On a symmetric congruence and its applications

M. Z. Garaev
Instituto de Matemáticas, UNAM
Campus Morelia, Apartado Postal 61-3 (Xangari)
C.P. 58089, Morelia, Michoacán, México
garaev@matmor.unam.mx

A. A. Karatsuba
Steklov Institute of Mathematics
Russian Academy of Sciences
GSP-1, ul. Gubkina 8
Moscow, Russia
karatsuba@mi.ras.ru

Abstract
For a large integer $m$, we obtain an asymptotic formula for the number of solutions of a certain congruence modulo $m$ with four variables, where the variables belong to special sets of residue classes modulo $m$. This formula are applied to obtain a new bound for a double trigonometric sum with an exponential function and new information on the exceptional set of the multiplication table problem in a residue ring modulo $m$.

1 Introduction
Throughout the paper the implied constants in the Landau ‘$O$’ and ‘$o$’ symbols as well as in the Vinogradov symbols ‘$\ll$’ and ‘$\gg$’ may depend on the
small positive quantity $\varepsilon$. By $p$ and $q$ we will always denote prime numbers.

Let $m$ be an integer parameter, $V$ be any subset of prime numbers coprime to $m$ and not exceeding $m^{1/2}$, and let $S$ and $L$ be any integers with $0 < L \leq m$. In this paper we obtain an asymptotic formula for the number of solutions of the congruence

$$v_1 y_1 \equiv v_2 y_2 \pmod{m}, \quad v_1, v_2 \in V, \quad S + 1 \leq y_1, y_2 \leq S + L$$

and give its applications.

Below $|V|$ stands for the number of elements in $V$. By $\tau(m)$ we denote the classical divisor function.

**Theorem 1.** The following asymptotic formula holds:

$$J = \frac{|V|^2 L^2}{m} + |V|L - \frac{|V|L^2}{m} + O\left(\frac{m^2 \log^2 m}{\phi(m)}\right),$$

where $\phi(m)$ is the Euler function.

Theorem 1 finds its application in estimating of double trigonometric sums with an exponential function. For a positive integer $m$ we denote by $\mathbb{Z}_m = \{0, 1, ..., m - 1\}$ the residue ring modulo $m$. Let $p$ be a large prime number, $T$ be a divisor of $p - 1$, $\lambda$ be an element of $\mathbb{Z}_p$ of multiplicative order $T$, i.e. $\lambda = g^{(p - 1)/T}$ for some primitive root $g$ modulo $p$, $\gamma(n)$ be any complex coefficients with $|\gamma(n)| \leq 1$. Denote

$$e_m(z) = \exp(2\pi iz/m).$$

**Theorem 2.** Let $a$ be any integer coprime to $m$. For any integers $K$ and $N$ with

$$0 < K + 1 \leq K + N \leq p - 1, \quad N \geq Tp^{1/2}(\log p)^3$$

and any set $X \subset \mathbb{Z}_{p - 1}$, the inequality

$$\sum_{x \in X} \left| \sum_{y=K+1}^{K+N} \gamma(y)e_p(a\lambda^{xy}) \right| \ll \frac{|X|^{1/2}N^{3/4}p_{\mathbb{Z}}^{7/4} + o(1)}{T^{1/4}}.$$

holds, where $|X|$ denotes the cardinality of the set $X$. 
Corollary 3. Let \( a \) be any integer coprime to \( m \). For any integers \( K, N, L, M \) with
\[
0 < K + 1 \leq K + N \leq p - 1, \quad 0 < L + 1 \leq L + M \leq p - 1
\]
and any coefficients \( \alpha_x \) and \( \beta_y \) with \( |\alpha_x| \leq 1, |\beta_y| \leq 1 \), the following inequality holds:
\[
\left| \sum_{x=L+1}^{L+M} \sum_{y=K+1}^{K+N} \alpha_x \beta_y e_p(a g^{xy}) \right| \ll (N M)^{5/8} p^{5/8+o(1)}.
\]

This estimate is nontrivial when \( N \geq M \geq p^{5/6+\varepsilon} \). For more information on trigonometric sums with an exponential function and their applications, see [1]-[5] and therein references.

To prove Corollary 3 we observe that the statement is trivial if \( N \leq p^{2/3} \) or if \( M \leq p^{2/3} \). Assuming \( \min\{N, M\} > p^{2/3} \), from Theorem 2 we derive,
\[
\left| \sum_{x=L+1}^{L+M} \sum_{y=K+1}^{K+N} \alpha_x \beta_y e_p(a g^{xy}) \right| \ll \sum_{x=L+1}^{L+M} \sum_{y=K+1}^{K+N} \beta_y e_p(a g^{xy}) \ll M^{1/2} N^{3/4} p^{5/8+o(1)},
\]
\[
\left| \sum_{x=L+1}^{L+M} \sum_{y=K+1}^{K+N} \alpha_x \beta_y e_p(a g^{xy}) \right| \ll \sum_{y=K+1}^{K+N} \sum_{x=L+1}^{L+M} \alpha_x e_p(a g^{xy}) \ll N^{1/2} M^{3/4} p^{5/8+o(1)}.
\]

The result now follows.

