Double exponential sums and congruences with intervals and exponential functions modulo a prime

M. Z. Garaev

Abstract

Let \( p \) be a large prime number and \( g \) be any integer of multiplicative order \( T \) modulo \( p \). We obtain a new estimate of the double exponential sum

\[
S = \left| \sum_{n \in \mathcal{N}} \sum_{m \in \mathcal{M}} e_p(ang^m) \right|, \quad \gcd(a, p) = 1,
\]

where \( \mathcal{N} \) and \( \mathcal{M} \) are intervals of consecutive integers with \( |\mathcal{N}| = N \) and \( |\mathcal{M}| = M < T \) elements. One representative example is the following consequence of the main result: if \( N = M \approx p^{1/3} \), then \( |S| < N^{2-1/8+o(1)} \). We then apply our estimate to obtain new results on additive congruences involving intervals and exponential functions.

Mathematical Subject Classification: 11L07, 11L79

Keywords: exponential sums, exponential functions, congruences

1 Introduction

Let \( p \) be a large prime number, \( g \) be an integer with \( \gcd(g, p) = 1 \). Denote by \( T \) the multiplicative order of \( g \) modulo \( p \). Let

\[
\mathcal{N} = \{u + 1, \ldots, u + N\} \quad \text{and} \quad \mathcal{M} = \{v + 1, \ldots, v + M\}
\]
be two intervals of consecutive integers with
\[ |\mathcal{N}| = N \leq p \quad \text{and} \quad |\mathcal{M}| = M \leq T. \]

In the present paper we are concerned with the problem of upper bound estimates for the double exponential sum
\[ S_{a,p,g}(\vec{\alpha}, \vec{\beta}; \mathcal{N}, \mathcal{M}) = \sum_{n \in \mathcal{N}} \sum_{m \in \mathcal{M}} \alpha_n \beta_m e_p(angm), \quad \gcd(a, p) = 1, \]
where \( \alpha_n \) and \( \beta_m \) are complex coefficients with \( |\alpha_n|, |\beta_m| \leq 1 \), and \( e_p(z) = e^{2\pi iz/p} \). Here, for a negative integer \( -k \), the number \( g^{-k} \) is defined to be an integer with \( g^{-k} g^k \equiv 1 \bmod p \).

In the special case \( \alpha_n = \beta_m = 1 \), the sum \( S_{a,p}(\vec{\alpha}, \vec{\beta}; \mathcal{N}, \mathcal{M}) \) has appeared in the work of Bourgain [1], where he has estimated it for very short intervals \( \mathcal{N} \) and \( \mathcal{M} \).

When \( M > p^{1/2} \), one can apply classical estimates of single sums with exponential functions which would lead to nontrivial bounds for \( S_{a,p}(\vec{\alpha}, \vec{\beta}; \mathcal{N}, \mathcal{M}) \) with reasonably good power savings. On the other hand, from the celebrated work of Bourgain, Glibichuk and Konyagin [2], it follows that for any \( \varepsilon > 0 \) there exists \( \delta > 0 \) such that if \( N > p^{\varepsilon}, M > p^{\varepsilon} \), then
\[ |S_{a,p,g}(\vec{\alpha}, \vec{\beta}; \mathcal{N}, \mathcal{M})| < NMp^{-\delta}. \]

However, the value of \( \delta \) in terms of \( \varepsilon \) is very small, and, in particular, it does not give good savings for medium sized intervals.

Recently, Shparlinski and Yau [10] obtained a number of new explicit estimates on \( S_{a,p}(\vec{\alpha}, \vec{\beta}; \mathcal{N}, \mathcal{M}) \). One of the features of [10] is that some of the estimates given there work well for certain ranges of \( N \) and \( M \) below the critical value \( p^{1/2} \). They also noted, that the work of Roche-Newton, Rudnev and Shkredov [9] leads to certain nontrivial bounds in the range \( M > p^{1/3+c} \), for any positive constant \( c \). Nevertheless, in some very interesting cases (for example, if \( N, M < p^{1/3} \)) these estimates become trivial and one naturally asks what can be done in these cases.
Note that by the Cauchy-Schwarz inequality,

\[ |S_{\alpha, \beta}(\alpha, \beta; N, M)|^2 \leq M \sum_{m \in M} \left| \sum_{n \in N} \alpha_n e_p(\text{ang } m) \right|^2 \]

\[ \leq M \sum_{n_1 \in N} \sum_{n_2 \in N} \left| \sum_{m \in M} e_p(a(n_1 - n_2)g^m) \right| \]

\[ \ll MN \sum_{0 \leq n \leq N} \left| \sum_{m \in M} e_p(\text{ang } m) \right|. \]

