Proceedings of the Edinburgh Mathematical Society (2007) **50**, 363–375 ©
DOI:10.1017/S0013091505000969 Printed in the United Kingdom

THE REPRESENTATION OF RESIDUE CLASSES BY PRODUCTS OF SMALL INTEGERS

M. Z. GARAEV[1] AND A. A. KARATSUBA[2]

[1] *Instituto de Matemáticas, Universidad Nacional Autónoma de México, Campus Morelia, Apartado Postal 61-3 (Xangari), CP 58089, Morelia, Michoacán, Mexico* (garaev@matmor.unam.mx)

[2] *Steklov Institute of Mathematics, Russian Academy of Sciences, GSP-1, ul. Gubkina 8, Moscow, Russia* (karatsuba@mi.ras.ru)

(Received 27 June 2005)

Abstract For a large integer m, we obtain asymptotic formulae for the number of solutions of certain congruences modulo m with several variables, where the variables belong to special sets of residue classes modulo m. In particular, we obtain new information on the exceptional set of the multiplication table problem in the residue ring modulo m.

Keywords: congruences; trigonometric sums; number of solutions; asymptotic formulae

2000 *Mathematics subject classification:* Primary 11A07; 11B50; 11L07

1. Introduction

In this paper we continue to study the distribution properties in residue classes of the sequence consisting of products of two positive integers bounded by a certain parameter.

For a prime number p, define the set

$$\mathcal{A} = \{xy \pmod p) : 1 \leqslant x, y \leqslant N\}.$$

The main problem is to find a value of N, as small as possible, for which any non-zero residue class modulo p would belong to $\mathcal{A}$. The main conjecture is that one can take N to be as small as $p^{1/2+o(1)}$.

Vâjâitu and Zaharescu [**6**] observed that it would completely solve the pair correlation problem for sequences of fractional parts of the form $\{\alpha n^2\}$ (see [**5**] for the details) if one could deal with the case $N = [p^{2/3-\varepsilon}]$ for some small $\varepsilon > 0$. However, it is only known that N can be taken to be of the size $O(p^{3/4})$ (see [**2**] and also [**1**, **4**]). The exponent $\frac{3}{4}$ is the best known at the time of writing this paper.

It is shown in [**1**] that for almost all primes p and $N = [p^{1/2}(\log p)^{1.087}]$ the set $\mathcal{A}$ contains $(1 + o(1))p$ residue classes modulo p. It is also conjectured that $\mathcal{A}$ possesses this property for any prime p and $N = [p^{1/2+\varepsilon}]$. We remark that one of our results from [**3**] says that for $N = p^{5/8+\varepsilon}$ the set $\mathcal{A}$ contains $(1 + o(1))p$ residue classes modulo p.

In this paper we will prove a general statement that in a particular case confirms the validity of the mentioned conjecture from [**1**] and improves the corresponding result of [**3**]. The arguments used in [**1**] and [**3**] are based on estimates of multiplicative character sums. The approach we use here is based on trigonometric sums.

Throughout the text, the letters p and q are used to denote prime numbers, m denotes a positive integer parameter, S and L are some integers with $0 < L \leqslant m$. For a given set $\mathcal{Q}$ we use $|\mathcal{Q}|$ to denote its cardinality.

Theorem 1.1. *Let $\Delta = \Delta(m) \to \infty$ as $m \to \infty$. Then the set*

$$\{qy \pmod m) : 1 \leqslant q \leqslant m^{1/2},\ S+1 \leqslant y \leqslant S + \Delta m^{1/2}\sqrt{m/\phi(m)}\log m\}$$

contains $(1 + O(\Delta^{-1}))m$ residue classes modulo m.

In particular we have the following corollary.

Corollary 1.2. *Let $\Delta = \Delta(p) \to \infty$ as $p \to \infty$. Then the set*

$$\{qy \pmod p) : q \leqslant p^{1/2},\ 1 \leqslant y \leqslant \Delta p^{1/2}\log p\}$$

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

$$\{qy : q \leqslant p^{1/2},\ S+1 \leqslant y \leqslant S + \Delta p^{1/2}\log p\}$$

contains only $O(p\Delta)$ integers. This shows that the ranges of variables in Theorem 1.1 and Corollary 1.2 are sharp.

To prove Theorem 1.1, we study the congruence

$$v_1(x_1 + y_1) \equiv v_2(x_2 + y_2) \pmod m,$$

where v_1, v_2 belong to the set of all primes not exceeding $m^{1/2}$ and not dividing m, and x_i, y_i run through integers of special intervals. Now we denote by $\mathcal{V}$ any subset of prime numbers not exceeding $m^{1/2}$ and not dividing m. Let J be the number of solutions of the congruence

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

Theorem 1.3. *The following asymptotic formula holds:*

$$J = \frac{|\mathcal{V}|(|\mathcal{V}|-1)}{m}L^2 + |\mathcal{V}|L + O\biggl(\frac{m^2\log^2 m}{\phi(m)}\biggr),$$

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

As we have mentioned, our argument is based on trigonometric sums. In particular, we establish a result on a special trigonometric sum that can be useful in applications to other additive congruences.

