motivation.** The problem of distribution of elements of sets involving products and sums of intervals and arbitrary sets in finite fields has been a subject of extensive investigation (see, for example [1–6, 9]). We continue studying this problem and consider some questions related to binary and ternary congruences modulo a sufficiently large prime number $p$, which involve products and inverses of elements from short intervals or arbitrary sets.

Let $\mathbb{F}_p$ denote the finite field of residue classes modulo $p$. Throughout the paper, we always assume that $\mathbb{F}_p$ is represented by the set $\{0, 1, \ldots, p-1\}$ and we freely alternate between equations in $\mathbb{F}_p$ and congruences modulo $p$. We also use $\varepsilon > 0$ to be an arbitrarily small real number.

The third author was partially supported by ARC Grants DP230100530 and DP230100534.

© The Author(s), 2025. Published by Cambridge University Press on behalf of Australian Mathematical Publishing Association Inc.



https://doi.org/10.1017/S0004972725000152 Published online by Cambridge University Press

Let $\mathcal{M}$ be an arbitrary subset of $\mathbb{F}_p^* := \mathbb{F}_p \setminus \{0\}$ with $M = \#\mathcal{M}$ elements, let $\mathcal{X} \subseteq \mathbb{F}_p^*$ be an arbitrary interval of length $H$ and let $s$ be a fixed positive integer. It is known from [6] that if

$$H > p^{17/35+\varepsilon}, \quad M > p^{17/35+\varepsilon}.$$

then the number $T_6(\lambda)$ of solutions of the congruence

$$\frac{m_1}{x_1^s} + \frac{m_2}{x_2^s} + \frac{m_3}{x_3^s} + \frac{m_4}{x_4^s} + \frac{m_5}{x_5^s} + \frac{m_6}{x_6^s} \equiv \lambda \bmod p \quad \text{with } m_i \in \mathcal{M},\ x_i \in \mathcal{X},\ i = 1, \dots, 6,$$

satisfies

$$T_6(\lambda) = \frac{H^6 M^6}{p}(1 + O(p^{-\delta})),$$

where $\delta > 0$ depends only on $s$ and $\varepsilon$. In [6, Section 1.2], an open question has been posed to obtain an asymptotic formula for the five-term analogue of $T_6(\lambda)$ with $H = M = o(p^{1/2})$.

**1.2. Main results.** The first result of our present paper deals with the solubility problem of the corresponding congruence with three summands, assuming that the set $\mathcal{X}$ starts from the origin. Although our result does not provide an asymptotic formula, we can still prove the existence of solutions.

In what follows, we use $\mathcal{H}$ to denote the set of the first $H$ positive integers: that is,

$$\mathcal{H} = \{1, 2, \dots, H\}.$$

We also recall that $\mathcal{M}$ is an arbitrary subset of $\mathbb{F}_p^*$ with $M = \#\mathcal{M}$ elements.

THEOREM 1.1. *Let $M = \lfloor p^{14/29} \rfloor$ and $H = \lfloor p^{14/29+\varepsilon} \rfloor$. Then any integer $\lambda$ can be represented in the form*

$$\frac{m_1}{x_1^s} + \frac{m_2}{x_2^s} + \frac{m_3}{x_3^s} \equiv \lambda \bmod p \quad m_i \in \mathcal{M},\ x_i \in \mathcal{H},\ i = 1, 2, 3.$$

We note that the problem of obtaining an asymptotic formula for the number of representations of $\lambda$ in the form given by Theorem 1.1 is still an open problem.

We now consider the problem of solubility of the corresponding congruence with two summands, with $M$ and $H$ of the critical size $p^{1/2+o(1)}$. The case $s \geqslant 2$ turns out to be very hard and currently we cannot say much about it. Here, we restrict ourselves to the case $s = 1$.

If $\mathcal{M}$ is a set of $M$ consecutive integers, then the question is reduced to the problem of the ratio of two intervals. This problem was considered in [3–5]. In this case, it is known from the proof of [5, Theorem 1.7] and [4, Lemma 5] that if $M > cp^{1/2}$, $H > cp^{1/2}$, then, for some suitable positive constant $c$, any integer $\lambda$ can be represented in the form

$$\frac{m_1}{x_1} + \frac{m_2}{x_2} \equiv \lambda \bmod p,$$

https://doi.org/10.1017/S0004972725000152 Published online by Cambridge University Press

with $m_1, m_2 \in \mathcal{M}$ and $x_1, x_2 \in \mathcal{H}$. However, the method of the aforementioned works does not apply for arbitrary sets $\mathcal{M}$.

