Available online at www.sciencedirect.com
ScienceDirect
Journal of Number Theory 128 (2008) 2520–2537
JOURNAL OF Number Theory
www.elsevier.com/locate/jnt

The equation $x_1x_2 = x_3x_4 + \lambda$ in fields of prime order and applications

M.Z. Garaev, V.C. Garcia *

Instituto de Matemáticas, Universidad Nacional Autónoma de México, Campus Morelia, Apartado Postal 61-3 (Xangari), CP 58089, Morelia, Michoacán, Mexico

Received 14 March 2007; revised 7 February 2008

Available online 13 June 2008

Communicated by K. Soundararajan

Abstract

Let p be a prime number, λ be an integer. We obtain new results related to the congruence $x_1x_2 \equiv x_3x_4 + \lambda \pmod p$.

MSC: 11A07; 11B50; 11B75; 11L07

Keywords: Congruences; Number of solutions; Asymptotic formulae; Character sums

1. Introduction

The congruence

$$x_1x_2 \equiv x_3x_4 \pmod p, \tag{1}$$

where p is a large prime, arises in many problems of number theory. Distribution properties of its solutions are proved to be important in many applications, see, for example, [1,5,7,9,13,14].

* Corresponding author.
E-mail addresses: garaev@matmor.unam.mx (M.Z. Garaev), garci@matmor.unam.mx (V.C. Garcia).

0022-314X/$ – see front matter
doi:10.1016/j.jnt.2008.02.017

Let L_i, N_i, $1 \leqslant i \leqslant 4$, be integers with $0 \leqslant L_i < L_i + N_i < p$. Denote by J the number of solutions of congruence (1) in the box

$$L_i + 1 \leqslant x_i \leqslant L_i + N_i \quad (1 \leqslant i \leqslant 4). \tag{2}$$

In view of the identity

$$\sum_{\chi} \chi(u) = \begin{cases} 0, & \text{if } u \not\equiv 1 \pmod p, \\ p-1, & \text{if } u \equiv 1 \pmod p, \end{cases}$$

where χ runs through the set of multiplicative characters modulo p, the value J can be expressed in terms of character sums

$$J = \frac{1}{p-1} \sum_{\chi} \sum_{x_1,x_2,x_3,x_4} \chi\big(x_1 x_2 x_3^* x_4^*\big),$$

where x^* denotes the multiplicative inverse of $x \pmod p$ and the range for the variables in summations over x_1, x_2, x_3, x_4 is defined by (2). The principal character $\chi = \chi_0$ contributes to the sum the quantity $N_1N_2N_3N_4/(p-1)$, which in many occasions indicates the asymptotic behavior of the value J. Ayyad, Cochrane and Zheng [1] proved that

$$J = \frac{N_1N_2N_3N_4}{p} + O\big(\sqrt{N_1N_2N_3N_4}\log^2 p\big). \tag{3}$$

They expressed the hope that the factor $\log^2 p$ can be replaced by $\log p$ which would be the best possible error term in general settings, see the discussion [1, p. 399]. In the special case $N_1 = N_2$, $N_3 = N_4$ or $N_1 = N_3$, $N_2 = N_4$, they proved that

$$J \approx \frac{N_1N_2N_3N_4}{p} + O(\sqrt{N_1N_2N_3N_4}\log p), \tag{4}$$

saving one factor $\log p$ at the cost of the asymptotic formula.

As consequences of (3) and (4) the authors of [1] claimed the following bounds for the fourth moments of character sums: for any integers L and $N > 0$ we have

$$\frac{1}{p-1} \sum_{\chi \neq \chi_0} \left| \sum_{x=L+1}^{L+N} \chi(x) \right|^4 \ll N^2 \log^2 p; \tag{5}$$

if in addition $N \ll \sqrt{p \log p}$, then

$$\frac{1}{p-1} \sum_{\chi \neq \chi_0} \left| \sum_{x=L+1}^{L+N} \chi(x) \right|^4 \ll N^2 \log p. \tag{6}$$

These results sharpen the one of Friedlander and Iwaniec [6, Lemma 3] where they had $N^2 \log^6 p$ instead of $N^2 \log^2 p$ in the right-hand side of (5); we remark that the proof of [6, Lemma 3] seems to contain a minor omission in the power of the logarithmic factor when Hölder's inequality is

applied and there apparently should be $N^2\log^8 p$ instead of $N^2\log^6 p$. Similar estimates can be found in Vaughan [16, p. 184], see also Harman [11, Lemma 2]. The methods of [6,11] and [16] apply for general modulus, but restricted to $L=0$.

As it was mentioned in [1], the work of Montgomery and Vaughan [12] implies the bound

$$\frac{1}{p-1}\sum_{\chi\neq\chi_0}\max_N\left|\sum_{x=1}^{N}\chi(x)\right|^4\ll p^2;$$

in particular, when N is close to p in (5) one can remove the factor $\log^2 p$. The work of Burgess [4] implies the inequality

$$\frac{1}{p}\sum_{L=1}^{p}\left\{\frac{1}{p-1}\sum_{\chi\neq\chi_0}\left|\sum_{x=L+1}^{L+N}\chi(x)\right|^4\right\}\ll N^2,$$

which illustrates that on average over L one also can remove the factor $\log^2 p$.