In passing, we remark that Theorem 2 and Corollary 3 remain true if \( e_p(a g^{xy}) \) is replaced by \( \chi(g^{xy} + a) \), where \( \chi \) is any nonprincipal character modulo \( p \).

Theorem 1 also finds its application in the problem of multiplication of intervals in a residue ring modulo \( m \).

Corollary 4. For any fixed \( \varepsilon > 0 \) the set
\[
\{ xy \pmod{m} : 1 \leq x \leq m^{1/2}, \quad S + 1 \leq y \leq S + m^{1/2}(\log m)^{2+\varepsilon} \}
\]
contains \( (1 + O((\log m)^{-\varepsilon}))m \) residue classes modulo \( m \).

The classical conjecture claims that for any prime number \( p \) any nonzero residue class modulo \( p \) can be represented in the form \( xy \pmod{p} \), where \( 1 \leq x, y \leq p^{1/2+o(1)} \). A weaker version of this conjecture has been stated
in [6], namely, for any prime $p$ there are $(1 + o(1))p$ residue classes modulo $p$ of the form $xy \pmod{p}$ with $1 \leq x, y \leq p^{1/2+o(1)}$. Furthermore, in [6] it has been proved that for almost all primes $p$ almost all residue classes modulo $p$ are representable in the form $xy \pmod{p}$ with $1 \leq x, y \leq p^{1/2}(\log p)^{1.087}$. The following consequence of Corollary 4 confirms the validity of the weaker version of the classical conjecture and essentially improves one of our results from [8].

**Corollary 5.** For any fixed $\varepsilon > 0$ and any prime number $p$ the set
\[
\{ xy \pmod{p} : 1 \leq x, y \leq p^{1/2}(\log p)^{2+\varepsilon}\}
\]
contains $(1 + o(1))p$ residue classes modulo $p$.

The method of the proof of Theorem 1 combined with an argument similar to that of [7] allows to improve the exponent of the logarithmic factor in Corollaries 4 and 5. More precisely, the following statement takes place.

**Theorem 6.** Let $\Delta = \Delta(m) \to \infty$ as $m \to \infty$. Then the set
\[
\{ qy \pmod{m} : 1 \leq q \leq m^{1/2}, \ S+1 \leq y \leq S + \Delta m^{1/2} \sqrt{m/\phi(m)} \log m \}
\]
contains $(1 + O(\Delta^{-1}))m$ residue classes modulo $m$.

In particular we have

**Corollary 7.** Let $\Delta = \Delta(p) \to \infty$ as $p \to \infty$. Then the set
\[
\{ qy \pmod{p} : 1 \leq q \leq p^{1/2}, \ 1 \leq y \leq \Delta p^{1/2} \log p \}
\]
contains $(1 + O(\Delta^{-1}))p$ residue classes modulo $p$.

Since there are $O(p^{1/2}(\log p)^{-1})$ primes not exceeding $p^{1/2}$, we see that the set
\[
\{ qy : 1 \leq x \leq p^{1/2}, \ S+1 \leq y \leq S + \Delta p^{1/2} \log p \}
\]
contains only $O(p\Delta)$ integers. This shows that the ranges of variables in Theorem 4 and Corollary 7 are sufficiently sharp.

We will also prove the corresponding result for the ratio of intervals modulo a prime which improves one of the results of [6].
Theorem 8. Let $\Delta = \Delta(p) \to \infty$ as $p \to \infty$. Then the set
\[
\{ xy^{-1} \pmod{p} : \quad N + 1 \leq x \leq N + \Delta p^{1/2}, \quad S + 1 \leq y \leq S + \Delta p^{1/2} \}
\]
contains $(1 + O(\Delta^{-2}))p$ residue classes modulo $p$.

Note however, that when $N = S = 0$ and $\Delta < p^{1/2}/2$, the set described in Theorem 8 misses $\gg p^{1/2} \Delta^{-1}$ reside classes modulo $p$, see [6]. For the detailed description on the multiplication table problem modulo a prime, see [6] and also [8].

The proofs of the results of [6] and [8] are based on estimates of multiplicative character sums. The approach we use here is based on trigonometric sums.

2 Proof of Theorem 1

Recall that $J$ denotes the number of solutions to the congruence
\[
v_1 y_1 \equiv v_2 y_2 \pmod{m}, \quad v_1, v_2 \in \mathcal{V}, \quad S + 1 \leq y_1, y_2 \leq S + L.
\]

We express $J$ in terms of trigonometric sums. Since
\[
v_1 v_2^{-1} y_1 \equiv y_2 \pmod{m},
\]
then
\[
J = \frac{1}{m} \sum_{a=0}^{m-1} \sum_{v_1 \in \mathcal{V}} \sum_{v_2 \in \mathcal{V}} \sum_{y_1 \in I} \sum_{y_2 \in I} e_m(a(v_1 v_2^{-1} y_1 - y_2)),
\]
where $I$ denotes the interval $[S+1, S+L]$. Picking up the term corresponding to $a = 0$, we obtain
\[
J = \frac{|\mathcal{V}|^2 L^2}{m} + \frac{1}{m} \sum_{a=1}^{m-1} \sum_{v_1 \in \mathcal{V}} \sum_{v_2 \in \mathcal{V}} \sum_{y_1 \in I} \sum_{y_2 \in I} e_m(a(v_1 v_2^{-1} y_1 - y_2)).
\]
Furthermore,