Our next result deals with a binary congruence for arbitrary sets $\mathcal{M} \subseteq \mathbb{F}_p^*$ for almost all prime moduli $p$. As usual, we denote the number of primes not exceeding $X$ by $\pi(X)$.

THEOREM 1.2. *Let $0 < \varepsilon < 0.1$ and let $X \geqslant 2$. The following holds for all but $\pi(X)/X^{0.01\varepsilon}$ primes $p \leqslant X$. Let $M = \lfloor p^{1/2} \rfloor$ and $H = \lfloor p^{1/2}(\log p)^{6+\varepsilon} \rfloor$. Then any integer $\lambda$ can be represented in the form*

$$\frac{m_1}{x_1} + \frac{m_2}{x_2} \equiv \lambda \bmod p, \quad m_i \in \mathcal{M},\ x_i \in \mathcal{H},\ i = 1, 2.$$

We now consider the binary problem with ratios of two intervals. First, we observe that if $N < p^{1/2}$, then all irreducible fractions

$$\frac{m}{x}, \quad 1 \leqslant m, x \leqslant N,$$

are distinct modulo $p$. Furthermore, the number of such fractions is asymptotically equal to $6N^2/\pi^2$. (For the best known error term, see [10, Ch. V, Section 5, Equation (12)].) Hence, if $N = \lfloor cp^{1/2} \rfloor$, where $c > \pi/\sqrt{12}$, then

$$\#\left\{\frac{m}{x} \bmod p :\ 1 \leqslant m,\ x \leqslant N\right\} > p/2$$

and, by the pigeonhole principle, we get the representability of any integer $\lambda$ in the form

$$\frac{m_1}{x_1} + \frac{m_2}{x_2} \equiv \lambda \bmod p,$$

with

$$1 \leqslant m_1, m_2, x_1, x_2 \leqslant \left\lfloor \sqrt{(\pi^2/12 + \varepsilon)p} \right\rfloor.$$

Note that, generally speaking, the sizes of the intervals cannot be taken as $o(p^{1/2})$. Indeed, it is easy to see that the congruence

$$\frac{m_1}{x_1} + \frac{m_2}{x_2} \equiv -1 \bmod p$$

has no solutions in positive integers $m_1, m_2, x_1, x_2$ below $\sqrt{p/3}$. Moreover, the congruence

$$\frac{m_1}{x_1} + \frac{m_2}{x_2} \equiv 0 \bmod p$$

has no solutions in positive integers $m_1, m_2, x_1, x_2$ below $\sqrt{p/2}$.

We now consider the case of two arbitrary intervals. More precisely, let $\mathcal{I}$ and $\mathcal{J}$ be subsets of $\mathbb{F}_p^*$ consisting of $N$ consecutive integers. Then, it follows from [4, 5] that the representability holds when $N > cp^{1/2}$ for some suitable constant $c$.

https://doi.org/10.1017/S0004972725000152 Published online by Cambridge University Press

Therefore, it is interesting to find the best possible constant $c$ in the problem of binary congruences with a ratio of intervals. Here, following the argument of [4, 5], we show that, for arbitrary intervals $\mathcal{I}$ and $\mathcal{J}$ of length $\lfloor cp^{1/2} \rfloor$, one can take $c = \sqrt{8}$.

THEOREM 1.3. *Let $\mathcal{I}$ and $\mathcal{J}$ be subsets of $\mathbb{F}_p^*$ comprising $\lfloor \sqrt{8p} \rfloor$ consecutive integers modulo $p$. Then any integer $\lambda$ can be represented in the form*

$$\frac{m_1}{x_1} + \frac{m_2}{x_2} \equiv \lambda \bmod p, \quad \text{with } m_1, m_2 \in \mathcal{I},\ x_1, x_2 \in \mathcal{J}.$$

**1.3. Notation and conventions.** We recall that $U = O(V)$, $U \ll V$ and $V \gg U$ are all equivalent to the statement that $|U| \leqslant cV$ holds with some constant $c > 0$.