2. New error term for J

The first result of our present paper is as follows:

Theorem 1. *The following asymptotic formula holds*:

$$J=\frac{N_1N_2N_3N_4}{p}+O\big(\sqrt{N_1N_2N_3N_4}\big(\sqrt{\log p}+\delta(N_1N_2)\big)\big(\sqrt{\log p}+\delta(N_3N_4)\big)\big),\qquad(7)$$

where

$$\delta(X)=\begin{cases}0, & \text{if } X\leqslant p,\\ \log\frac{X}{p}, & \text{if } X\geqslant p.\end{cases}$$

The equality in (7) *also holds if the products N_1N_2 and N_3N_4 are replaced with any other pairing of the N_i.*

Theorem 1 implies the following bound on the fourth moment of character sums:

$$\frac{1}{p-1}\sum_{\chi\neq\chi_0}\left|\sum_{x=L+1}^{L+N}\chi(x)\right|^4\ll N^2\left(\log p+\log^2\frac{N^2}{p}\right).$$

In particular, estimate (6) holds in the range $N\ll p^{1/2}e^{c\sqrt{\log p}}$ for any fixed positive constant c.

Furthermore, Theorem 1 implies the asymptotic behavior $J\sim N_1N_2N_3N_4/p$ in a wider range of parameters than the one suggested by (3). For example, if $N_1=N_2=N_3=N_4=N$ and if

$$\frac{N}{p^{1/2}(\log p)^{1/2}}\to\infty,\quad p\to\infty,$$

then

$$J = \frac{N^4}{p}\big(1 + o(1)\big),$$

while formula (3) implies this asymptotic formula when

$$\frac{N}{p^{1/2}\log p} \to \infty, \quad p \to \infty.$$

Using our Theorem 1 we can get the following result on the representability of residue classes by products of small integers.

Theorem 2. *Let $N_1N_2 = \Delta p \log p$, where $\Delta = \Delta(p) \to \infty$ as $p \to \infty$. Then the set*

$$\big\{xy \pmod p\colon\ L_1 + 1 \leqslant x \leqslant L_1 + N_1,\ L_2 + 1 \leqslant y \leqslant L_2 + N_2\big\}$$

contains $(1 + O(\frac{1}{\Delta} + \frac{\log^2 \Delta}{\Delta \log p}))p$ residue classes modulo p. In particular, this set contains almost all residue classes modulo p.

We recall that the work of Tenenbaum [15] implies that if

$$L_1 = L_2 = 0, \qquad N_1 = N_2 = N \leqslant p^{1/2}(\log p)^{0.5\kappa - \varepsilon},$$

where $\kappa = 1 - (\log(e\log 2))/\log 2 \approx 0.08607\ldots$, then the set defined in Theorem 2 contains only $o(p)$ residue classes modulo p. The result of [9] implies that the set

$$\big\{qy \pmod p\colon\ q \leqslant p^{1/2},\ L + 1 \leqslant y \leqslant L + \Delta p^{1/2}\log p\big\},$$

where q denotes prime numbers, contains $(1 + O(\Delta^{-1}))p$ residue classes modulo p. This result can be stated in more general settings and has its version for composite modulus as well. For further information on this subject we refer the reader to [9], to the works of Shparlinski [13,14], and therein references.

3. Combinatorial properties and solvability

From (3) it is immediate that if $N_1N_2N_3N_4 > cp^2\log^4 p$, where c is a suitable constant, then the box (2) contains a solution of (1). Ayyad, Cochrane and Zheng [1] asked whether the factor $\log^4 p$ can be removed altogether. Our next result shows that the factor $\log^4 p$ can be relaxed to $\log p$. In the case if N_1N_3 and N_2N_4 are of the same order of magnitude, we will prove that one indeed can remove $\log^4 p$ altogether.

Theorem 3. *There exists a constant c such that if $N_1N_2N_3N_4 > cp^2\log p$ then the box* (2) *contains a solution of* (1).

The proof of Theorem 3 uses an idea from [9, Theorem 1.7] and relies upon trigonometric sums.