Thus, in what follows we shall concentrate our attention on the sum

\[ S_{\alpha, \beta}(N, M) = \sum_{n \in N} \left| \sum_{m \in M} e_p(\text{ang } m) \right|. \]

In the present paper we obtain a new explicit estimate for \( S_{\alpha, \beta}(N, M) \) which, in particular, is nontrivial in the range \( N = M > p^{2/7} + c \), for any constant \( c > 0 \). Then we apply our bound to obtain new results on congruences involving intervals and exponential functions.

**Notations.** In what follows, we use the notation \( A \lesssim B \) to mean that \( |A| < BP^ \epsilon(1) \), or equivalently, for any \( \epsilon > 0 \) there is a constant \( c = c(\epsilon) \) such that \( |A| < CB^\epsilon \). Given two sets \( X \) and \( Y \) their product-set \( X \cdot Y \) and the sum-set \( X + Y \) are defined by

\[ X \cdot Y = \{ ab; \ a \in X, b \in Y \}, \quad X + Y = \{ a + b; \ a \in X, b \in Y \}. \]

As usual, for a positive integer \( k \), the \( k \)-fold sum-set \( kX \) is defined by

\[ kX = \{ a_1 + \ldots + a_k; \ a_k \in X \}. \]

The notation \( |X| \) stands for the cardinality of the set \( X \).

## 2 Our results

**Theorem 1.** Let \( M < p^{2/3} \). Then

\[ S_{\alpha, \beta}(N, M) = \sum_{n \in N} \left| \sum_{m \in M} e_p(\text{ang } m) \right| = NM\Delta, \]
where
\[ \Delta \lesssim \frac{1}{M^{3/8}} + \left( \frac{p}{NM^{5/2}} \right)^{1/4} + \left( \frac{p}{N^{4/3}M^{7/3}} \right)^{3/16} + \left( \frac{p}{N^{2}M^{3/2}} \right)^{1/4}. \]

In particular, if \( N = M \approx p^{1/3} \), then \( S_{a,p,g}(N, M) \lesssim N^{2-1/8} \).

It is well-known that nontrivial exponential sum estimates is a basic tool in investigation of additive problems. Theorem 1 has the following application.

**Theorem 2.** Let \( \varepsilon > 0 \) be a fixed small positive constant and let \( N_i \) and \( M_i \) be intervals of consecutive integers with \( |N_i| = N_i \) and \( |M_i| = M_i \), satisfying
\[ p \geq N_i > p^{1/3 + \varepsilon}, \quad T \geq M_i > p^{1/3 + \varepsilon}, \quad i = 1, 2, \ldots, 10. \]
Then for any integer \( \lambda \) the number \( J_{10} \) of solutions of the congruence
\[ x_1g^{y_1} + \ldots + x_{10}g^{y_{10}} \equiv \lambda \pmod{p}, \quad x_i \in N_i, y_i \in M_i, \]
satisfies
\[ J_{10} = \prod_{i=1}^{10} \frac{(N_iM_i)}{p} \left( 1 + O(p^{-\delta}) \right), \quad \delta = \delta(\varepsilon) > 0. \]

Theorem 2 provides with the asymptotic formula for the number of solutions of the congruence. But if one is interested only on the question of solubility, then our intermediate result that we obtain in the course of the proof of Theorem 1 combined with the result of Glibichuk [7] and Roche-Newton, Rudnev and Shkredov [9], leads to the following results.