Theorem 1.4. *Let $\mathcal{P}$ be any subset of prime numbers not exceeding $p^{1/2}$. Then, for any complex coefficients α_x, β_y, the formula*

$$\sum_{a=1}^{p-1}\biggl|\sum_{q\in\mathcal{P}}\sum_{x=1}^{p}\sum_{y=1}^{p}\alpha_x\beta_y \mathrm{e}^{2\pi \mathrm{i}aq(x+y)/p}\biggr|^2 = |\mathcal{P}|\sum_{a=1}^{p-1}\biggl|\sum_{x=1}^{p}\sum_{y=1}^{p}\alpha_x\beta_y \mathrm{e}^{2\pi \mathrm{i}a(x+y)/p}\biggr|^2 + \theta p^2 I_1 I_2$$

holds, where $|\theta|\leqslant 1$ and

$$I_1=\sum_{x=1}^{p}|\alpha_x|^2,\qquad I_2=\sum_{y=1}^{p}|\beta_y|^2.$$

From Theorem 1.4 one derives the following statement.

Corollary 1.5. *Let $\mathcal{X}\subset\mathbb{Z}_p$, $\mathcal{Y}\subset\mathbb{Z}_p$, and let $\mathcal{P}$ be any subset of prime numbers not exceeding $p^{1/2}$. If J' denotes the number of solutions of the congruence*

$$q_1(x_1+y_1)\equiv q_2(x_2+y_2) \pmod p,\quad q_1,q_2\in\mathcal{P},\ x_1,x_2\in\mathcal{X},\ y_1,y_2\in\mathcal{Y},$$

then

$$J'=\frac{|\mathcal{P}|(|\mathcal{P}|-1)}{p}|\mathcal{X}|^2|\mathcal{Y}|^2+|\mathcal{P}|I+\theta p|\mathcal{X}|\,|\mathcal{Y}|,$$

where $|\theta|\leqslant 1$ and I denotes the number of solutions of the congruence

$$x_1+y_1\equiv x_2+y_2 \pmod p,\quad x_1,x_2\in\mathcal{X},\ y_1,y_2\in\mathcal{Y}.$$

Since $I\leqslant|\mathcal{X}|^{3/2}|\mathcal{Y}|^{3/2}$, we see that if

$$|\mathcal{P}|^2|\mathcal{X}|\,|\mathcal{Y}|=p^2\Delta,\quad \Delta=\Delta(p)\to\infty \text{ as } p\to\infty,$$

then

$$J'=\frac{|\mathcal{P}|^2|\mathcal{X}|^2|\mathcal{Y}|^2}{p}(1+O(\Delta^{-1/2})).$$

In particular, the set

$$\{q(x+y) \pmod p,\ q\in\mathcal{P},\ x\in\mathcal{X},\ y\in\mathcal{Y}\}$$

contains $(1+O(\Delta^{-1/2}))p$ residue classes modulo p.

Corollary 1.5 also follows from the following statement.

Theorem 1.6. *Let $\mathcal{X}\subset\mathbb{Z}_p$, $\mathcal{Y}\subset\mathbb{Z}_p$, and let $\mathcal{Z}$ be any subset of positive integers not exceeding $p^{1/2}$. If J'' denotes the number of solutions of the congruence*

$$z_1(x_1+y_1)\equiv z_2(x_2+y_2) \pmod p,\quad z_1,z_2\in\mathcal{Z},\ x_1,x_2\in\mathcal{X},\ y_1,y_2\in\mathcal{Y},$$

https://doi.org/10.1017/S0013091505000969 Published online by Cambridge University Press

subject to the additional condition $(z_1, z_2) = 1$, *then*

$$J'' = \frac{|\mathcal{X}|^2|\mathcal{Y}|^2 T_{\mathcal{Z}}}{p} + \theta p|\mathcal{X}|\,|\mathcal{Y}|,$$

where $|\theta| \leqslant 1$ *and* $T_{\mathcal{Z}}$ *is the number of pairs* $z_1, z_2 \in \mathcal{Z}$ *with* $(z_1, z_2) = 1$.

We will also prove the following result on the ratio of intervals modulo a prime, which improves one of the results of [**1**].

Theorem 1.7. *Let* $\Delta = \Delta(p) \to \infty$ *as* $p \to \infty$. *Then the set*

$$\{xy^{-1} \pmod p : N+1 \leqslant x \leqslant N + \Delta p^{1/2},\ S+1 \leqslant y \leqslant S + \Delta p^{1/2}\}$$

contains $(1 + O(\Delta^{-2}))p$ *residue classes modulo* p.

Note, however, that when $N = S = 0$ and $\Delta < \frac{1}{2}p^{1/2}$ the set described in Theorem 1.7 misses more than $cp^{1/2}\Delta^{-1}$ residue classes modulo p for some positive constant c (see [**1**]).

The rest of the paper is organized as follows. In § 2 we prove Theorem 1.3. In § 3 we combine the method of § 2 with that described in [**2**] and establish Theorem 1.1. The rest of the results are proved in §§ 4–6.