\[
\frac{1}{m} \sum_{a=1}^{m-1} \sum_{v_1 \in V} \sum_{v_2 \in V} \sum_{y_1 \in I} \sum_{y_2 \in I} e_m(a(v_1 v_2^{-1}y_1 - y_2)) = \\
\frac{1}{m} \sum_{a=1}^{m-1} \sum_{v_1 \in V} \sum_{y_1 \in I} \sum_{y_2 \in I} e_m(a(y_1 - y_2)) + \\
\frac{1}{m} \sum_{a=1}^{m-1} \sum_{v_1 \in V} \sum_{v_2 \in V} \sum_{y_1 \in I} \sum_{y_2 \in I} e_m(a(v_1 v_2^{-1}y_1 - y_2)) = \\
|V|L - \frac{|V|L^2}{m} + \frac{1}{m} \sum_{a=1}^{m-1} \sum_{v_1 \in V} \sum_{v_2 \in V} \sum_{y_1 \in I} \sum_{y_2 \in I} e_m(a(v_1 v_2^{-1}y_1 - y_2)).
\]

Therefore

\[
J = \frac{|V|^2L^2}{m} + |V|L - \frac{|V|L^2}{m} + \frac{1}{m} \sum_{a=1}^{m-1} \sum_{v_1 \in V} \sum_{v_2 \in V} \sum_{y_1 \in I} \sum_{y_2 \in I} e_m(a(v_1 v_2^{-1}y_1 - y_2)).
\]

Here \(\theta_1\), and \(\theta_j\) everywhere below, denote some functions with \(|\theta_j| \leq 1\).

For a given \(n\) let \(r(n)\) be the number of solutions of the congruence

\[v_1v_2^{-1} \equiv n \pmod{m}, \quad v_1, v_2 \in V, \quad v_1 \neq v_2.\]

In particular \(r(1) = 0\), and if \((n, m) > 1\), then \(r(n) = 0\). Therefore, the above formula takes the form

\[
J = \frac{|V|^2L^2}{m} + |V|L - \frac{|V|L^2}{m} + \frac{1}{m} \sum_{a=1}^{m-1} \sum_{v_1 \in V} \sum_{v_2 \in V} \sum_{y_1 \in I} \sum_{y_2 \in I} e_m(a(ny_1^{-1}y_2)).
\]

It is important to note that \(v^2 \leq m\) for any \(v \in V\). For this reason we have \(r(n) \leq 1\) for any \(n, 1 \leq n \leq m\). Indeed, if

\[v_1v_2^{-1} \equiv v_3v_4^{-1} \pmod{m}\]

for some \(v_1, v_2, v_3, v_4 \in V\) and if \(v_1 \neq v_2\), then

\[v_1v_4 \equiv v_3v_2 \pmod{m}.\]
Since \( v^2 \leq m \) for any \( v \in V \), then we derive that \( v_1 v_4 = v_3 v_2 \). But \( V \) consists only on prime numbers and \( v_1 \neq v_2 \). Hence, \( v_1 = v_3, v_2 = v_4 \).

Thus

\[
J = \frac{|V|^2 L^2}{m} + |V| L - \frac{|V| L^2}{m} + \frac{\theta_2}{m} \sum_{a=1}^{m-1} \sum_{1 \leq n \leq m \atop (n,m)=1} \left| \sum_{y_1 \in I, y_2 \in I} e_m(a(ny_1 - y_2)) \right|. \tag{1}
\]

It is now useful to recall the bound

\[
\left| \sum_{y \in I} e_m(by) \right| \leq \frac{1}{|\sin(\pi b/m)|},
\]

which, in application to (1), yields

\[
J = \frac{|V|^2 L^2}{m} + |V| L - \frac{|V| L^2}{m} + \frac{\theta_2}{m} \sum_{a=1}^{m-1} \sum_{1 \leq n \leq m \atop (n,m)=1} \frac{1}{|\sin(\pi an/m)|} \frac{1}{|\sin(\pi a/m)|}. \tag{2}
\]

For each divisor \( s|m \) we collect together the values of \( a \) with \( (a,m) = s \). Then

\[
\sum_{a=1}^{m-1} \sum_{1 \leq n \leq m \atop (n,m)=1} \frac{1}{|\sin(\pi an/m)|} \frac{1}{|\sin(\pi a/m)|} =
\]

\[
\sum_{s|m} \sum_{1 \leq a \leq m-1} \sum_{1 \leq n \leq m \atop (n,m)=1} \frac{1}{|\sin(\pi an/m)|} \frac{1}{|\sin(\pi a/m)|} \leq
\]

\[
\sum_{s|m} \sum_{1 \leq b \leq m/s-1} \sum_{1 \leq n \leq m/s \atop (b,m/s)=1} \frac{1}{|\sin(\pi bn/(m/s))|} \frac{1}{|\sin(\pi b/(m/s))|} \leq
\]

\[
\sum_{s|m} \left( \sum_{1 \leq b \leq m/s \atop (b,m/s)=1} \frac{1}{|\sin(\pi b/(m/s))|} \right)^2 \leq
\]

\[
\sum_{s|m} \left( \sum_{1 \leq b \leq m/2s} \frac{m}{bs} \right)^2 \leq \frac{m^3 \log^2 m}{\phi(m)},
\]
where we have used the inequality
\[ \sum_{s|m} \frac{1}{s} \leq \prod_{p|m} \frac{1}{1 - p^{-1}} = \frac{m}{\phi(m)}. \]
Inserting this bound into (2), we obtain the required estimate.