Any implied constants in symbols $O$, $\ll$ and $\gg$ may occasionally, where obvious, depend on the integer parameters $\ell$ and $s$, the real parameter $\varepsilon > 0$ and the fixed constant $c$, and are absolute otherwise.

Given two quantities $U$ and $V > 0$, we write $U = o(V)$ and $U = V^{o(1)}$ to mean that $|U| \leqslant \psi(V)V$ and $|U| \leqslant V^{\psi(V)}$, respectively, for some function $\psi$ such that $\psi(V) \to 0$ as $V \to \infty$.

We also use $U \lesssim V$ to mean that $|U| < Vp^{o(1)}$.

Given a set $\mathcal{X}$, we use $|\mathcal{X}|$ to denote its cardinality.

For a positive integer $N$, as usual, $\pi(N)$ denotes the number of primes $p \leqslant N$, while, for a real $z$ and a prime $p$, we use the notation $\mathbf{e}_p(z) = \exp(2\pi i z/p)$.

## 2. Auxiliary lemmas

We recall that $s$ is a fixed positive integer constant, $\mathcal{M} \subseteq \mathbb{F}_p^*$ with $M = |\mathcal{M}| < p^{1/2}$ and $\mathcal{H} = \{1, 2, \ldots, H\} \bmod p$.

LEMMA 2.1. *Assume that*

$$M = |\mathcal{M}| < p^{1/2}, \quad H = |\mathcal{H}| < p^{1/2}.$$

*Then, for the cardinality of the set*

$$\mathcal{M} \cdot \mathcal{H}^{-s} = \{mh^{-s} \bmod p : m \in \mathcal{M},\ h \in \mathcal{H}\},$$

*we have the bound*

$$|\mathcal{M} \cdot \mathcal{H}^{-s}| \gg \min\{MH/\log p,\ H^2/\log^2 p\}.$$

PROOF. Let $J$ be the number of solutions of the congruence

$$m_1 q_1^{-s} \equiv m_2 q_2^{-s} \bmod p, \quad m_1, m_2 \in \mathcal{M}, \quad q_1, q_2 \in \mathcal{R},$$

where $\mathcal{R}$ is the set of primes from $\mathcal{H}$. We have

$$R = |\mathcal{R}| \gg \frac{H}{\log p}. \tag{2.1}$$

https://doi.org/10.1017/S0004972725000152 Published online by Cambridge University Press

We claim that,

$$J \leqslant s(M^2 + MR).$$

If $m_1 = m_2$, then $q_1^s \equiv q_2^s \bmod p$ and we have at most $sMR$ possibilities in this case.

Let $m_1 \neq m_2$ be fixed. Denoting $\lambda \equiv m_1 m_2^{-1} \not\equiv 1 \pmod p$, we have

$$(q_1 q_2^{-1})^s \equiv \lambda \bmod p. \tag{2.2}$$

Clearly, $q_1 \neq q_2$ for each solution to (2.2). It follows that, for any fixed $\lambda$, there are at most $s$ different values for $q_1 q_2^{-1}$ modulo $p$. But, for each such value of $q_1 q_2^{-1}$, the primes $q_1$ and $q_2$ are defined uniquely. Indeed, if there are two such pairs of primes $q_1 \neq q_2$ and $r_1 \neq r_2$, then

$$q_1 r_2 \equiv q_2 r_1 \bmod p.$$

Since both sides are positive integers less than $p$, this congruence becomes an equality $q_1 r_2 = q_2 r_1$, which implies that $q_1 = r_1$ and $q_2 = r_2$. Therefore, when $m_1 \neq m_2$, and thus $\lambda \neq 1$, the congruence (2.2) has at most $s$ solutions $(q_1, q_2)$, which leads to the term $sM^2$ in the bound on $J$.

Now we use the standard relationship between the number of solutions and the cardinalities, which follows from the Cauchy-Schwarz inequality: that is,

$$\sum_{m \in \mathcal{M}} \sum_{q \in \mathcal{R}} 1 = \sum_{\lambda \in \mathcal{M} \cdot \mathcal{R}^{-s}} \sum_{\substack{m \in \mathcal{M},\ q \in \mathcal{R} \\ mq^{-s} \equiv \lambda \bmod p}} \sum 1 \leqslant \sqrt{|\mathcal{M} \cdot \mathcal{R}^{-s}| J},$$

where $\mathcal{R}^{-s} = \{q^{-s} : \ q \in \mathcal{R}\}$. We now derive that

$$|\mathcal{M} \cdot \mathcal{H}^{-s}| \geqslant |\mathcal{M} \cdot \mathcal{R}^{-s}| \geqslant \frac{sM^2R^2}{s(M^2 + MR)} \gg \min\{R^2, MR\},$$

which, together with (2.1), concludes the proof. □

We also need the following result given by [6, Theorem 1.2].