In what follows, we use the abbreviation

$$\boldsymbol{e}_k(z) = \mathrm{e}^{2\pi \mathrm{i} z/k}.$$

2. Proof of Theorem 1.3

Recall that J denotes the number of solutions to the congruence

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

We express J in terms of trigonometric sums. Since

$$v_1 v_2^{-1} y_1 \equiv y_2 \pmod m,$$

we have

$$J = \frac{1}{m} \sum_{a=0}^{m-1} \sum_{v_1 \in \mathcal{V}} \sum_{v_2 \in \mathcal{V}} \sum_{y_1 \in \mathcal{I}} \sum_{y_2 \in \mathcal{I}} \boldsymbol{e}_m(a(v_1 v_2^{-1} y_1 - y_2)),$$

where $\mathcal{I}$ denotes the interval $[S+1, S+L]$. Picking up the term corresponding to $a = 0$, we obtain

$$J = \frac{|\mathcal{V}|^2 L^2}{m} + \frac{1}{m} \sum_{a=1}^{m-1} \sum_{v_1 \in \mathcal{V}} \sum_{v_2 \in \mathcal{V}} \sum_{y_1 \in \mathcal{I}} \sum_{y_2 \in \mathcal{I}} \boldsymbol{e}_m(a(v_1 v_2^{-1} y_1 - y_2)).$$

Furthermore,

$$\frac{1}{m}\sum_{a=1}^{m-1}\sum_{v_1\in\mathcal{V}}\sum_{v_2\in\mathcal{V}}\sum_{y_1\in\mathcal{I}}\sum_{y_2\in\mathcal{I}}\boldsymbol{e}_m(a(v_1v_2^{-1}y_1-y_2))$$
$$=\frac{1}{m}\sum_{a=1}^{m-1}\sum_{v\in\mathcal{V}}\sum_{y_1\in\mathcal{I}}\sum_{y_2\in\mathcal{I}}\boldsymbol{e}_m(a(y_1-y_2))$$
$$+\frac{1}{m}\sum_{a=1}^{m-1}\sum_{v_1\in\mathcal{V}}\sum_{\substack{v_2\in\mathcal{V}\\ v_2\neq v_1}}\sum_{y_1\in\mathcal{I}}\sum_{y_2\in\mathcal{I}}\boldsymbol{e}_m(a(v_1v_2^{-1}y_1-y_2))$$
$$=|\mathcal{V}|L-\frac{|\mathcal{V}|L^2}{m}+\frac{1}{m}\sum_{a=1}^{m-1}\sum_{v_1\in\mathcal{V}}\sum_{\substack{v_2\in\mathcal{V}\\ v_2\neq v_1}}\sum_{y_1\in\mathcal{I}}\sum_{y_2\in\mathcal{I}}\boldsymbol{e}_m(a(v_1v_2^{-1}y_1-y_2)).$$

Therefore,

$$J=\frac{|\mathcal{V}|^2L^2}{m}+|\mathcal{V}|L-\frac{|\mathcal{V}|L^2}{m}+\frac{\theta_1}{m}\sum_{a=1}^{m-1}\sum_{v_1\in\mathcal{V}}\sum_{\substack{v_2\in\mathcal{V}\\ v_2\neq v_1}}\biggl|\sum_{y_1\in\mathcal{I}}\sum_{y_2\in\mathcal{I}}\boldsymbol{e}_m(a(v_1v_2^{-1}y_1-y_2))\biggr|.$$

Here and everywhere below, θ_j denotes a function with $|\theta_j|\leqslant 1$.

For a given n, let $r(n):=r_{\mathcal{V}}(n)$ be the number of solutions of the congruence

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

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

$$J=\frac{|\mathcal{V}|^2L^2}{m}+|\mathcal{V}|L-\frac{|\mathcal{V}|L^2}{m}+\frac{\theta_1}{m}\sum_{a=1}^{m-1}\sum_{\substack{1\leqslant n\leqslant m\\ (n,m)=1}}r(n)\biggl|\sum_{y_1\in\mathcal{I}}\sum_{y_2\in\mathcal{I}}\boldsymbol{e}_m(a(ny_1-y_2))\biggr|.$$

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

$$v_1v_2^{-1}\equiv v_3v_4^{-1} \pmod m$$

for some $v_1,v_2,v_3,v_4\in\mathcal{V}$ and if $v_1\neq v_2$, then

$$v_1v_4\equiv v_3v_2 \pmod m.$$

Since $v^2\leqslant m$ for any $v\in\mathcal{V}$, we derive that $v_1v_4=v_3v_2$. The elements of $\mathcal{V}$ are prime numbers and $v_1\neq v_2$. Hence, $v_1=v_3$, $v_2=v_4$.