It is to be remarked that in a series of papers the problem of representability of the zero by a nonsingular quadratic form $Q(x_1, x_2, x_3, x_4) \pmod p$ in short intervals has been investigated. It is known that in the problem of solvability of the congruence

$$Q(x_1, x_2, x_3, x_4) \equiv \lambda \pmod p$$

the case $\lambda \not\equiv 0 \pmod p$ essentially differs from the case $\lambda \equiv 0 \pmod p$, see the question raised in [5, p. 176]. A similar situation occurs in our problem as well. Consider the equation

$$x_1 x_2 \equiv x_3 x_4 + \lambda \pmod p. \tag{8}$$

Theorem 3 corresponds to the case $\lambda \equiv 0 \pmod p$. For arbitrary λ, Theorems 1, 2 together with Lemmas 3, 4 imply that for some numerical constant $c > 0$, if $N_1 N_2 N_3 N_4 > cp^2 \log^3 p$, then for any integer λ the box (2) contains a solution of (8). The question is whether the factor $\log^3 p$ can be removed altogether (note that if, for example, $N_1 N_2$ is about of the same order of magnitude as $N_3 N_4$, one can change $\log^3 p$ to $\log^2 p$). A possible approach to this question is the study of combinatorial aspects of Eq. (8). For given subsets $\mathcal{U}$ and $\mathcal{V}$ of the residue field $\mathbb{F}_p$, we recall that

$$\mathcal{U} + \mathcal{V} = \{u + v\colon\ u \in \mathcal{U},\ v \in \mathcal{V}\}, \qquad \mathcal{U} - \mathcal{V} = \{u - v\colon\ u \in \mathcal{U},\ v \in \mathcal{V}\},$$
$$k\mathcal{U} = \{u_1 + \cdots + u_k\colon\ u_i \in \mathcal{U},\ 1 \leqslant i \leqslant k\}, \qquad \mathcal{U}\mathcal{V} = \{uv\colon\ u \in \mathcal{U},\ v \in \mathcal{V}\}.$$

By $|\mathcal{U}|$ we denote the cardinality of $\mathcal{U}$. Glibichuk [10] proved that if $\mathcal{A}$ and $\mathcal{B}$ are subsets of $\mathbb{F}_p$ with $|\mathcal{A}||\mathcal{B}| \geqslant 2p$, then

$$8\mathcal{A}\mathcal{B} = \mathbb{F}_p.$$

One can observe that the result of [10] (see the inequality at the end of the proof of [10, Theorem 1]) also implies that

$$2(2\mathcal{A})(2\mathcal{B}) = \mathbb{F}_p, \qquad (2\mathcal{A})(2\mathcal{B}) - (2\mathcal{A})(2\mathcal{B}) = \mathbb{F}_p.$$

In particular, for any integer λ, if $N_1 N_2 > 10p$, the congruence (8) is solvable with

$$L_1 + 1 \leqslant x_1, x_3 \leqslant L_1 + N_1, \qquad L_2 + 1 \leqslant x_2, x_4 \leqslant L_2 + N_2.$$

This observation naturally leads to the following conjecture.

Conjecture 1. *There exists a positive constant c such that if $\mathcal{A}, \mathcal{B}, \mathcal{C}, \mathcal{D}$ are subsets of $\mathbb{F}_p \setminus \{0\}$ with $|\mathcal{A}||\mathcal{B}||\mathcal{C}||\mathcal{D}| > cp^2$, then*

$$(2\mathcal{A})(2\mathcal{B}) + (2\mathcal{C})(2\mathcal{D}) = \mathbb{F}_p.$$

Validity of this conjecture would remove the logarithmic factors in the above mentioned results and, in particular, would affirmatively solve the mentioned question from [1]. The use of trigonometric sums in conjunction with combinatorial arguments from [2,3,10] allows us to establish Conjecture 1 in certain important cases.

Theorem 4. *Let $\mathcal{A}, \mathcal{B}, \mathcal{C}, \mathcal{D}$ be subsets of $\mathbb{F}_p \setminus \{0\}$ such that*

$$|\mathcal{A}||\mathcal{C}| > (2+\sqrt{2})p, \qquad |\mathcal{B}||\mathcal{D}| > (2+\sqrt{2})p.$$

Then

$$(2\mathcal{A})(2\mathcal{B}) + (2\mathcal{C})(2\mathcal{D}) = \mathbb{F}_p.$$

In particular, if $N_1N_3 > 15p$, $N_2N_4 > 15p$, then for any integer λ the box (2) contains a solution of the congruence

$$x_1x_2 \equiv x_3x_4 + \lambda \pmod{p}.$$

4. Notations and lemmas

Throughout the text we will use the abbreviation

$$\mathbf{e}_p(z) = \exp(2\pi i z/p).$$

For a given nonzero element $x \in \mathbb{F}_p$ we use x^* to denote its multiplicative inverse. We also recall the basic identity

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

which is useful in calculations of the number of solutions of various congruences.

The underlying idea of the proof of Theorem 1 is based on the combination of the methods from [1] and [8]. In particular, we need the following lemma from [1].

Lemma 1. *The following bound holds*:

$$J \ll \frac{N_1N_2N_3N_4}{p} + (p + N_1N_2\log p)^{1/2}(p + N_3N_4\log p)^{1/2}.$$

Moreover, the inequality holds if the products N_1N_2 and N_3N_4 are replaced with any other pairing of the N_i.