LEMMA 2.2. *Let $s$ be a fixed positive integer and let integers $K$ and $H$ be such that*

$$0 < K + 1 < K + H < p.$$

*Then, for any fixed positive integer $\ell$, the following bound holds:*

$$\sum_{m \in \mathcal{M}} \left| \sum_{K+1 \leqslant x \leqslant K+H} \mathbf{e}_p(amx^{-s}) \right| \lesssim HM\left(\frac{p}{MH^{2\ell/(\ell+1)}} + \frac{1}{M}\right)^{1/(2\ell)}.$$

Finally, we recall the following statement from [3, Theorem 3]; we refer the reader to [7, Ch. 3] or [8, Section 4.2] for the background on characters.

LEMMA 2.3. *Let $c$ be a positive constant and let*

$$Q = (\log X)^c, \quad \Delta > 0, \quad \Delta \to 0 \quad \text{as } X \to +\infty.$$

https://doi.org/10.1017/S0004972725000152 Published online by Cambridge University Press

*Then, for all but*

$$O(X^{2c^{-1}-4(\log\Delta)(\log Q)^{-1}}e^{-\log X/100c\log\log X})$$

*positive integers $k \leqslant X$, the inequality*

$$\Big|\sum_{\substack{q\leqslant Q\\ q \text{ prime}}}\chi(q)\Big| \leqslant \pi(Q)\Delta$$

*holds for any primitive multiplicative character $\chi$ modulo $k$.*

We note that, for a prime modulus $k = p$, all nontrivial characters are primitive.

## 3. Proof of the theorems

PROOF OF THEOREM 1.1. Let

$$\mathcal{D} = \mathcal{M}\cdot\mathcal{H}^{-s}.$$

By Lemma 2.1,

$$|\mathcal{D}| \gg \min\{MH/\log p,\ H^2/\log^2 p\} = MH/\log p.$$

It suffices to prove the solubility of the congruence

$$d_1 + d_2 + \frac{m}{x^s} \equiv \lambda \bmod p, \tag{3.1}$$

with

$$d_1, d_2 \in \mathcal{D}, \quad m \in \mathcal{M}, \quad x \in \mathcal{H}.$$

Using the orthogonality of exponential functions and expressing the number $T$ of solutions of (3.1) via exponential sums, we see that

$$T = \sum_{d_1\in\mathcal{D}}\sum_{d_2\in\mathcal{D}}\sum_{m\in\mathcal{M}}\sum_{x\in\mathcal{H}}\frac{1}{p}\sum_{a=0}^{p-1}\mathbf{e}_p(a(d_1+d_2+mx^{-s}-\lambda)).$$

Next, changing the order of summation and separating the term corresponding to $a = 0$, we obtain

$$T = \frac{1}{p}\sum_{a=0}^{p-1}\sum_{d_1\in\mathcal{D}}\sum_{d_2\in\mathcal{D}}\sum_{m\in\mathcal{M}}\sum_{x\in\mathcal{H}}\mathbf{e}_p(a(d_1+d_2+mx^{-s}-\lambda)) = \frac{|D|^2HM}{p} + O(E), \tag{3.2}$$

where

$$\begin{aligned} E &= \frac{1}{p}\Big|\sum_{a=1}^{p-1}\sum_{d_1\in\mathcal{D}}\sum_{d_2\in\mathcal{D}}\sum_{m\in\mathcal{M}}\sum_{x\in\mathcal{H}}\mathbf{e}_p(a(d_1+d_2+mx^{-s}-\lambda))\Big| \\ &\leqslant \frac{1}{p}\sum_{a=1}^{p-1}\Big|\sum_{d\in\mathcal{D}}\mathbf{e}_p(ad)\Big|^2\Big|\sum_{m\in\mathcal{M}}\sum_{x\in\mathcal{H}}\mathbf{e}_p(amx^{-s})\Big|. \end{aligned}$$

https://doi.org/10.1017/S0004972725000152 Published online by Cambridge University Press