3 Proof of Theorem 2

If \(|X|^{1/2}N^{1/4}T^{1/4}p^{-7/8} \leq 10\) then the estimate of Theorem 2 becomes trivial. Therefore, we can suppose that
\[ Q := |X|^{1/2}N^{1/4}T^{1/4}p^{-7/8} \geq 10. \]

For a given divisor \(d \mid p - 1\) let \(L_d\) be the set of all integers \(y\) such that \(dy \in [K + 1, K + N]\) and \((dy, p - 1) = d\). Then
\[ W_{a}(\gamma; T; X; K; N) \leq \sum_{d \mid p - 1} R_{a}(\gamma; d, X, L_{d}), \]
where \(R_{a}(\gamma; d, X, L_{d})\) is defined by
\[ R_{a}(\gamma; d, X, L_{d}) = \sum_{x \in X} \left| \sum_{y \in L_{d}} \gamma(dy)e_{p}(ag^{tdy}) \right|. \]
Note that \(|L_{d}| \leq Nd^{-1} + 1\) and that the elements of \(L_{d}\) are relatively prime to \((p - 1)/d\).

For the divisors \(d \mid p - 1\) with the condition \(d \geq Q\) we use the trivial estimate
\[ R_{a}(\gamma; d, X, L_{d}) \leq |X||L_{d}| \leq \frac{|X|N}{Q} + |X| \ll \frac{|X|^{1/2}N^{3/4}p^{7/8}}{T^{1/4}}. \]
Therefore, in view of \(\tau(p - 1) \leq p^{o(1)}\), from (3) we obtain
\[ W_{a}(\gamma; T; X; K; N) \ll \sum_{d \mid p - 1; d \leq Q} R_{a}(\gamma; d, X, L_{d}) + \frac{|X|^{1/2}N^{3/4}p^{7/8+o(1)}}{T^{1/4}}. \]

(4)
Below we suppose that \(d \leq Q\) (and therefore \(|\mathcal{L}_d| \leq 2Nd^{-1}\)) and our aim is to obtain a suitable upper bound for \(R_a(\gamma; d, \mathcal{X}, \mathcal{L}_d)\).

Observe that if \(p^{1/4}T^{1/2}N^{-1/2}Q^{-1/2} \leq \log p\) then the estimate of Theorem 2 becomes trivial. Indeed, in this case we would have that

\[
p^{1/4}T^{1/2}N^{-1/2}|\mathcal{X}|^{-1/4}N^{-1/8}T^{-1/8}p^{7/16} \leq \log p.
\]

Therefore,

\[
T^{1/4} \leq |\mathcal{X}|^{1/6}N^{5/12}p^{-11/24+o(1)},
\]

whence

\[
\frac{|\mathcal{X}|^{1/2}N^{3/4}p^{7/8+o(1)}}{T^{1/4}} = |\mathcal{X}|^{1/3}N^{1/3}p^{4/3+o(1)} \geq |\mathcal{X}|N.
\]

Hence, without loss of generality we may assume that

\[
p^{1/4}T^{1/2}N^{-1/2}Q^{-1/2} \geq \log p.
\tag{5}
\]

Denote by \(\mathcal{V}\) the set of the first \(\left[p^{1/4}T^{1/2}N^{-1/2}d^{-1/2}\right]\) prime numbers which are not divisible by \(p - 1\). Since any positive integer \(m\) has only \(O(\log m)\) (even \(O(\log m/\log \log m)\)) different prime divisors, then from (5) we deduce that for any \(v \in \mathcal{V}\) we have

\[
v \ll (|\mathcal{V}| + \log p) \log p \ll |\mathcal{V}| \log p.
\]

Here \(|\mathcal{V}|\), as before, denotes the cardinality of \(\mathcal{V}\), that is

\[
|\mathcal{V}| = \left[p^{1/4}T^{1/2}N^{-1/2}d^{-1/2}\right].
\]

We observe that if \(TN \leq p^{3/2}\), then the estimate of Theorem 2 again becomes trivial. Hence, we may suppose that

\[
TN \geq p^{3/2}.
\tag{6}
\]

Now we follow the idea of [5] in order to relate the problem of obtaining an upper bound for \(R_a(\gamma; d, \mathcal{X}, \mathcal{L}_d)\) with Theorem 1. For a given divisor \(d \mid p - 1\) denote by \(\mathcal{U}_d\) the set of all elements of the ring \(\mathbb{Z}_{(p-1)/d}\) relatively prime to \((p-1)/d\), that is \(\mathcal{U}_d = \mathbb{Z}_{(p-1)/d}^*\). For any given integer \(y\) with \((y, (p-1)/d) = 1\) consider the congruence

\[
uv \equiv y \pmod{(p-1)/d}, \quad u \in \mathcal{U}_d, \quad v \in \mathcal{V}.
\tag{7}
\]
The number of solutions of this congruence is exactly equal to $|V|$. This follows from the fact that once $v$ is fixed then $u$ is determined uniquely.