Lemma 2. *In order to prove Theorem* 1 *it is sufficient to establish* (7) *in the case $L_1 = L_3$, $L_2 = L_4$, $N_1 = N_3$, $N_2 = N_4$.*

Proof. The proof is similar to the argument described in [1, p. 408]. We have

$$J = \frac{1}{p-1} \sum_{\chi} \sum_{x_1=L_1+1}^{L_1+N_1} \sum_{x_2=L_2+1}^{L_2+N_2} \sum_{x_3=L_3+1}^{L_3+N_3} \sum_{x_4=L_4+1}^{L_4+N_4} \chi\left(x_1x_2x_3^*x_4^*\right).$$

Picking up the term corresponding to the principal character $\chi = \chi_0$ and then applying the Cauchy–Schwarz inequality, we obtain

$$J - \frac{N_1N_2N_3N_4}{p-1} \ll \sqrt{S_1S_2},$$

where

$$S_1 = \frac{1}{p-1}\sum_{\chi\neq\chi_0}\left|\sum_{x_1=L_1+1}^{L_1+N_1}\sum_{x_2=L_2+1}^{L_2+N_2}\chi(x_1x_2)\right|^2,$$

$$S_2 = \frac{1}{p-1}\sum_{\chi\neq\chi_0}\left|\sum_{x_3=L_3+1}^{L_3+N_3}\sum_{x_4=L_4+1}^{L_4+N_4}\chi\left(x_3^*x_4^*\right)\right|^2.$$

Clearly,

$$S_1 = J' - \frac{N_1^2N_3^2}{p-1}, \qquad S_2 = J'' - \frac{N_2^2N_4^2}{p-1},$$

where J' is the number of solutions of the congruence

$$x_1x_2 \equiv y_1y_2 \pmod p, \quad L_1+1 \leqslant x_1, y_1 \leqslant L_1+N_1,\ L_2+1 \leqslant x_2, y_2 \leqslant L_2+N_2$$

and J'' is the number of solutions of the congruence

$$x_3x_4 \equiv y_3y_4 \pmod p, \quad L_3+1 \leqslant x_3, y_3 \leqslant L_3+N_3,\ L_4+1 \leqslant x_4, y_4 \leqslant L_4+N_4.$$

Therefore, assuming that (7) holds in the case $L_1 = L_3$, $L_2 = L_4$, $N_1 = N_3$, $N_2 = N_4$, we obtain

$$S_1 \ll N_1N_2\left(\sqrt{\log p} + \delta(N_1N_2)\right)^2, \qquad S_2 \ll N_3N_4\left(\sqrt{\log p} + \delta(N_3N_4)\right)^2.$$

The case of pairing $\delta(N_1N_3)$ and $\delta(N_2N_4)$ is dealt with analogously; the only difference is that in this case we define S_1, S_2 as

$$S_1 = \frac{1}{p-1}\sum_{\chi\neq\chi_0}\left|\sum_{x_1=L_1+1}^{L_1+N_1}\sum_{x_3=L_3+1}^{L_3+N_3}\chi\left(x_1x_3^*\right)\right|^2,$$

$$S_2 = \frac{1}{p-1}\sum_{\chi\neq\chi_0}\left|\sum_{x_2=L_2+1}^{L_2+N_2}\sum_{x_4=L_4+1}^{L_4+N_4}\chi\left(x_2x_4^*\right)\right|^2. \qquad \square$$

The following well-known statement is very useful in estimating of cardinalities of sets via the number of solutions of the associated equation.

Lemma 3. *Let s_n be any sequence of elements (not necessarily distinct) of the residue field $\mathbb{F}_p$. Let $M \geqslant 1$ be an integer. If I denotes the number of solutions of the equation*

$$s_n = s_m, \quad 1 \leqslant n, m \leqslant M,$$

then

$$\#\{s_n\colon\ 1 \leqslant n \leqslant M\} \geqslant \frac{M^2}{I}.$$

Proof. Indeed, for a given $\lambda \in \{s_n\colon\ 1 \leqslant n \leqslant M\}$ denote by $I(\lambda)$ the number of solutions of the equation $s_n = \lambda$. Then,

$$\sum_{\lambda} I(\lambda) = M, \qquad \sum_{\lambda} I^2(\lambda) = I,$$

where in the summations λ runs through the set $\{s_n\colon\ 1 \leqslant n \leqslant M\}$. The required estimate now follows from the Cauchy–Schwarz inequality. □

The following lemma is a weaker form of the mentioned in Section 1 result from [1].

Lemma 4. *If $N_1 = N_2$, $N_3 = N_4$ and $N_2N_4 \ll p$, then*

$$J \ll N_2N_4 \log p.$$

Note that Lemma 4 can also be viewed as a particular case of Theorem 1.