**Theorem 3.** Let \( \varepsilon > 0 \) be a fixed small positive constant and let
\[ N > p^{1/3 + \varepsilon}, \quad M > p^{1/3 + \varepsilon}. \]
Then any integer \( \lambda \) modulo \( p \) can be represented in the form
\[ x_1g^{y_1} + \ldots + x_8g^{y_8} \equiv \lambda \pmod{p}, \]
for some \( x_i \in \mathcal{N} \) and \( y_i \in \mathcal{M} \).

**Theorem 4.** Let \( \varepsilon > 0 \) be a fixed small positive constant and let
\[ N > p^{2/7 + \varepsilon}, \quad M > p^{2/7 + \varepsilon}. \]
Then any integer \( \lambda \) modulo \( p \) can be written in the form
\[ x_1g^{y_1} + \ldots + x_{16}g^{y_{16}} \equiv \lambda \pmod{p}, \]
for some \( x_i \in \mathcal{N} \) and \( y_i \in \mathcal{M} \).
3 Lemmas

The following lemma is contained in [4] under the additional restriction $|\mathcal{U}| < p^{2/5}$. This restriction has been removed in [6]. Note that when $\mathcal{U}$ is a subgroup of size $|\mathcal{U}| > p^{1/2}$, the statement follows from [3, Theorem 1].

Lemma 1. Let $H$ be a positive integer and let $\mathcal{U} \subset \mathbb{F}_p^*$ be such that $|\mathcal{U} \cdot \mathcal{U}| < 10|\mathcal{U}|$.

Then the number $J_0$ of solutions of the congruence

$$xr \equiv x_1r_1 \pmod{p}; \quad x, x_1 \in \mathbb{N}, \quad x, x_1 \leq H, \quad r, r_1 \in \mathcal{U}$$

satisfies

$$J_0 \lesssim |\mathcal{U}|H + \frac{|\mathcal{U}|^2H^2}{p} + \frac{|\mathcal{U}|^{7/4}H}{p^{1/4}}.$$

Lemma 2. The number $J$ of solutions of the congruence

$$xg^y \equiv x_1g^{y_1} \pmod{p}; \quad x, x_1 \in \mathcal{N}, \quad y, y_1 \in \mathcal{M} \quad (1)$$

satisfies

$$J \lesssim M^2 + MN + \frac{M^2N^2}{p} + \frac{M^{7/4}N}{p^{1/4}}.$$

Proof. Given $y, y_1 \in \mathcal{M}$, denote by $J(y, y_1)$ the number of solutions of (1) in variables $x, x_1 \in \mathcal{N}$. Then

$$J = \sum_{y, y_1} J(y, y_1).$$

We can restrict the summation to those $y, y_1 \in \mathcal{M}$ for which $J(y, y_1) \neq 0$. Thus, there is a pair $x_0, x'_0 \in \mathcal{N}$ depending on $y, y_1$ such that

$$(x - x_0)g^y \equiv (x_1 - x'_0)g^{y_1} \pmod{p}.$$

Note that $|x - x_0| \leq N$, $|x_1 - x'_0| \leq N$. Hence,

$$J(y, y_1) \leq J_0(y, y_1),$$

where $J_0(y, y_1)$ is the number of solutions of the congruence

$$xg^y \equiv x_1g^{y_1} \pmod{p}, \quad |x|, |x_1| \leq N.$$
Thus,

\[ J \leq \sum_{y,y_1} J_0(y, y_1) = J'_0, \]

where \( J'_0 \) is the number of solutions of the congruence

\[ x g^y \equiv x_1 g^{y_1} \pmod{p}, \quad |x|, |x_1| \leq N, \quad y, y_1 \in \mathcal{M}. \]

If \( x = 0 \), then \( x_1 = 0 \) and this case contributes to \( J'_0 \) the quantity \( M^2 \). If \( x \neq 0 \), then \( x_1 \neq 0 \). In this case we apply the Cauchy-Schwarz inequality to symmetrize the equation, and then the desired result follows from application of Lemma 1 to the set \( U = \{ g^y \pmod{p}, y \in \mathcal{M} \} \).

\[ \square \]

**Corollary 1.** The following bound holds:

\[ \left| \{ x g^y \pmod{p}, x \in \mathcal{N}, y \in \mathcal{M} \} \right| \gtrsim \min \{ N^2, NM, p, p^{1/4}M^{1/4}N \}. \]

We need the following result of Roche-Newton, Rudnev and Shkredov [9].