We replace $\lambda$ by $g^t$, where $t = (p - 1)/T$, and consider the sum

$$\sum_{y \in L_d} \gamma(dy)e_p(\alpha g^{tdy}).$$

Denote by $\delta(y) := \delta(L_d; y)$ the characteristic function of the set $L_d$ in the ring $\mathbb{Z}_{(p - 1)/d}$. Since the number of solutions of the congruence (7) is equal to $|V|$ for any fixed $y \in L_d$, then

$$\sum_{y \in L_d} \gamma(dy)e_p(\alpha g^{tdy}) = \frac{1}{|V|} \sum_{u \in U_d} \sum_{v \in V} \gamma(duv)\delta(uv)e_p(\alpha g^{tduv}).$$

Therefore, setting

$$R_a(\gamma; d, \mathcal{X}, L_d) = \sum_{x \in \mathcal{X}} \left| \sum_{y \in L_d} \gamma(dy)e_p(\alpha g^{tdy}) \right|$$

we see that

$$R_a(\gamma; d, \mathcal{X}, L_d) = \frac{1}{|V|} \sum_{x \in \mathcal{X}} \left| \sum_{u \in U_d} \sum_{v \in V} \gamma(duv)\delta(uv)e_p(\alpha g^{tduv}) \right|.$$

Application of the Cauchy inequality to the sums over $x$ and $u$ yields

$$\left| R_a(\gamma; d, \mathcal{X}, L_d) \right|^2 \leq \frac{|U_d||\mathcal{X}|}{|V|^2} \sum_{u \in U_d} \sum_{x = 1}^{p-1} \left| \sum_{v \in V} \gamma(duv)\delta(uv)e_p(\alpha g^{tduv}) \right|^2.$$

If $(n, p - 1) = d$, if $x$ runs through $\mathbb{Z}_{p-1}$ and if $z$ runs through the reduced residue system modulo $p$, then $g^{nx}$ and $z^d$ run the same system of residues modulo $p$ (including the multiplicities). Since $(du, p - 1) = d$, then

$$\left| R_a(\gamma; d, \mathcal{X}, L_d) \right|^2 \leq \frac{|U_d||\mathcal{X}|}{|V|^2} \sum_{u \in U_d} \sum_{z = 1}^{p-1} \left| \sum_{v \in V} \gamma(duv)\delta(uv)e_p(\alpha z^{tdv}) \right|^2,$$

whence

$$\left| R_a(\gamma; d, \mathcal{X}, L_d) \right|^2 \leq \frac{|U_d||\mathcal{X}|}{|V|^2} \sum_{u \in U_d} \sum_{v_1 \in V} \sum_{v_2 \in V} \gamma(duv_1)\gamma(duv_2)\delta(uv_1)\delta(uv_2) \sum_{z = 1}^{p-1} e_p(\alpha (z^{tdv_1} - z^{tdv_2})).$$

10
The rightmost sum is equal to $p - 1$ when $v_1 = v_2$ and, according to the Weil estimate, is bounded by $(\max\{v_1, v_2\})t dp^{1/2}$ when $v_1 \neq v_2$. Recall that $\max\{v_1, v_2\} \ll |V| \log p$,

and $|U_d| = \phi(\frac{p-1}{d}) \leq \frac{p}{d}$. Therefore,

$$|R_a(\gamma; d, X, L_d)|^2 \ll \frac{p^2 |X|}{d|V|^2} \sum_{u \in U_d} \sum_{v \in V} \delta^2(uv) + \frac{p^{3/2} |X| t \log p}{|V|} \sum_{u \in U_d} \sum_{v_1, v_2 \in V} \delta(u v_1) \delta(u v_2).$$  \hspace{1cm} (8)

Next, from (7) we derive the formula

$$\sum_{u \in U_d} \sum_{v \in V} \delta^2(uv) = |V| |L_d|. \hspace{1cm} (9)$$

Now set

$$J = \sum_{u \in U_d} \sum_{v_1, v_2 \in V} \delta(u v_1) \delta(u v_2)$$

and observe that $J$ is equal to the number of solutions of the system of congruences

$$\begin{cases} uv_1 \equiv y_2 \pmod{\frac{p-1}{d}} \\ uv_2 \equiv y_1 \pmod{\frac{p-1}{d}} \end{cases}$$

subject to the conditions

$$u \in U_d, \quad v_1, v_2 \in V, \quad y_1, y_2 \in L_d.$$  

It then follows that

$$v_1 y_1 \equiv v_2 y_2 \pmod{\frac{p-1}{d}}.$$  

Therefore, from (8) and (9), we derive that

$$|R_a(\gamma; d, X, L_d)|^2 \ll \frac{p^2 |X|}{d|V|^2} |V| |L_d| + \frac{p^{5/2} |X| \log p}{T |V|} J,$$

whence

$$|R_a(\gamma; d, X, L_d)|^2 \ll \frac{p^2 |X| N}{d^2 |V|} + \frac{p^{5/2} |X| \log p}{T |V|} J_d,$$  \hspace{1cm} (10)
where \( J_d \) denotes the number of solutions of the congruence

\[
v_1 y_1 \equiv v_2 y_2 \pmod{p - 1 \over d}, \quad v_1, v_2 \in \mathcal{V}, \quad K + 1 \leq y_1, y_2 \leq K + N \over d.
\]