5. Proof of Theorem 1

According to Lemma 2 it is sufficient to deal with the case

$$L_1 = L_3, \qquad L_2 = L_4, \qquad N_1 = N_3, \qquad N_2 = N_4.$$

Thus, in this case J denotes the number of solutions of the congruence

$$x_1x_2x_3^* \equiv x_4 \pmod{p}$$

with variables subject to the conditions

$$L_1 + 1 \leqslant x_1, x_3 \leqslant L_1 + N_1, \qquad L_2 + 1 \leqslant x_2, x_4 \leqslant L_2 + N_2.$$

Our aim is to prove that

$$J - \frac{N_1^2N_2^2}{p} \ll N_1N_2\bigl(\log p + \bigl(\delta(N_1N_2)\bigr)^2\bigr).$$

We can assume that $N_1 \geqslant 10$, $N_2 \geqslant 10$. Following the idea of [8], we first take two positive integer parameters $M_1 \leqslant N_1/2$, $M_2 \leqslant N_2/2$, to be explicitly defined later on. Define J_1 to be the number of solutions of the congruence

$$(x_1 + y_1)x_2x_3^* \equiv x_4 + y_4 \pmod{p}$$

subject to the conditions

$$\begin{aligned} L_1 + 1 \leqslant x_1 \leqslant L_1 + N_1 - M_1, &\qquad 1 \leqslant y_1 \leqslant M_1, \\ L_2 + 1 \leqslant x_2 \leqslant L_2 + N_2, &\qquad L_1 + 1 \leqslant x_3 \leqslant L_1 + N_1, \\ L_2 + 1 \leqslant x_4 \leqslant L_2 + N_2 - M_2, &\qquad 1 \leqslant y_4 \leqslant M_2. \end{aligned} \tag{9}$$

By J_2 we denote the number of solutions of the congruence

$$(x_1 - y_1)x_2x_3^* \equiv x_4 - y_4 \pmod{p}$$

subject to the conditions

$$\begin{aligned} L_1 + 1 \leqslant x_1 \leqslant L_1 + N_1 + M_1, &\qquad 1 \leqslant y_1 \leqslant M_1, \\ L_2 + 1 \leqslant x_2 \leqslant L_2 + N_2, &\qquad L_1 + 1 \leqslant x_3 \leqslant L_1 + N_1, \\ L_2 + 1 \leqslant x_4 \leqslant L_2 + N_2 + M_2, &\qquad 1 \leqslant y_4 \leqslant M_2. \end{aligned} \tag{10}$$

Then,

$$\frac{J_1}{M_1M_2} \leqslant J \leqslant \frac{J_2}{M_1M_2}. \tag{11}$$

We shall prove that for suitably chosen M_1 and M_2 the following estimates hold:

$$\frac{J_1}{M_1M_2} - \frac{N_1^2N_2^2}{p} \ll N_1N_2\bigl(\log p + \bigl(\delta(N_1N_2)\bigr)^2\bigr),$$

$$\frac{J_2}{M_1M_2} - \frac{N_1^2N_2^2}{p} \ll N_1N_2\bigl(\log p + \bigl(\delta(N_1N_2)\bigr)^2\bigr).$$

This will finish the proof of Theorem 1.

We express J_1 in terms of trigonometric sums, that is

$$J_1 = \frac{1}{p} \sum_{-(p-1)/2 \leqslant a \leqslant (p-1)/2} \sum_{x_1,x_2,x_3,x_4,y_1,y_4} \mathbf{e}_p\bigl(a\bigl((x_1 + y_1)x_2x_3^* - x_4 - y_4\bigr)\bigr),$$

where the variables are subject to (9). Picking up the term corresponding to $a = 0$, we obtain

$$J_1 - \frac{N_1N_2(N_1-M_1)(N_2-M_2)M_1M_2}{p} \ll \frac{1}{p}\sum_{1\leqslant a\leqslant (p-1)/2} f(a)\Big|\sum_{x_1,x_2,x_3,y_1} \mathbf{e}_p\big(a(x_1+y_1)x_2x_3^*\big)\Big|,$$

where

$$f(a) = \min\big(N_2,\, p/|a|\big)\min\big(M_2,\, p/|a|\big).$$

For $1 \leqslant |b| \leqslant (p-1)/2$ let $I(a,b)$ be the number of solutions of the congruence

$$ax_2x_3^* \equiv b \pmod p, \quad L_2+1 \leqslant x_2 \leqslant L_2+N_2,\ L_1+1 \leqslant x_3 \leqslant L_1+N_1.$$

Then,

$$J_1 - \frac{N_1N_2(N_1-M_1)(N_2-M_2)M_1M_2}{p} \ll \frac{1}{p}\sum_{1\leqslant a\leqslant (p-1)/2}\ \sum_{1\leqslant |b|\leqslant (p-1)/2} f(a)g(b)I(a,b),$$

where

$$g(b) = \min\big(N_1,\, p/|b|\big)\min\big(M_1,\, p/|b|\big).$$

Without loss of generality, we can remove the sign of the modulus from $|b|$ (by reflecting the interval of the range of x_3 with respect to the point $p/2$). Define the following intervals:

$$\mathcal{A}_1 = [1,\, p/N_2]\cap\mathbb{Z}, \qquad \mathcal{A}_2 = [p/N_2,\, p/M_2]\cap\mathbb{Z}, \qquad \mathcal{A}_3 = \big[p/M_2,\, (p-1)/2\big]\cap\mathbb{Z},$$

$$\mathcal{B}_1 = [1,\, p/N_1]\cap\mathbb{Z}, \qquad \mathcal{B}_2 = [p/N_1,\, p/M_1]\cap\mathbb{Z}, \qquad \mathcal{B}_3 = \big[p/M_1,\, (p-1)/2\big]\cap\mathbb{Z}.$$