**Lemma 3.** Let \( M < p^{2/3} \). Then the number \( E_+(g^M) \) of solutions of the congruence

\[ g^{m_1} + g^{m_2} \equiv g^{m_3} + g^{m_4} \pmod{p}, \quad m_1, m_2, m_3, m_4 \in \mathcal{M}, \]

satisfies \( E_+(g^M) \ll M^{5/2} \).

We also need the following result of Glibichuk [7].

**Lemma 4.** Let \( \mathcal{X}, \mathcal{Y} \subset \mathbb{F}_p \) be such that \( |\mathcal{X}||\mathcal{Y}| > 2p \). Then \( 8(\mathcal{X} \cdot \mathcal{Y}) = \mathbb{F}_p \).

### 4 Proof of Theorem 1

Let \( \gamma_n \) be complex numbers such that \( |\gamma_n| = 1 \) and

\[ \left| \sum_{m \in \mathcal{M}} e_p(\text{ang} \, m) \right| = \gamma_n \sum_{m \in \mathcal{M}} e_p(\text{ang} \, m) \]

We have that

\[ S_{n,p,g}(\mathcal{N}, \mathcal{M}) = \sum_{n \in \mathcal{N}} \left| \sum_{m \in \mathcal{M}} e_p(\text{ang} \, m) \right| = \sum_{n \in \mathcal{N}} \sum_{m \in \mathcal{M}} \gamma_n e_p(\text{ang} \, m). \]
We recall that \( \mathcal{M} = \{v + 1, \ldots, v + M\} \). As in the work of Friedlander and Iwaniec [5], we introduce the function

\[
\begin{align*}
f(x) &= \begin{cases} 
0 & \text{if } x \leq v; \\
x - v & \text{if } v \leq x \leq v + 1; \\
1 & \text{if } v + 1 \leq x \leq v + M; \\
v + M + 1 - x & \text{if } v + M \leq x \leq v + M + 1; \\
0 & \text{if } x \geq v + M + 1.
\end{cases}
\end{align*}
\]

Let \( F \) denote the Fourier transform of \( f \),

\[
F(y) = \int_{-\infty}^{\infty} f(x) e^{-2\pi i y x} \, dx.
\]

Then integrating by part it follows that \( |F(y)| \leq \min\{M, |\pi y|^{-1}, |\pi y|^{-2}\} \). Hence,

\[
\int_{-\infty}^{\infty} |F(y)| \, dy \leq \int_{0}^{1/M} M \, dy + \int_{1/M}^{1} |\pi y|^{-1} \, dy + \int_{1}^{\infty} |\pi y|^{-2} \, dy \ll \log M. \tag{2}
\]

Therefore, since \( f(x) = \int_{-\infty}^{\infty} F(y) e^{2\pi i y x} \, dy \), we get that

\[
S_{a,p,g}(\mathcal{N}, \mathcal{M}) = \sum_{n \in \mathcal{N}} \sum_{m \in \mathcal{M}} \gamma_n e_p(\text{ang}^m) = \\
\sum_{n \in \mathcal{N}} \sum_{m = -\infty}^{\infty} \gamma_n f(m) e_p(\text{ang}^m) = \\
\frac{1}{M} \sum_{k=1}^{M} \sum_{n \in \mathcal{N}} \sum_{m = v-M}^{v+M-1} \gamma_n f(k + m) e_p(\text{ang}^k \text{g}^m) = \\
\frac{1}{M} \int_{-\infty}^{\infty} F(y) \left( \sum_{k=1}^{M} \sum_{n \in \mathcal{N}} \sum_{m = v-M}^{v+M-1} \gamma_n e^{2\pi i (k+m) y} e_p(\text{ang}^k \text{g}^m) \right) \, dy.
\]