It is important to note that the condition of Theorem 2 yields, for any \( v \in \mathcal{V} \), the bound

\[
v^2 \leq |\mathcal{V}|^2 (\log p)^{2+o(1)} \leq p^{1/2} (\log p)^{2+o(1)} T N^{-1} d^{-1} \leq p - 1 \over d.
\]

Hence, we can apply Theorem 1 with \( m = (p - 1)/d \). It gives

\[
J_d \ll \frac{|\mathcal{V}|^2 N^2}{(p - 1)d} + \frac{|\mathcal{V}| N^2}{d} + \frac{p (\log \log p) \log^2 p}{d},
\]

whence, using \( |\mathcal{V}| \leq p^{1/4} T^{1/2} N^{-1/2} \), we obtain

\[
J_d \ll \frac{p^{-1/2+o(1)} T N}{d} \left( 1 + \frac{p^{3/4} T^{1/2} N^{-1/2}}{T N} + \frac{p^{3/2}}{T N} \right).
\]

Taking into account (6), we deduce

\[
J_d \ll \frac{p^{-1/2+o(1)} T N}{d}.
\]

Combining this estimate with (10), we conclude

\[
|\mathcal{R}_a(\gamma; d, \mathcal{X}, \mathcal{L}_d)| \ll \frac{|\mathcal{V}|^{1/2} N^{3/4} p^{7/8+o(1)}}{d^{1/4} T^{1/4}}.
\]

The result now follows in view of (4).

4 Proof of Theorem 6

Without loss of generality we may suppose that

\[
\Delta m^{1/2} \sqrt{m/\phi(m) \log m} < m,
\]

as otherwise the statement of Theorem 6 is trivial.
Denote by $V$ the set of prime numbers coprime to $m$ and not exceeding $m^{1/2}$. Let $J$ denote the number of solutions to the congruence

$$v_1(y_1 + z_1) \equiv v_2(y_2 + z_2) \pmod{m}$$

subject to the conditions

$$v_1, v_2 \in V, \quad y_1, y_2, z_1, z_2 \in I,$$

where $I$ denotes the set of integers $x, [S/2] + 1 \leq x \leq [S/2] + L$, and

$$L = \left[ \frac{\Delta m^{1/2} \sqrt{m/\phi(m)} \log m}{2} \right].$$

Obviously that

$$S + 1 \leq y_i + z_i \leq S + \Delta m^{1/2} \log m, \quad i = 1, 2.$$

Following the lines of the proof of Theorem 1, we express $J$ in terms of trigonometric sums. Since

$$v_1 v_2^{-1}(y_1 + z_1) \equiv y_2 + z_2 \pmod{m},$$

then

$$J = \frac{1}{m} \sum_{a=0}^{m-1} \sum_{v_1 \in V} \sum_{v_2 \in V} \sum_{y_1, z_1 \in I} \sum_{y_2, z_2 \in I} e_m(a(v_1 v_2^{-1}(y_1 + z_1) - y_2 - z_2)).$$

Picking up the term corresponding to $a = 0$, we obtain

$$J = \frac{|V|^2 L^4}{m} + \frac{1}{m} \sum_{a=1}^{m-1} \sum_{v_1 \in V} \sum_{v_2 \in V} \sum_{y_1, z_1 \in I} \sum_{y_2, z_2 \in I} e_m(a(v_1 v_2^{-1}(y_1 + z_1) - y_2 - z_2)).$$

Since the number of solutions of the congruence

$$y_1 + z_1 \equiv y_2 + z_2 \pmod{m}, \quad y_1, z_1, y_2, z_2 \in I$$

is $O(L^3)$, then we obtain

$$\left| \frac{1}{m} \sum_{a=1}^{m-1} \sum_{v_1 \in V} \sum_{y_1, z_1 \in I} \sum_{y_2, z_2 \in I} e_m(a(y_1 + z_1 - y_2 - z_2)) \right| \leq$$

$$\frac{|V|^{m-1}}{m} \sum_{a=0}^{m-1} \left| \sum_{y_1 \in I} e_m(ay_1) \right|^4 \ll |V| L^3.$$
Therefore,

\[
\frac{1}{m} \sum_{a=1}^{m-1} \sum_{v_1 \in V} \sum_{v_2 \in V} \sum_{y_1, z_1 \in \mathcal{I}} \sum_{y_2, z_2 \in \mathcal{I}} e_m(a(v_1 v_2^{-1}(y_1 + z_1) - y_2 - z_2)) = O(|V|^3) + \frac{1}{m} \sum_{a=1}^{m-1} \sum_{v_1 \in V} \sum_{v_2 \in V} \sum_{y_1, z_1 \in \mathcal{I}} \sum_{y_2, z_2 \in \mathcal{I}} e_m(a(v_1 v_2^{-1}(y_1 + z_1) - y_2 - z_2)).
\]