Thus,

$$J=\frac{|\mathcal{V}|^2L^2}{m}+|\mathcal{V}|L-\frac{|\mathcal{V}|L^2}{m}+\frac{\theta_2}{m}\sum_{a=1}^{m-1}\sum_{\substack{1\leqslant n\leqslant m\\ (n,m)=1}}\biggl|\sum_{y_1\in\mathcal{I}}\sum_{y_2\in\mathcal{I}}\boldsymbol{e}_m(a(ny_1-y_2))\biggr|. \tag{2.1}$$

It is now useful to recall the bound

$$\biggl|\sum_{y\in\mathcal{I}} \boldsymbol{e}_m(by)\biggr| \leqslant \frac{1}{|\sin(\pi b/m)|},$$

which, applied to (2.1), yields

$$J = \frac{|\mathcal{V}|^2L^2}{m} + |\mathcal{V}|L - \frac{|\mathcal{V}|L^2}{m} + \frac{\theta_3}{m}\sum_{a=1}^{m-1}\sum_{\substack{1\leqslant n\leqslant m\\(n,m)=1}} \frac{1}{|\sin(\pi an/m)|}\frac{1}{|\sin(\pi a/m)|}. \tag{2.2}$$

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

$$\begin{aligned}
\sum_{a=1}^{m-1}&\sum_{\substack{1\leqslant n\leqslant m\\(n,m)=1}} \frac{1}{|\sin(\pi an/m)|}\frac{1}{|\sin(\pi a/m)|}\\
&= \sum_{\substack{s\mid m\\s<m}}\ \sum_{\substack{1\leqslant a\leqslant m-1\\(a,m)=s}}\ \sum_{\substack{1\leqslant n\leqslant m\\(n,m)=1}} \frac{1}{|\sin(\pi an/m)|}\frac{1}{|\sin(\pi a/m)|}\\
&\leqslant \sum_{\substack{s\mid m\\s<m}} s \sum_{\substack{1\leqslant b\leqslant m/s-1\\(b,m/s)=1}}\ \sum_{\substack{1\leqslant n\leqslant m/s\\(n,m/s)=1}} \frac{1}{|\sin(\pi bn/(m/s))|}\frac{1}{|\sin(\pi b/(m/s))|}\\
&\leqslant \sum_{\substack{s\mid m\\s<m}} s \biggl(\sum_{\substack{1\leqslant b\leqslant m/s\\(b,m/s)=1}} \frac{1}{|\sin(\pi b/(m/s))|}\biggr)^2\\
&\ll \sum_{\substack{s\mid m\\s<m}} s \biggl(\sum_{1\leqslant b\leqslant m/2s} \frac{m}{bs}\biggr)^2\\
&\leqslant \frac{m^3\log^2 m}{\phi(m)},
\end{aligned}$$

where we have used the inequality

$$\sum_{s\mid m}\frac{1}{s} \leqslant \prod_{p\mid m}\frac{1}{1-p^{-1}} = \frac{m}{\phi(m)}.$$

Inserting this bound into (2.2), we obtain the required estimate.

3. Proof of Theorem 1.1

Without loss of generality, we may assume that

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

as otherwise the statement of Theorem 1.1 is trivial.

https://doi.org/10.1017/S0013091505000969 Published online by Cambridge University Press

We take $\mathcal{V}$ to be the set of all prime numbers coprime to m and not exceeding $m^{1/2}$. Let J_1 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

$$v_1, v_2 \in \mathcal{V}, \qquad y_1, y_2, z_1, z_2 \in \mathcal{I},$$

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

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

It is obvious that

$$S+1 \leqslant y_i + z_i \leqslant S + \Delta m^{1/2}\sqrt{m/\phi(m)}\log m, \quad i=1,2.$$

Following the lines of the proof of Theorem 1.3, we express J_1 in terms of trigonometric sums. Since

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

we have

$$J_1 = \frac{1}{m}\sum_{a=0}^{m-1}\sum_{v_1\in\mathcal{V}}\sum_{v_2\in\mathcal{V}}\sum_{y_1,z_1\in\mathcal{I}}\sum_{y_2,z_2\in\mathcal{I}} \boldsymbol{e}_m(a(v_1v_2^{-1}(y_1+z_1)-y_2-z_2)).$$

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

$$J_1 = \frac{|\mathcal{V}|^2L^4}{m} + \frac{1}{m}\sum_{a=1}^{m-1}\sum_{v_1\in\mathcal{V}}\sum_{v_2\in\mathcal{V}}\sum_{y_1,z_1\in\mathcal{I}}\sum_{y_2,z_2\in\mathcal{I}} \boldsymbol{e}_m(a(v_1v_2^{-1}(y_1+z_1)-y_2-z_2)).$$

Since the number of solutions of the congruence

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

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

$$\frac{1}{m}\left|\sum_{a=1}^{m-1}\sum_{v\in\mathcal{V}}\sum_{y_1,z_1\in\mathcal{I}}\sum_{y_2,z_2\in\mathcal{I}} \boldsymbol{e}_m(a(y_1+z_1-y_2-z_2))\right| \leqslant \frac{|\mathcal{V}|}{m}\sum_{a=0}^{m-1}\left|\sum_{y\in\mathcal{I}}\boldsymbol{e}_m(ay_1)\right|^4 \ll |\mathcal{V}|L^3.$$