From Lemma 2.2 with $\ell = 3$,

$$\left|\sum_{m\in\mathcal{M}}\sum_{x\in\mathcal{H}} \mathbf{e}_p(amx^{-s})\right| \lesssim HM\Big(\frac{p}{MH^{3/2}} + \frac{1}{M}\Big)^{1/6}.$$

Observing that

$$\frac{p}{MH^{3/2}} + \frac{1}{M} \ll \frac{p}{MH^{3/2}} \quad \text{and} \quad \sum_{a=0}^{p-1}\left|\sum_{d\in\mathcal{D}} \mathbf{e}_p(ad)\right|^2 = p|D|,$$

we get

$$\begin{aligned} E &\lesssim HM\frac{p^{1/6}}{pM^{1/6}H^{1/4}}\sum_{a=0}^{p-1}\left|\sum_{d\in\mathcal{D}} \mathbf{e}_p(ad)\right|^2 \\ &= HM\frac{p^{1/6}}{M^{1/6}H^{1/4}}|D| = \frac{|D|^2HM}{p}\times\Delta, \end{aligned}$$

where

$$\Delta = \frac{p^{7/6}}{|D|M^{1/6}H^{1/4}} < p^{-0.1\varepsilon}.$$

Inserting this into (3.2), yields

$$T = (1+o(1))\frac{|D|^2HM}{p},$$

and the result follows. □

PROOF OF THEOREM 1.2. In Lemma 2.3, we take

$$c = 6+\varepsilon, \quad Q = (\log X)^{6+\varepsilon}, \quad \Delta = (\log X)^{-1-0.1\varepsilon}.$$

Then we have at most $O(X^{1-0.6\varepsilon/(6+\varepsilon)})$ exceptional positive integers $k \leqslant X$. Hence, for $\pi(X)(1+O(X^{-0.05\varepsilon}))$ primes $p$ with $X^{1/2} < p \leqslant X$, the inequality

$$\left|\sum_{q\leqslant Q}\chi(q)\right| \leqslant \pi(Q)(\log X)^{-1-0.1\varepsilon} \tag{3.3}$$

holds for any nonprincipal character $\chi$ modulo $p$.

Let

$$\mathcal{D} = \{m/h :\ m\in\mathcal{M},\ h\in\{1,\dots,\lfloor 0.01p^{1/2}\rfloor\}\}.$$

Note that if $X^{1/2} < p \leqslant X$, $h \leqslant [0.01p^{1/2}]$ and $q \leqslant (\log X)^{6+\varepsilon}$, then $hq \leqslant p^{1/2}(\log p)^{6+\varepsilon}$.

We now prove that if (3.3) holds for some $p$ with $X^{1/2} < p \leqslant X$, then the cardinality of the set

$$\mathcal{G} = \{d/q \bmod p :\ d\in\mathcal{D},\ q\leqslant (\log X)^{6+\varepsilon}\}$$

satisfies

$$|\mathcal{G}| = (1+o(1))p. \tag{3.4}$$

https://doi.org/10.1017/S0004972725000152 Published online by Cambridge University Press

This implies that

$$\mathcal{G} + \mathcal{G} = \mathbb{F}_p,$$

which, together with $\mathcal{G} \subseteq \mathcal{M}/\mathcal{H} \bmod p$, yields the desired result.

By Lemma 2.1,

$$|\mathcal{D}| \gg \frac{p}{\log^2 p}. \tag{3.5}$$

Let $\mathcal{G}^c = \mathbb{F}_p^* \setminus \mathcal{G}$. Thus, (3.4) is equivalent to $|\mathcal{G}^c| = o(p)$.

By the definition of $\mathcal{G}$, there is no solution to the congruence

$$d \equiv qy \bmod p, \quad d \in \mathcal{D},\ q \leqslant Q,\ y \in \mathcal{G}^c.$$

Hence, using the orthogonality of multiplicative characters and expressing the number of solutions (which is zero) via sums of characters $\chi$ modulo $p$,

$$0 = \sum_{d \in \mathcal{D}} \sum_{q \leqslant Q} \sum_{y \in \mathcal{G}^c} \frac{1}{p-1} \sum_{\chi \bmod p} \chi(d^{-1}qy).$$