Hence, in view of (2), for some \( y \in \mathbb{R} \) we have that

\[
S_{a,p,g}(\mathcal{N}, \mathcal{M}) \lesssim \frac{1}{M} \int_{-\infty}^{\infty} F(y) \left( \sum_{k=1}^{M} \sum_{n \in \mathcal{N}} \sum_{m = v-M}^{v+M-1} \gamma_n \delta_k \delta_m e_p(\text{ang}^k \text{g}^m) \right) \, dy,
\]

where \( \delta_j = e^{2\pi i j y} \). Thus,

\[
S_{a,p,g}(\mathcal{N}, \mathcal{M}) \lesssim \frac{W}{M}, \tag{3}
\]
where

\[ W = \sum_{k=1}^{M} \sum_{n \in \mathcal{N}} \left| \sum_{m = v - M}^{v - M + 1} \delta_m e_p(\lambda n^k g^m) \right|. \]

Applying the Cauchy-Schwarz inequality, we obtain that

\[ W^2 \leq N M \sum_{k=1}^{M} \sum_{n \in \mathcal{N}} \left| \sum_{m = v - M}^{v - M + 1} \delta_m e_p(\lambda n^k g^m) \right|^2 = \]

\[ N M \sum_{k=1}^{M} \sum_{n \in \mathcal{N}} \sum_{m = v - M}^{v - M + 1} \sum_{m = v - M}^{v - M + 1} \delta_m e_p(\lambda n^k (g^{m_1} - g^{m_2})) \leq \]

Thus, if we denote by \( I_\lambda \) the number of solutions of the congruence

\[ g^{m_1} - g^{m_2} \equiv \lambda \pmod{p}, \quad v - M \leq m_1, m_2 \leq v + M - 1, \]

we get that

\[ W^2 \leq N M \sum_{\lambda=0}^{p-1} I_\lambda \left| \sum_{k=1}^{M} \sum_{n \in \mathcal{N}} e_p(\lambda n^k) \right|. \]

Applying Cauchy-Schwarz inequality again, we get that

\[ W^4 \leq N^2 M^2 \left( \sum_{\lambda=0}^{p-1} I_\lambda^2 \right) \sum_{\lambda=0}^{p-1} \left| \sum_{k=1}^{M} \sum_{n \in \mathcal{N}} e_p(\lambda n^k) \right|^2 \]

The quantity \( \sum_{\lambda=0}^{p-1} I_\lambda^2 \) is equal to the number of solutions of the congruence

\[ g^{m_1} - g^{m_2} \equiv g^{m_3} - g^{m_4} \pmod{p}, \quad v - M \leq m_1, m_2, m_3, m_4 \leq v + M - 1. \]

It then follows from Lemma 3 that

\[ \sum_{\lambda=0}^{p-1} I_\lambda^2 \ll M^{5/2}. \] (5)

Furthermore,

\[ \sum_{\lambda=0}^{p-1} \left| \sum_{k=1}^{M} \sum_{n \in \mathcal{N}} e_p(\lambda n^k) \right|^2 = p J, \]
where \( J \) is the number of solutions of the congruence
\[
g^k n \equiv n_1 g^{k_1} \pmod{p}, \quad 1 \leq n, n_1 \leq N, \quad 1 \leq k, k_1 \leq M.
\]

Applying Lemma 2, we get that
\[
\sum_{\lambda=0}^{p-1} \left| \sum_{k=1}^{M} \sum_{n \in N} e_p(a\lambda ng^k) \right|^2 \lesssim p \left( M^2 + MN + \frac{M^2 N^2}{p} + \frac{M^{7/4} N}{p^{1/4}} \right).
\]

Inserting this and (5) into (4), we obtain that
\[
\frac{W^4}{M^4} \lesssim p N^2 M^{5/2} + p N^3 M^{3/2} + N^4 M^{5/2} + N^3 M^{9/4} p^{3/4}.
\]

Thus,
\[
\frac{W}{M} \lesssim N M \left( \frac{1}{M^{3/8}} + \left( \frac{p}{N M^{5/2}} \right)^{1/4} + \left( \frac{p}{N^{4/3} M^{7/3}} \right)^{3/16} + \left( \frac{p}{N^2 M^{3/2}} \right)^{1/4} \right).
\]

Substituting this in (3), we conclude the proof.