Thus, we have

$$J_1 - \frac{N_1N_2(N_1-M_1)(N_2-M_2)M_1M_2}{p} \ll \sum_{\nu=1}^{3}\sum_{\mu=1}^{3} T_{\nu\mu}, \tag{12}$$

where

$$T_{\nu\mu} = \frac{1}{p}\sum_{a\in\mathcal{A}_\nu}\sum_{b\in\mathcal{B}_\mu} f(a)g(b) \sum_{\substack{ax_2\equiv bx_3 \pmod p\\ L_2+1\leqslant x_2\leqslant L_2+N_2\\ L_1+1\leqslant x_3\leqslant L_1+N_1}} 1.$$

In order to estimate $T_{\nu\mu}$ we use Lemma 1. For T_{11} we immediately get

$$T_{11} \ll N_1N_2M_1M_2\log p. \tag{13}$$

To estimate T_{12}, we split the interval of summation of b into subintervals of the form $e^{j-1}p/N_1 \leqslant b \leqslant e^j p/N_1$, where $1 \leqslant j \ll \log \frac{N_1}{M_1}$. Then application of Lemma 1 gives

$$T_{12} \ll N_2 M_1 M_2 \sum_{j \ll \log \frac{N_1}{M_1}} \frac{1}{e^j (p/N_1)} \sum_{a \leqslant p/N_2} \sum_{b \leqslant e^j p/N_1} \sum_{\substack{ax_2 \equiv bx_3 \pmod p \\ L_2+1 \leqslant x_2 \leqslant L_2+N_2 \\ L_1+1 \leqslant x_3 \leqslant L_1+N_1}} 1$$

$$\ll \frac{N_1 N_2 M_1 M_2}{p} \sum_{j \ll \log \frac{N_1}{M_1}} \frac{1}{e^j} \left(e^j p + e^{j/2} p \log p\right) \ll N_1 N_2 M_1 M_2 \log p.$$

The same estimate holds for T_{21}, so we get

$$T_{12} + T_{21} \ll N_1 N_2 M_1 M_2 \log p. \tag{14}$$

For T_{13} we get

$$T_{13} \ll p N_2 M_2 \sum_j \frac{1}{e^{2j} (p^2/M_1^2)} \sum_{a \leqslant p/N_2} \sum_{b \leqslant e^j p/M_1} \sum_{\substack{ax_2 \equiv bx_3 \pmod p \\ L_2+1 \leqslant x_2 \leqslant L_2+N_2 \\ L_1+1 \leqslant x_3 \leqslant L_1+N_1}} 1$$

$$\ll \frac{M_1^2 N_2 M_2}{p} \sum_j \frac{1}{e^{2j}} \left(\frac{e^j N_1 p}{M_1} + e^{j/2} (N_1/M_1)^{1/2} p \log p \right) \ll N_1 N_2 M_1 M_2 \log p.$$

The same bound holds for T_{31}; thus

$$T_{13} + T_{31} \ll N_1 N_2 M_1 M_2 \log p. \tag{15}$$

Next, we estimate T_{22} which will produce the extra term $\delta(N_1 N_2)$ that occurs in the statement of Theorem 1. We have

$$T_{22} \ll p M_1 M_2 \sum_{\substack{i \ll \log(N_2/M_2) \\ j \ll \log(N_1/M_1)}} \frac{N_1 N_2}{e^{i+j} p^2} \sum_{a \leqslant e^i p/N_2} \sum_{b \leqslant e^j p/N_1} \sum_{\substack{ax_2 \equiv bx_3 \pmod p \\ L_2+1 \leqslant x_2 \leqslant L_2+N_2 \\ L_1+1 \leqslant x_3 \leqslant L_1+N_1}} 1$$

$$\ll \frac{N_1 N_2 M_1 M_2}{p} \sum_{\substack{i \ll \log(N_2/M_2) \\ j \ll \log(N_1/M_1)}} \frac{1}{e^{i+j}} \left(e^{i+j} p + e^{(i+j)/2} p \log p\right),$$

whence we get

$$T_{22} \ll N_1 N_2 M_1 M_2 \left(\log p + \log \frac{N_1}{M_1} \log \frac{N_2}{M_2} \right). \tag{16}$$