Changing the order of summation and separating the term that corresponds to the principal character $\chi = \chi_0$, we derive

$$\pi(Q) \cdot |\mathcal{D}| \cdot |\mathcal{G}^c| \leqslant \sum_{\chi \ne \chi_0} \left| \sum_{q \leqslant Q} \chi(q) \right| \left| \sum_{y \in \mathcal{G}^c} \chi(y) \right| \left| \sum_{d \in \mathcal{D}} \chi(d^{-1}) \right|.$$

Using (2.3) to estimate the sum over $q \leqslant Q$, and then following the standard procedure with an application of the Cauchy–Schwarz inequality, yields

$$\pi(Q) \cdot |\mathcal{D}| \cdot |\mathcal{G}^c| \leqslant \pi(Q) (\log X)^{-1-0.1\varepsilon} T_1^{1/2} T_2^{1/2}, \tag{3.6}$$

where

$$T_1 = \sum_{\chi \bmod p} \left| \sum_{y \in \mathcal{G}^c} \chi(y) \right|^2 = (p-1)|\mathcal{G}^c|$$

and

$$T_2 = \sum_{\chi \bmod p} \left| \sum_{d \in \mathcal{D}} \chi(d^{-1}) \right|^2 = (p-1)|\mathcal{D}|.$$

Therefore, from (3.6),

$$|\mathcal{D}||\mathcal{G}^c| \leqslant (p-1)(\log X)^{-1-0.1\varepsilon} |\mathcal{D}|^{1/2} |\mathcal{G}^c|^{1/2}.$$

Thus,

$$|\mathcal{G}^c| \leqslant \frac{p^2}{|\mathcal{D}|(\log X)^{2+0.2\varepsilon}}.$$

https://doi.org/10.1017/S0004972725000152 Published online by Cambridge University Press

This, together with (3.5), implies that

$$|\mathcal{G}^c| \ll \frac{p}{(\log X)^{0.2\varepsilon}} = o(p),$$

and thus establishes (3.4) and finishes the proof of Theorem 1.2. □

REMARK 3.1. It is well known that, under the generalised Riemann hypothesis (GRH) a version of Lemma 2.3 holds for all moduli (see [8, Equation (13.21)]). Thus, under the GRH, we have a version of Theorem 1.2 that holds for all sufficiently large $p$.

PROOF OF THEOREM 1.3. Let

$$\mathcal{I} = \{L+1, \dots, L+\lfloor\sqrt{8p}\rfloor\} \quad \text{and} \quad \mathcal{J} = \{K+1, \dots, K+\lfloor\sqrt{8p}\rfloor\}.$$

Denote

$$\mathcal{W} = \{m/x \bmod p : m \in \mathcal{I},\ x \in \mathcal{J}\},$$

and let $\mathcal{W}^c = \mathbb{F}_p \setminus \mathcal{W}$. It suffices to prove that $|\mathcal{W}^c| < p/2$. Indeed, in this case, $|\mathcal{W}| > p/2$ and the claim then follows from the pigeonhole principle.

Let $N = \lfloor\sqrt{2p}\rfloor$ and note that $2N \leqslant \lfloor\sqrt{8p}\rfloor$. Clearly, for $t \in \mathcal{W}^c$, there is no solution to the congruence

$$m_1 + m_2 \equiv (x_1 + x_2)t \bmod p,$$

with positive integers $m_1, m_2, x_1, x_2$ satisfying

$$m_1 \in [L+1, L+N], \quad x_1 \in [K+1, K+N], \quad m_2 \leqslant N, \quad x_2 \leqslant N.$$

As in the proof of Theorem 1.1, we write the number of solutions of this congruence (which is zero) in terms of exponential sums and see that

$$0 = \frac{1}{p}\sum_{a=0}^{p-1}\sum_{m_1=L+1}^{L+N}\sum_{m_2=1}^{N}\sum_{x_1=K+1}^{K+N}\sum_{x_2=1}^{N}\sum_{t\in\mathcal{W}^c}\mathbf{e}_p(a(m_1+m_2-(x_1+x_2)t)).$$