Therefore,

$$\frac{1}{m}\sum_{a=1}^{m-1}\sum_{v_1\in\mathcal{V}}\sum_{v_2\in\mathcal{V}}\sum_{y_1,z_1\in\mathcal{I}}\sum_{y_2,z_2\in\mathcal{I}} \boldsymbol{e}_m(a(v_1v_2^{-1}(y_1+z_1)-y_2-z_2))$$
$$= O(|\mathcal{V}|L^3) + \frac{1}{m}\sum_{a=1}^{m-1}\sum_{v_1\in\mathcal{V}}\sum_{\substack{v_2\in\mathcal{V}\\ v_2\neq v_1}}\sum_{y_1\in\mathcal{I}}\sum_{y_2\in\mathcal{I}} \boldsymbol{e}_m(a(v_1v_2^{-1}(y_1+z_1)-y_2-z_2)).$$

https://doi.org/10.1017/S0013091505000969 Published online by Cambridge University Press

Using exactly the same argument that we used in the proof of Theorem 1.3, we derive the formula

$$J_1 = \frac{|\mathcal{V}|^2 L^4}{m} + O(|\mathcal{V}|L^3) + O(R),$$

where

$$R = \frac{1}{m} \sum_{a=1}^{m-1} \sum_{\substack{1\leqslant n\leqslant m\\ (n,m)=1}} \left| \sum_{y_1,z_1\in\mathcal{I}} \sum_{y_2,z_2\in\mathcal{I}} \boldsymbol{e}_m(a(n(y_1+z_1)-y_2-z_2)) \right|.$$

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

$$\begin{aligned}
R &= \frac{1}{m} \sum_{\substack{s\mid m\\ s<m}} \sum_{\substack{b\leqslant m/s-1\\ (b,m/s)=1}} \sum_{\substack{1\leqslant n\leqslant m\\ (n,m)=1}} \left| \sum_{y_1,z_1\in\mathcal{I}} \sum_{y_2,z_2\in\mathcal{I}} \boldsymbol{e}_{m/s}(b(n(y_1+z_1)-y_2-z_2)) \right| \\
&\leqslant \frac{1}{m} \sum_{\substack{s\mid m\\ s<m}} s \sum_{\substack{b\leqslant m/s-1\\ (b,m/s)=1}} \sum_{\substack{1\leqslant n\leqslant m/s\\ (n,m/s)=1}} \left| \sum_{y_1,z_1\in\mathcal{I}} \sum_{y_2,z_2\in\mathcal{I}} \boldsymbol{e}_{m/s}(bn(y_1+z_1)-b(y_2+z_2)) \right| \\
&\leqslant \frac{1}{m} \sum_{\substack{s\mid m\\ s<m}} s \Biggl(\sum_{\substack{1\leqslant n\leqslant m/s\\ (n,m/s)=1}} \left| \sum_{y_1,z_1\in\mathcal{I}} \boldsymbol{e}_{m/s}(n(y_1+z_1)) \right| \Biggr)^2 \\
&= \frac{1}{m} \sum_{\substack{s\mid m\\ s<m}} s \Biggl(\sum_{\substack{1\leqslant n\leqslant m/s\\ (n,m/s)=1}} \left| \sum_{y\in\mathcal{I}} \boldsymbol{e}_{m/s}(ny) \right|^2 \Biggr)^2.
\end{aligned}$$

Therefore,

$$J_1 = \frac{|\mathcal{V}|^2 L^4}{m} + O(|\mathcal{V}|L^3) + O(R_1) + O(R_2), \tag{3.1}$$

where

$$R_1 = \frac{1}{m} \sum_{\substack{s\mid m\\ s<m/L}} s \Biggl(\sum_{\substack{1\leqslant n\leqslant m/s\\ (n,m/s)=1}} \left| \sum_{y\in\mathcal{I}} \boldsymbol{e}_{m/s}(ny) \right|^2 \Biggr)^2, \tag{3.2}$$

$$R_2 = \frac{1}{m} \sum_{\substack{s\mid m\\ m/L\leqslant s<m}} s \Biggl(\sum_{\substack{1\leqslant n\leqslant m/s\\ (n,m/s)=1}} \left| \sum_{y\in\mathcal{I}} \boldsymbol{e}_{m/s}(ny) \right|^2 \Biggr)^2. \tag{3.3}$$

If $s<m/L$, then $m/s>L$ and, therefore, the congruence

$$y_1 \equiv y_2 \pmod{m/s}, \quad y_1, y_2 \in \mathcal{I},$$

has L solutions. Hence,

$$\sum_{1\leqslant n\leqslant m/s} \left| \sum_{y\in\mathcal{I}} \boldsymbol{e}_{m/s}(ny) \right|^2 = \frac{mL}{s},$$

https://doi.org/10.1017/S0013091505000969 Published online by Cambridge University Press

whence, using (3.2),

$$\begin{aligned} R_1 &\leqslant \frac{1}{m} \sum_{\substack{s \mid m \\ s<m/L}} s\biggl(\sum_{1\leqslant n\leqslant m/s}\biggl|\sum_{y\in\mathcal{I}} \boldsymbol{e}_{m/s}(ny)\biggr|^2\biggr)^2 \\ &= mL^2 \sum_{\substack{s \mid m \\ s<m/L}} s^{-1} \\ &\leqslant mL^2 \sum_{s\mid m} s^{-1} \\ &\leqslant \frac{m^2L^2}{\phi(m)}. \end{aligned}$$