Using exactly the same argument that we used in the proof of Theorem 1, we derive the formula

\[
J = \frac{|V|^2 L^4}{m} + O(|V|^3) + O(R),
\]

where

\[
R = \frac{1}{m} \sum_{s|m} \sum_{b \leq m/s-1} \sum_{1 \leq n \leq m} \left| \sum_{y_1, z_1 \in \mathcal{I}} \sum_{y_2, z_2 \in \mathcal{I}} e_m(b(n y_1 + z_1) - y_2 - z_2) \right|
\]

Next, introducing \( s = (a, m) \), we obtain

\[
R = \frac{1}{m} \sum_{s|m} \sum_{b \leq m/s-1} \sum_{1 \leq n \leq m/s} \left| \sum_{y_1, z_1 \in \mathcal{I}} \sum_{y_2, z_2 \in \mathcal{I}} e_m(b n y_1 + z_1 - b y_2 + z_2) \right| 
\]

\[
\frac{1}{m} \sum_{s|m} \sum_{b \leq m/s-1} \sum_{1 \leq n \leq m/s} \left| \sum_{y_1, z_1 \in \mathcal{I}} \sum_{y_2, z_2 \in \mathcal{I}} e_m(b n y_1 + z_1 - b y_2 + z_2) \right| 
\]

\[
\frac{1}{m} \sum_{s|m} \sum_{b \leq m/s-1} \sum_{1 \leq n \leq m/s} \left| \sum_{y_1, z_1 \in \mathcal{I}} \sum_{y_2, z_2 \in \mathcal{I}} e_m(b n y_1 + z_1 - b y_2 + z_2) \right| 
\]

\[
\frac{1}{m} \sum_{s|m} \sum_{b \leq m/s-1} \sum_{1 \leq n \leq m/s} \left| \sum_{y_1, z_1 \in \mathcal{I}} \sum_{y_2, z_2 \in \mathcal{I}} e_m(b n y_1 + z_1 - b y_2 + z_2) \right| 
\]

Therefore,

\[
J = \frac{|V|^2 L^4}{m} + O(|V|^3) + O(R_1) + O(R_2), \quad (11)
\]
where

\[
R_1 = \frac{1}{m} \sum_{s|m, s<m/L} s \left( \sum_{1 \leq n \leq m/s \atop (n, m/s) = 1} \left| \sum_{y \in I} e_{m/s}(ny) \right|^2 \right)
\]  \tag{12}

\[
R_2 = \frac{1}{m} \sum_{s|m, m/L \leq s < m} s \left( \sum_{1 \leq n \leq m/s \atop (n, m/s) = 1} \left| \sum_{y \in I} e_{m/s}(ny) \right|^2 \right)
\]  \tag{13}

If \( s < m/L \) then \( m/s > L \) and therefore, the congruence

\[y_1 \equiv y_2 \pmod{m/s}, \quad y_1, y_2 \in I\]

has \( L \) solutions. Hence,

\[
\sum_{1 \leq n \leq m/s} \left| \sum_{y \in I} e_{m/s}(ny) \right|^2 = \frac{mL}{s},
\]

whence, using (12),

\[
R_1 \leq \frac{1}{m} \sum_{s|m, s<m/L} s \left( \sum_{1 \leq n \leq m/s \atop (n, m/s) = 1} \left| \sum_{y \in I} e_{m/s}(ny) \right|^2 \right) = \frac{mL^2}{s} \sum_{s|m, s<m/L} s^{-1} \leq \frac{m^2 L^2}{\phi(m)}.
\]

Inserting this bound into (11), we deduce

\[
J = \frac{|V|^2 L^4}{m} + O(|V| L^3) + O(m^2 L^2 / \phi(m)) + O(R_2).
\]  \tag{14}

Now we proceed to estimate \( R_2 \). Note that in (13) we have \((n, m/s) = 1\). Therefore, for any integer \( K \),

\[
\sum_{y=K+1}^{K+m/s} e_{m/s}(ny) = 0,
\]
whence we deduce that there exist integers $A$ and $B$ with $0 < B \leq m/s$ such that

$$\sum_{y \in I} e_{m/s}(ny) = \sum_{A < y \leq A + B} e_{m/s}(ny).$$

Hence

$$\sum_{1 \leq n \leq m/s \atop (n, m/s) = 1} \left| \sum_{y \in I} e_{m/s}(ny) \right|^2 = \sum_{1 \leq n \leq m/s \atop (n, m/s) = 1} \left| \sum_{A < y \leq A + B} e_{m/s}(ny) \right|^2 \leq \sum_{n=1}^{m/s} \left| \sum_{A < y \leq A + B} e_{m/s}(ny) \right|^2 = \frac{mB}{s} \leq \frac{m^2}{s^2}.$$

Taking this into account, from (13) we deduce

$$R_2 \leq \frac{1}{m} \sum_{s \geq m/L} s(m^4/s^4) \ll mL^2.$$

Therefore, in view of (14), we obtain the asymptotic formula

$$J = \frac{|V|^2 L^4}{m} + O(|V|L^3) + O(m^2 L^2/\phi(m)) = \frac{|V|^2 L^4}{m} \left( 1 + O \left( \frac{m}{|V|L} + \frac{m^3}{\phi(m)|V|^2 L^2} \right) \right).$$