Separating the term corresponding to $a = 0$ and following the standard procedure, we derive

$$N^4|\mathcal{W}^c| \leqslant \sum_{a=1}^{p-1} S_1(a)S_2(a)\Big(\sum_{t\in\mathcal{W}^c} T_1(at)T_2(at)\Big), \tag{3.7}$$

where

$$S_1(a) = \Big|\sum_{m_1=L+1}^{L+N}\mathbf{e}_p(am_1)\Big|, \quad S_2 = \Big|\sum_{m_2=1}^{N} e_p(am_2\Big|$$

and

$$T_1(at) = \Big|\sum_{x_1=K+1}^{K+N}\mathbf{e}_p(-atx_1)\Big|, \quad T_2(at) = \Big|\sum_{x_2=1}^{N}\mathbf{e}_p(-atx_2)\Big|.$$

https://doi.org/10.1017/S0004972725000152 Published online by Cambridge University Press

Now, we observe that

$$\sum_{t\in\mathcal{W}^c} T_1(at)T_2(at) \leqslant \sum_{t=0}^{p-1} T_1(at)T_2(at) = \sum_{t=0}^{p-1} T_1(t)T_2(t).$$

Therefore, applying the Cauchy–Schwarz inequality, we obtain

$$\sum_{t\in\mathcal{W}^c} T_1(at)T_2(at) \leqslant \Big(\sum_{t=0}^{p-1} T_1^2(t)\Big)^{1/2}\Big(\sum_{t=0}^{p-1} T_2^2(t)\Big)^{1/2} = pN.$$

Analogously,

$$\sum_{a=1}^{p-1} S_1(a)S_2(a) = \sum_{a=0}^{p-1} S_1(a)S_2(a) - N^2 \leqslant pN - N^2.$$

Inserting these estimates into (3.7), we derive

$$|\mathcal{W}^c| \leqslant \frac{(p-N)p}{N^2} = \frac{p}{2}\cdot\frac{2p-2N}{N^2}.$$

Since $N^2 + 2N = (N+1)^2 - 1 > 2p - 1$ and $N^2 + 2N \neq 2p$, we see that

$$N^2 > 2p - 2N,$$

which implies that $|\mathcal{W}^c| < p/2$. □

## References


[1] N. Bag and I. E. Shparlinski, 'Bounds of some double exponential sums', *J. Number Theory* **219** (2021), 228–236.

[2] W. Banks and I. E. Shparlinski, 'Congruences with intervals and arbitrary sets', *Arch. Math. (Basel)* **114** (2020), 527–539.

[3] M. Z. Garaev, 'Character sums in short intervals and the multiplication table modulo a prime', *Monatsh. Math.* **148** (2006), 127–138.

[4] M. Z. Garaev and V. C. Garcia, 'The equation $x_1x_2 = x_3x_4 + \lambda$ in fields of prime order and applications', *J. Number Theory* **128** (2008), 2520–2537.

[5] M. Z. Garaev and A. A. Karatsuba, 'The representation of residue classes by products of small integers', *Proc. Edinb. Math. Soc. (2)* **50** (2007), 363–375.

[6] M. Z. Garaev and I. E. Shparlinski, 'On some congruences and exponential sums', *Finite Fields Appl.* **98** (2024), Article no. 102451, 17 pages.

[7] H. Iwaniec and E. Kowalski, *Analytic Number Theory* (American Mathematical Society, Providence, RI, 2004).

[8] H. L. Montgomery and R. C. Vaughan, *Multiplicative Number Theory I: Classical Theory* (Cambridge University Press, Cambridge, 2006).

[9] I. E. Shparlinski, 'Modular hyperbolas', *Jpn. J. Math.* **7** (2012), 235–294.

[10] A. Walfisz, *Weylsche Exponentialsummen in der neueren Zahlentheorie* (B.G. Teubner, Leipzig, 1963).


https://doi.org/10.1017/S0004972725000152 Published online by Cambridge University Press

MOUBARIZ Z. GARAEV, Centro de Ciencias Matemáticas,
Universidad Nacional Autónoma de México, C.P. 58089 Morelia,
Michoacán, México
e-mail: garaev@matmor.unam.mx

JULIO C. PARDO, Centro de Ciencias Matemáticas,
Universidad Nacional Autónoma de México, C.P. 58089 Morelia,
Michoacán, México
e-mail: jcpardo@matmor.unam.mx

IGOR E. SHPARLINSKI, School of Mathematics and Statistics,
University of New South Wales, Sydney, NSW 2052, Australia
e-mail: igor.shparlinski@unsw.edu.au

https://doi.org/10.1017/S0004972725000152 Published online by Cambridge University Press