5 Proofs of Theorems 2, 3 and 4

We start with the proof of Theorem 2. First of all we note that if \( M > p^{2/3} \), then from the classical bounds of exponential sums with exponential functions, we know that
\[
\max_{\gcd(a,p)=1} \left| \sum_{m \in M} e_p(a g^m) \right| \lesssim p^{1/2}.
\]

Hence, in this case we have that
\[
\left| \sum_{n \in N} \sum_{m \in M} e_p(ang^m) \right| \lesssim M + N p^{1/2 + o(1)} \lesssim N M p^{-1/6}.
\]

If \( M < p^{2/3} \), then by Theorem 1 we get that
\[
\left| \sum_{n \in N} \sum_{m \in M} e_p(ang^m) \right| < \frac{N M}{p^{1/24 + \delta_0}}, \quad \delta_0 = \delta_0(\varepsilon) > 0.
\]
Thus, the estimate (6) holds. Expressing $J_{10}$ in terms of exponential sums, we get

$$J_{10} = \frac{1}{p} \sum_{a=0}^{p-1} \prod_{j=1}^{10} \left( \sum_{x \in \mathcal{N}_j} \sum_{y \in \mathcal{M}_j} e_p(axg^y) \right) e_p(-a\lambda).$$

Separating the term that corresponds to $a = 0$ and then using (6), we obtain that

$$|J - \prod_{j=1}^{10} (N_j M_j) / p| < \prod_{j=1}^{8} (N_j M_j)^{1/3 + 8\delta_0} R \tag{7}$$

where

$$R = \frac{1}{p} \sum_{a=0}^{p-1} \left| \sum_{x \in \mathcal{N}_9} \sum_{y \in \mathcal{M}_9} e_p(axg^y) \right| \left| \sum_{x \in \mathcal{N}_{10}} \sum_{y \in \mathcal{M}_{10}} e_p(axg^y) \right|.$$

Applying the Cauchy-Schwarz inequality, we get that

$$R \leq \sqrt{\frac{1}{p} \sum_{a=0}^{p-1} \left| \sum_{x \in \mathcal{N}_9} \sum_{y \in \mathcal{M}_9} e_p(axg^y) \right|^2} \times \sqrt{\frac{1}{p} \sum_{a=0}^{p-1} \left| \sum_{x \in \mathcal{N}_{10}} \sum_{y \in \mathcal{M}_{10}} e_p(axg^y) \right|^2}.$$

Furthermore,

$$\frac{1}{p} \sum_{a=0}^{p-1} \left| \sum_{x \in \mathcal{N}_j} \sum_{y \in \mathcal{M}_j} e_p(axg^y) \right|^2 = T_j,$$

where $T_j$ is the number of solutions of the congruence

$$xg^y \equiv x_1g^{y_1} \pmod{p}, \quad x, x_1 \in \mathcal{N}_j, \quad y, y_1 \in \mathcal{M}_j.$$

Thus,

$$R \leq \sqrt{T_9 T_{10}}.$$

From Lemma 2 it follows that

$$T_j \lesssim N_j^2 M_j^2 \left( \frac{1}{N_j^2} + \frac{1}{N_j M_j} + \frac{1}{p} + \frac{1}{p^{1/4} M_j^{1/4} N_j} \right) < \frac{N_j^2 M_j^2}{p^{2/3 + 1.1\varepsilon}}.$$

Hence,

$$R \leq \sqrt{T_9 T_{10}} \leq \frac{N_9 M_9 N_{10} M_{10}}{p^{2/3 + \varepsilon}}.$$
Inserting this into (7), we get that

\[ \left| j - \frac{\prod_{j=1}^{10} (N_j M_j)}{p} \right| < \frac{\prod_{j=1}^{10} (N_j M_j)}{p} p^{-\delta}, \quad \delta = \delta(\varepsilon) > 0. \]

This finishes the proof of Theorem 2.