Recalling that $|V| \gg m^{1/2} / \log m$ and $L = \left\lfloor \Delta m^{1/2} \sqrt{m/\phi(m)} \log m \right\rfloor$, we arrive at the formula

$$J = \frac{|V|^2 L^4}{m} \left( 1 + O(\Delta^{-1}) \right).$$

Next, define

$$H = \{ q(y + z) \pmod{m}, \quad q \leq m^{1/2}, \quad [S/2] + 1 \leq y, z \leq [S/2] + L \}.$$

Obviously, $S + 1 \leq y + z \leq S + \Delta m^{1/2} \sqrt{m/\phi(m)} \log m$. For a given $h \in H$, by $J(h)$ we denote the number of solutions of the congruence

$$q(y + z) \equiv h \pmod{m}, \quad q \leq m^{1/2}, \quad [S/2] + 1 \leq y, z \leq [S/2] + L.$$
Then
\[ J = \sum_{h \in H} J^2(h) \geq \frac{1}{|H|} \left( \sum_{h \in H} J(h) \right)^2 = \frac{1}{|H|} |\mathcal{V}|^2 L^4. \]

Therefore,
\[ |H| \geq \frac{|\mathcal{V}|^2 L^4}{J} \geq \frac{m}{1 + O(\Delta^{-1})} = (1 + O(\Delta^{-1}))m. \]

The result now follows in view of \(|H| \leq m|.|\)

5 Proof of Theorem 8

Without loss of generality we may suppose that
\[ 0 < N < N + \Delta p^{1/2} < p, \quad 0 < M < M + \Delta p^{1/2} < p. \]

Denote \( X = [\Delta p^{1/2}/2], \ N_1 = [N/2], \ S_1 = [S/2], \) and let \( H^* \) be the set of all residue classes of the form \((x + t)(y + z)^{-1} \) \((\text{mod } p), \)
where
\[ N_1 + 1 \leq x, t \leq N_1 + X, \quad S_1 + 1 \leq y, z \leq S_1 + X. \]

Obviously,
\[ N + 1 \leq x + t \leq N + \Delta p^{1/2}, \quad S + 1 \leq y + z \leq S + \Delta p^{1/2}. \]

Next, let
\[ H_1^* = \{ h \pmod{p} : h \not\in H^*, \ h \not\equiv 0 \pmod{p} \}. \]

Then the congruence
\[ x + t - (y + z)h \equiv 0 \pmod{p} \]
has no solutions in variables \( h, x, t, y, z \) subject to the condition
\[ h \in H_1^*, \quad N_1 + 1 \leq x, t \leq N_1 + X, \quad S_1 + 1 \leq y, z \leq S_1 + X. \]

Therefore,
\[ \sum_{a=0}^{p-1} \sum_{h \in H_1^*} \sum_{x,t \in I_1} \sum_{y,z \in I_2} e^{2\pi i a(x + t - h(y + z))} p = 0, \]
where $I_1$ and $I_2$ denote the intervals $[N_1+1, N_1+X]$ and $[S_1+1, S_1+X]$ correspondingly.

Separating the term corresponding to $a = 0$ we deduce that

$$|H_1^*|X^4 \leq \sum_{a=1}^{p-1} \left| \sum_{x,t \in I_1} e^{2\pi i a(x+t)} \right| \left| \sum_{y,z \in I_2} \sum_{h \in H_1^*} e^{2\pi i ah(y+z)} \right|.$$  

On the other hand for $(a, p) = 1$ we have

$$\left| \sum_{y,z \in I_2} \sum_{h \in H_1^*} e^{2\pi i ah(y+z)} \right| \leq \sum_{h \in H_1^*} \left| \sum_{y,z \in I_2} e^{2\pi i ah(y+z)} \right| \leq pX,$$

and similarly,

$$\sum_{a=1}^{p-1} \left| \sum_{x,t \in I_1} e^{2\pi i a(x+t)} \right| \leq pX.$$

Hence

$$|H_1^*|X^4 \leq p^2 X^2,$$

whence

$$|H_1^*| \leq \frac{p^2}{X^2} \ll p \Delta^{-2}.$$  

Since $|H| = p - 1 - |H_1^*|$, then the result follows.

References

[1] W. D. Banks, A. Conflitti, J. B. Friedlander and I. E. Shparlinski, **Exponential sums over Mersenne numbers**, Compos. Math. **140**, no. 1, 15–30 (2004).

[2] W. D. Banks, J. B. Friedlander, M. Z. Garaev and I. E. Shparlinski, **Exponential sums over smooth numbers**, (Preprint).

[3] J. Bourgain, **New bounds on exponential sums related to Diffie-Hellman distributions**, C. R. Math. Acad. Sci. Paris, **338**, no. 11, 825–830 (2004).
[4] J. B. Friedlander and I. E. Shparlinski, *Double exponential sums over thin sets*, Proc. Amer. Math. Soc., **129**, 1617–1621 (2001).

[5] M. Z. Garaev, *Double exponential sums related to Diffie-Hellman distributions*, Int. Math. Res. Notices (to appear).

[6] M. Z. Garaev, *Character sums in short intervals and the multiplication table modulo a prime*, Monatsh. Math. (to appear).

[7] M. Z. Garaev, *On the logarithmic factor in error term estimates in certain additive congruence problems*, Preprint.

[8] M. Z. Garaev and A. A. Karatsuba, *On character sums and the exceptional set of a congruence problem*, J. Number Theory, (to appear).