Analogously we deal with T_{23} and T_{32}:

$$T_{23} \ll M_2 p^2 \sum_{\substack{i \ll \log(N_2/M_2) \\ j}} \frac{N_2 M_1^2}{e^{i+2j} p^3} \sum_{a \leqslant e^i p/N_2} \sum_{b \leqslant e^j p/M_1} \sum_{\substack{ax_2 \equiv bx_3 \pmod p \\ L_2+1 \leqslant x_2 \leqslant L_2+N_2 \\ L_1+1 \leqslant x_3 \leqslant L_1+N_1}} 1$$

$$\ll \frac{N_2 M_2 M_1^2}{p} \sum_{\substack{i \ll \log(N_2/M_2) \\ j}} \frac{1}{e^{i+2j}} \left(\frac{e^{i+j} N_1 p}{M_1} + e^{(i+j)/2} p \log p (N_1/M_1)^{1/2} \right)$$

$$\ll N_1 N_2 M_1 M_2 \log p.$$

The same bound holds for T_{32}, so we have

$$T_{23} + T_{32} \ll N_1 N_2 M_1 M_2 \log p. \tag{17}$$

Finally, for T_{33} we obtain

$$T_{33} = p^3 \sum_{i,j} \frac{M_2^2 M_1^2}{e^{2i+2j} p^4} \sum_{a \leqslant e^i p/M_2} \sum_{b \leqslant e^j p/M_1} \sum_{\substack{ax_2 \equiv bx_3 \pmod p \\ L_2+1 \leqslant x_2 \leqslant L_2+N_2 \\ L_1+1 \leqslant x_3 \leqslant L_1+N_1}} 1$$

$$\ll \frac{M_1^2 M_2^2}{p} \sum_{i,j} \frac{1}{e^{2i+2j}} \left(\frac{(e^i p/M_2) N_2 (p/M_1) e^j N_1}{p} + e^{(i+j)/2} \sqrt{\frac{N_1 N_2}{N_2 M_2}} p \log p \right).$$

Thus,

$$T_{33} \ll N_1 N_2 M_1 M_2 \log p. \tag{18}$$

Inserting (13)–(18) into (12), we deduce

$$\frac{J_1}{M_1 M_2} - \frac{N_1^2 N_2^2}{p} \ll N_1 N_2 \left(\log p + \log \frac{N_1}{M_1} \log \frac{N_2}{M_2} + \frac{N_1 M_2}{p} + \frac{N_2 M_1}{p} \right),$$

provided that $M_1 \leqslant N_1/2$, $M_2 \leqslant N_2/2$.

If $N_1 N_2 \leqslant 10p$, we define $M_1 = [N_1/2]$, $M_2 = [N_2/2]$ and obtain

$$\frac{J_1}{M_1 M_2} - \frac{N_1^2 N_2^2}{p} \ll N_1 N_2 \log p.$$

If $N_1 N_2 \geqslant 10p$, then define $M_1 = [p/N_2] < N_1/2$, $M_2 = [p/N_1] < N_2/2$ and obtain

$$\frac{J_1}{M_1 M_2} - \frac{N_1^2 N_2^2}{p} \ll N_1 N_2 \left(\log p + \log^2 \frac{N_1 N_2}{p} \right). \tag{19}$$

Thus, estimate (19) holds in both cases.

Analogously,

$$\frac{J_2}{M_1M_2}-\frac{N_1^2N_2^2}{p}\ll N_1N_2\left(\log p+\log^2\frac{N_1N_2}{p}\right). \tag{20}$$

Comparing (11), (19) and (20), we conclude the proof of Theorem 1.

6. Proof of Theorem 2

We can assume that $\Delta < p$. Let J be the number of solutions of the congruence (1) under the conditions

$$L_1+1\leqslant x_1,x_3\leqslant L_1+N_1,\qquad L_2+1\leqslant x_2,x_4\leqslant L_2+N_2,$$

and let $I(\lambda)$ be the number of solutions of the congruence

$$x_1x_2\equiv\lambda \pmod p,\quad L_1+1\leqslant x_1\leqslant L_1+N_1,\ L_2+1\leqslant x_2\leqslant L_2+N_2.$$

Then

$$\sum_{\lambda=0}^{p-1}\left(I(\lambda)-\frac{N_1N_2}{p}\right)^2=\sum_{\lambda=0}^{p-1}I^2(\lambda)-\frac{N_1^2N_2^2}{p}.$$

Since $\sum_{\lambda=0}^{p-1}I^2(\lambda)=J$, from Theorem 1 we obtain

$$\sum_{\lambda=0}^{p-1}\big(I(\lambda)-\Delta\log p\big)^2\ll N_1N_2\big(\log p+\log^2\Delta\big)=\Delta p\big(\log p+\log^2\Delta\big)\log p.$$

Let $\mathcal{E}\subset\{0,1,2,\dots,p-1\}$ be such that $I(\lambda)=0$ for $\lambda\in\mathcal{E}$. Then

$$|\mathcal{E}|\Delta^2\log^2 p\ll\Delta p\big(\log p+\log^2\Delta\big)\log p$$

and the result follows.