Inserting this bound into (3.1), we deduce that

$$J = \frac{|\mathcal{V}|^2L^4}{m} + O(|\mathcal{V}|L^3) + O(m^2L^2/\phi(m)) + O(R_2). \tag{3.4}$$

We now proceed to estimate R_2. Note that in (3.3) we have $(n, m/s) = 1$. Therefore, for any integer K,

$$\sum_{y=K+1}^{K+m/s} \boldsymbol{e}_{m/s}(ny) = 0,$$

whence we deduce that there exist integers A and B with $0 < B \leqslant m/s$ such that

$$\sum_{y\in\mathcal{I}} \boldsymbol{e}_{m/s}(ny) = \sum_{A<y\leqslant A+B} \boldsymbol{e}_{m/s}(ny).$$

Hence

$$\begin{aligned} \sum_{\substack{1\leqslant n\leqslant m/s \\ (n,m/s)=1}} \biggl|\sum_{y\in\mathcal{I}} \boldsymbol{e}_{m/s}(ny)\biggr|^2 &= \sum_{\substack{1\leqslant n\leqslant m/s \\ (n,m/s)=1}} \biggl|\sum_{A<y\leqslant A+B} \boldsymbol{e}_{m/s}(ny)\biggr|^2 \\ &\leqslant \sum_{n=1}^{m/s} \biggl|\sum_{A<y\leqslant A+B} \boldsymbol{e}_{m/s}(ny)\biggr|^2 \\ &= mB/s \leqslant m^2/s^2. \end{aligned}$$

Taking this into account, from (3.3) we deduce that

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

Therefore, in view of (3.4), we obtain the asymptotic formula

$$\begin{aligned} J_1 &= \frac{|\mathcal{V}|^2L^4}{m} + O(|\mathcal{V}|L^3) + O(m^2L^2/\phi(m)) \\ &= \frac{|\mathcal{V}|^2L^4}{m}\biggl(1 + O\biggl(\frac{m}{|\mathcal{V}|L} + \frac{m^3}{\phi(m)|\mathcal{V}|^2L^2}\biggr)\biggr). \end{aligned}$$

https://doi.org/10.1017/S0013091505000969 Published online by Cambridge University Press

Recalling that $|\mathcal{V}| \gg m^{1/2}/\log m$ and

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

we arrive at the formula

$$J_1 = \frac{|\mathcal{V}|^2 L^4}{m}(1 + O(\Delta^{-1})).$$

Next, define

$$\mathcal{H} = \{q(y+z) \pmod m,\ q \in \mathcal{V},\ [S/2]+1 \leqslant y, z \leqslant [S/2]+L\}.$$

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

$$q(y+z) \equiv h \pmod m, \quad q \in \mathcal{V},\ [S/2]+1 \leqslant y, z \leqslant [S/2]+L.$$

Then

$$J_1 = \sum_{h\in\mathcal{H}} I^2(h) \geqslant \frac{1}{|\mathcal{H}|}\biggl(\sum_{h\in\mathcal{H}} I(h)\biggr)^2 = \frac{1}{|\mathcal{H}|}|\mathcal{V}|^2 L^4.$$

Therefore,

$$|\mathcal{H}| \geqslant \frac{|\mathcal{V}|^2 L^4}{J_1} = \frac{m}{1+O(\Delta^{-1})} = (1+O(\Delta^{-1}))m.$$

The result now follows in view of $|\mathcal{H}| \leqslant m$.

4. Proof of Theorem 1.4

Set

$$S = \sum_{a=1}^{p-1}\biggl|\sum_{q\in\mathcal{P}}\sum_{x=1}^{p}\sum_{y=1}^{p}\alpha_x\beta_y \boldsymbol{e}_p(aq(x+y))\biggr|^2.$$

In the identity

$$\sum_{a=1}^{p-1}\boldsymbol{e}_p(au) = \begin{cases} -1, & \text{if } u \not\equiv 0 \pmod p,\\ p-1, & \text{if } u \equiv 0 \pmod p,\end{cases}$$

we successively take $u = q_1(x_1+y_1) - q_2(x_2+y_2)$ and then

$$u = q_1 q_2^{-1}(x_1+y_1) - (x_2+y_2),$$

where q_2^{-1} is defined from $q_2 q_2^{-1} \equiv 1 \pmod p$, and obtain

$$\sum_{a=1}^{p-1}\boldsymbol{e}_p(a(q_1(x_1+y_1) - q_2(x_2+y_2))) = \sum_{a=1}^{p-1}\boldsymbol{e}_p(a(q_1 q_2^{-1}(x_1+y_1) - (x_2+y_2))).$$