In order to prove Theorem 3 let \( M_1 = \lfloor 0.5 M \rfloor \) and define the sets \( \mathcal{X} \) and \( \mathcal{Y} \) as follows:

\[ \mathcal{X} = \{ xg^y \pmod{p}, x \in \mathcal{N}, y \in \mathcal{M}_1 \}, \quad \mathcal{Y} = \{ g^y \pmod{p}, 1 \leq y \leq M_1 \}, \]

where \( \mathcal{M}_1 = \{ v + 1, v + 2, \ldots, v + M_1 \} \). By Corollary 11, we have

\[ |\mathcal{X}| |\mathcal{Y}| \geq p^{2/3} p^{1/3 + 0.5\varepsilon} > 2p. \]

Therefore, by Lemma 4, \( 8(\mathcal{X} \cdot \mathcal{Y}) = \mathbb{F}_p \). Since

\[ \mathcal{X} \mathcal{Y} \subset \{ xg^y \pmod{p}, x \in \mathcal{N}, y \in \mathcal{M} \}, \]

the claim follows.

The proof of Theorem 4 is similar. We can assume that \( M < p^{2/3} \). Define \( M_1, \mathcal{M}_1 \) and \( \mathcal{X} \) as in the proof of Theorem 3 and define \( \mathcal{Y} \) by

\[ \mathcal{Y} = \{ g^{y_1} + g^{y_2} \pmod{p}, 1 \leq y_1, y_2 \leq M_1 \}. \]

From Corollary 2 we have that \( |\mathcal{X}| \geq p^{4/7 + \varepsilon} \). Also from Lemma 3 and the relationship between the number of solutions and the cardinality, it follows that \( |\mathcal{Y}| \gg M^{3/2} \). Hence,

\[ |\mathcal{X}| |\mathcal{Y}| \geq p^{4/7 + \varepsilon} p^{3/7} > 2p. \]

Hence, by Lemma 4, \( 8(\mathcal{X} \cdot \mathcal{Y}) = \mathbb{F}_p \). Since

\[ \mathcal{X} \mathcal{Y} \subset \{ x_1 g^{y_1} + x_2 g^{y_2} \pmod{p}, x_1, x_2 \in \mathcal{N}, y_1, y_2 \in \mathcal{M} \}, \]

the result follows.

References

[1] J. Bourgain, ‘On the distribution of the residues of small multiplicative subgroups of \( \mathbb{F}_p \), Israel J. Math., 172 (2009), 61–74.
[2] J. Bourgain, A. A. Glibichuk and S. V. Konyagin, ‘Estimates for the number of sums and products and for exponential sums in fields of prime order’, J. London Math. Soc., 73 (2006), no. 2, 380–398.

[3] J. Bourgain, S. V. Konyagin and I. E. Shparlinski, ‘Product sets of rationals, multiplicative translates of subgroups in residue rings, and fixed points of the discrete logarithm’, Int. Math. Res. Not., (2008), Art. ID rnn 090, 29 pp.

[4] J. Cilleruelo and M. Z. Garaev, ‘Congruences involving product of intervals and sets with small multiplicative doubling modulo a prime and applications’, Math. Proc. Cambridge Philos. Soc., 160 (2016), 477–494.

[5] J. Friedlander and H. Iwaniec, ‘Estimates for character sums’, Proc. Amer. Math. Soc., 119 (1993), 365–372.

[6] M. Z. Garaev, ‘On distribution of elements of subgroups in arithmetic progressions modulo a prime’, Preprint, (2017).

[7] A. A. Glibichuk, ‘Combinatorial properties of sets of residues modulo a prime and the Erdős-Graham problem’, Mat. Zametki, 79 (2006), 384–395; translation in: Math. Notes, 79 (2006), 356–365.

[8] S. V. Konyagin and I. E. Shparlinski, Character sums with exponential functions and their applications, Cambridge Univ. Press, Cambridge, 1999.

[9] O. Roche-Newton, M. Rudnev and I. D. Shkredov, ‘New sum-product type estimates over finite fields’, Adv. Math., 293 (2016), 589–605.

[10] I. E. Shparlinski and K. H. Yau, ‘Double exponential sums with exponential functions’, Int. J. Number Theory, 13 (2017), no. 10, 2531–2543.

Address of the author:

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