Multiplying both sides by $\alpha_{x_1}\bar{\alpha}_{x_2}\beta_{y_1}\bar{\beta}_{y_2}$, performing the summation over

$$q_1, q_2 \in \mathcal{P}, \quad 1 \leqslant x_1, x_2, y_1, y_2 \leqslant p,$$

https://doi.org/10.1017/S0013091505000969 Published online by Cambridge University Press

and then changing the order of summation, we obtain

$$S=\sum_{a=1}^{p-1}\sum_{\substack{q_1\in\mathcal{P}\\ q_2\in\mathcal{P}}}\sum_{\substack{x_1\in\mathbb{Z}_p\\ x_2\in\mathbb{Z}_p}}\sum_{\substack{y_1\in\mathbb{Z}_p\\ y_2\in\mathbb{Z}_p}}\alpha_{x_1}\bar{\alpha}_{x_2}\beta_{y_1}\bar{\beta}_{y_2}\boldsymbol{e}_p(aq_1q_2^{-1}(x_1+y_1)-a(x_2+y_2)),$$

where $\mathbb{Z}_p=\{1,2\dots,p\}$. The contribution to S which comes from the case $q_1=q_2$ is equal to

$$|\mathcal{P}|\sum_{a=1}^{p-1}\sum_{\substack{x_1\in\mathbb{Z}_p\\ x_2\in\mathbb{Z}_p}}\sum_{\substack{y_1\in\mathbb{Z}_p\\ y_2\in\mathbb{Z}_p}}\alpha_{x_1}\bar{\alpha}_{x_2}\beta_{y_1}\bar{\beta}_{y_2}\boldsymbol{e}_p(a(x_1+y_1-x_2-y_2))$$
$$=|\mathcal{P}|\sum_{a=1}^{p-1}\biggl|\sum_{x=1}^{p}\sum_{y=1}^{p}\alpha_x\beta_y\boldsymbol{e}_p(a(x+y))\biggr|^2.$$

Therefore,

$$S=|\mathcal{P}|\sum_{a=1}^{p-1}\biggl|\sum_{x=1}^{p}\sum_{y=1}^{p}\alpha_x\beta_y\boldsymbol{e}_p(a(x+y))\biggr|^2+S_1,$$

where

$$S_1=\sum_{a=1}^{p-1}\sum_{\substack{q_1\in\mathcal{P}\\ q_2\in\mathcal{P}\\ q_1\neq q_2}}\sum_{\substack{x_1\in\mathbb{Z}_p\\ x_2\in\mathbb{Z}_p}}\sum_{\substack{y_1\in\mathbb{Z}_p\\ y_2\in\mathbb{Z}_p}}\alpha_{x_1}\bar{\alpha}_{x_2}\beta_{y_1}\bar{\beta}_{y_2}\boldsymbol{e}_p(aq_1q_2^{-1}(x_1+y_1)-a(x_2+y_2)).$$

Hence, if we prove that $|S_1|\leqslant p^2I_1I_2$, then we are done. To this end, we observe that

$$|S_1|\leqslant\sum_{a=1}^{p-1}\sum_{n=1}^{p-1}r(n)\biggl|\sum_{\substack{x_1\in\mathbb{Z}_p\\ x_2\in\mathbb{Z}_p}}\sum_{\substack{y_1\in\mathbb{Z}_p\\ y_2\in\mathbb{Z}_p}}\alpha_{x_1}\bar{\alpha}_{x_2}\beta_{y_1}\bar{\beta}_{y_2}\boldsymbol{e}_p(an(x_1+y_1)-a(x_2+y_2))\biggr|,$$

where $r(n):=r_{\mathcal{P}}(n)$ denotes the number of solutions of the representation

$$q_1q_2^{-1}\equiv n\ (\mathrm{mod}\,p),\quad q_1,q_2\in\mathcal{P},\quad q_1\neq q_2.$$

From the definition of the set $\mathcal{P}$ we derive that $r(n)\leqslant 1$. Hence,

$$|S_1|\leqslant\sum_{a=1}^{p-1}\sum_{n=1}^{p-1}\biggl|\sum_{\substack{x_1\in\mathbb{Z}_p\\ x_2\in\mathbb{Z}_p}}\sum_{\substack{y_1\in\mathbb{Z}_p\\ y_2\in\mathbb{Z}_p}}\alpha_{x_1}\bar{\alpha}_{x_2}\beta_{y_1}\bar{\beta}_{y_2}\boldsymbol{e}_p(an(x_1+y_1)-a(x_2+y_2))\biggr|.$$

When n runs through the reduced residue system modulo p, an runs through the same system for any fixed $a\not\equiv 0\ (\mathrm{mod}\,p)$. Therefore,

$$|S_1|\leqslant\biggl(\sum_{a=1}^{p-1}\biggl|\sum_{x=1}^{p}\sum_{y=1}^{p}\alpha_x\beta_y\boldsymbol{e}_p(a(x+y))\biggr|\biggr)^2$$
$$=\biggl(\sum_{a=1}^{p-1}\biggl|\sum_{x=1}^{p}\alpha_x\boldsymbol{e}_p(ax)\biggr|\biggl|\sum_{y=1}^{p}\beta_y\boldsymbol{e}_p(ay)\biggr|\biggr)^2.$$

https://doi.org/10.1017/S0013091505000969 Published online by Cambridge University Press

Applying the Cauchy inequality, we obtain

$$|S_1| \leqslant \biggl(\sum_{a=0}^{p-1}\biggl|\sum_{x=1}^{p}\alpha_x \boldsymbol{e}_p(ax)\biggr|^2\biggr)\biggl(\sum_{a=0}^{p-1}\biggl|\sum_{y=1}^{p}\beta_y \boldsymbol{e}_p(ay)\biggr|^2\biggr) = p^2 I_1 I_2,$$

which concludes our proof of Theorem 1.4.

5. Proof of Theorem 1.6

The proof proceeds along exactly the same lines as that of Theorem 1.4: by remarking that, for any given residue class n, the congruence

$$z_1 z_2^{-1} \equiv n \pmod p, \quad z_1, z_2 \in \mathcal{Z}, \ (z_1, z_2) = 1,$$

has at most one solution.

6. Proof of Theorem 1.7

Without loss of generality we may suppose that

$$0 < N < N + \Delta p^{1/2} < p, \qquad 0 < M < M + \Delta p^{1/2} < p.$$

Define $X = [\Delta p^{1/2}/2]$, $N_1 = [N/2]$, $S_1 = [S/2]$, and let $\mathcal{H}^*$ be the set of all residue classes of the form $(x+t)(y+z)^{-1} \pmod p$, where

$$N_1 + 1 \leqslant x, t \leqslant N_1 + X, \qquad S_1 + 1 \leqslant y, z \leqslant S_1 + X.$$

Obviously,

$$N + 1 \leqslant x + t \leqslant N + \Delta p^{1/2}, \qquad S + 1 \leqslant y + z \leqslant S + \Delta p^{1/2}.$$

Next, let

$$\mathcal{H}_1^* = \{h \pmod p : h \notin \mathcal{H}^*, \ h \not\equiv 0 \pmod p\}.$$

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 conditions

$$h \in \mathcal{H}_1^*, \qquad N_1 + 1 \leqslant x, t \leqslant N_1 + X, \qquad S_1 + 1 \leqslant y, z \leqslant S_1 + X.$$

Therefore,

$$\sum_{a=0}^{p-1} \sum_{h \in \mathcal{H}_1^*} \sum_{x,t \in \mathcal{I}_1} \sum_{y,z \in \mathcal{I}_2} \boldsymbol{e}_p(a(x + t - h(y+z))) = 0,$$

where $\mathcal{I}_1$ and $\mathcal{I}_2$ denote the intervals $[N_1+1, N_1+X]$ and $[S_1+1, S_1+X]$, respectively.

https://doi.org/10.1017/S0013091505000969 Published online by Cambridge University Press

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

$$|\mathcal{H}_1^*|X^4 \leqslant \sum_{a=1}^{p-1} \left| \sum_{x,t\in\mathcal{I}_1} \boldsymbol{e}_p(a(x+t)) \right| \left| \sum_{y,z\in\mathcal{I}_2} \sum_{h\in\mathcal{H}_1^*} \boldsymbol{e}_p(ah(y+z)) \right|.$$

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

$$\begin{aligned}\left| \sum_{y,z\in\mathcal{I}_2} \sum_{h\in\mathcal{H}_1^*} \boldsymbol{e}_p(ah(y+z)) \right| &\leqslant \sum_{h\in\mathcal{H}_1^*} \left| \sum_{y,z\in\mathcal{I}_2} \boldsymbol{e}_p(ah(y+z)) \right| \\ &\leqslant \sum_{h=1}^{p-1} \left| \sum_{y,z\in\mathcal{I}_2} \boldsymbol{e}_p(ah(y+z)) \right| \\ &\leqslant \sum_{h=0}^{p-1} \left| \sum_{y,z\in\mathcal{I}_2} \boldsymbol{e}_p(h(y+z)) \right| \\ &= pX,\end{aligned}$$

and, similarly,

$$\sum_{a=1}^{p-1} \left| \sum_{x,t\in\mathcal{I}_1} \boldsymbol{e}_p(a(x+t)) \right| \leqslant pX.$$

Hence,

$$|\mathcal{H}_1^*|X^4 \leqslant p^2X^2,$$

whence

$$|\mathcal{H}_1^*| \leqslant \frac{p^2}{X^2} \ll p\Delta^{-2}.$$

Since $|\mathcal{H}| = p - 1 - |\mathcal{H}_1^*|$, the result follows.

Acknowledgements. The authors are highly thankful to the anonymous referee for many useful comments.

References

1. M. Z. Garaev, Character sums in short intervals and the multiplication table modulo a prime, *Monatsh. Math.* **148** (2006), 127–138.
2. M. Z. Garaev, On the logarithmic factor in error term estimates in certain additive congruence problems, *Acta. Arith.* **124** (2006), 27–39.
3. M. Z. Garaev and A. A. Karatsuba, On character sums and the exceptional set of a congruence problem, *J. Number Theory* **114** (2005), 182–192.
4. M. Z. Garaev and K.-L. Kueh, Distribution of special sequences modulo a large prime, *Int. J. Math. Math. Sci.* **50** (2003), 3189–3194.
5. Z. Rudnik, P. Sarnak and A. Zaharescu, The distribution of spacings between the fractional parts of $n^2\alpha$, *Invent. Math.* **145**(1) (2001), 37–57.
6. M. Vâjâitu and A. Zaharescu, Differences between powers of a primitive root, *Int. J. Math. Math. Sci.* **29**(2) (2002), 325–331.