7. Proof of Theorem 3

We can assume that $N_1N_3\geqslant N_2N_4$. Denote

$$\mathcal{H}_1=\big\{x_1x_3^* \pmod p\colon\ L_1\leqslant x_1\leqslant L_1+N_1,\ L_3+1\leqslant x_3\leqslant L_3+N_3\big\},$$

$$\mathcal{H}_2=\big\{x_4x_2^* \pmod p\colon\ L_2\leqslant x_2\leqslant L_2+N_2,\ L_4+1\leqslant x_4\leqslant L_4+N_4\big\}.$$

By the pigeon-hole principle it suffices to show that $|\mathcal{H}_1|+|\mathcal{H}_2|>p$. Let

$$\mathcal{R}_1=\big\{h \pmod p\colon\ h\notin\mathcal{H}_1\big\}.$$

Then the congruence

$$x + t - (y + z)h \equiv 0 \pmod{p}$$

has no solutions in variables h, x, t, y, z with $h \in \mathcal{R}_1$ and

$$\begin{aligned} &[0.5L_1] + 1 \leqslant x, t \leqslant [0.5L_1] + [0.5N_1], \\ &[0.5L_3] + 1 \leqslant y, z \leqslant [0.5L_3] + [0.5N_3]. \end{aligned} \tag{21}$$

Therefore,

$$\sum_{a=0}^{p-1} \sum_{h \in \mathcal{R}_1} \sum_{x,t} \sum_{y,z} \mathbf{e}_p\big(a\big(x + t - h(y + z)\big)\big) = 0,$$

where the range for the variables in summations over x, t, y, z is given by (21). Separating the term corresponding to $a = 0$, we deduce

$$|\mathcal{R}_1| X_1^2 X_3^2 \leqslant \sum_{a=1}^{p-1} \left| \sum_{x,t} \mathbf{e}_p\big(a(x + t)\big) \right| \left| \sum_{y,z} \sum_{h \in \mathcal{R}_1} \mathbf{e}_p\big(ah(y + z)\big) \right|,$$

where $X_i = [0.5N_i]$. On the other hand, for $(a, p) = 1$, we have

$$\begin{aligned} \left| \sum_{y,z} \sum_{h \in \mathcal{R}_1} \mathbf{e}_p\big(ah(y + z)\big) \right| &\leqslant \sum_{h=0}^{p-1} \left| \sum_{y,z} \mathbf{e}_p\big(ah(y + z)\big) \right| \\ &= \sum_{n=0}^{p-1} \left| \sum_{y,z} \mathbf{e}_p\big(n(y + z)\big) \right| = pX_3. \end{aligned}$$

Also,

$$\sum_{a=1}^{p-1} \left| \sum_{x,t} \mathbf{e}_p\big(a(x + t)\big) \right| \leqslant pX_1.$$

Hence,

$$|\mathcal{R}_1| X_1^2 X_3^2 \leqslant p^2 X_1 X_3.$$

Since p is large, we deduce

$$|\mathcal{H}_1| = p - |\mathcal{R}_1| \geqslant p - \frac{p^2}{X_1 X_3} \geqslant p - \frac{4.5p^2}{N_1 N_3}. \tag{22}$$

If $N_2 N_4 > 10p$, then defining

$$\mathcal{R}_2 = \big\{h \pmod{p}\colon\ h \notin \mathcal{H}_2\big\},$$

and following the same lines as in the proof of inequality (22), we obtain

$$|\mathcal{H}_2| = p - |\mathcal{R}_2| \geqslant p - \frac{4.5p^2}{N_2N_4}.$$

Therefore,

$$|\mathcal{H}_1| + |\mathcal{H}_2| \geqslant 2p - \frac{4.5p^2}{N_2N_4} - \frac{4.5p^2}{N_1N_3} > p,$$

and the result follows in the case $N_2N_4 > 10p$.

Let now $N_2N_4 \leqslant 10p$. Let I denote the number of solutions of the congruence

$$x_4x_2^* \equiv y_4y_2^* \pmod p, \quad L_2 + 1 \leqslant x_2, y_2 \leqslant L_2 + N_2,\ L_4 + 1 \leqslant x_4, y_4 \leqslant L_4 + N_4.$$

From Lemma 4,

$$I \ll N_2N_4 \log p.$$

Hence, by Lemma 3,

$$|\mathcal{H}_2| \geqslant \frac{N_2^2N_4^2}{I} \geqslant \frac{c_0N_2N_4}{\log p},$$

where c_0 is an absolute constant. Combining this with (22), we obtain that

$$|\mathcal{H}_1| + |\mathcal{H}_2| \geqslant p - \frac{4.5p^2}{N_1N_3} + \frac{c_0N_2N_4}{\log p} \geqslant p + \frac{c_0N_2N_4}{\log p} - \frac{4.5N_2N_4}{c\log p}.$$

Taking $c = 5c_0$, we conclude that

$$|\mathcal{H}_1| + |\mathcal{H}_2| > p.$$

8. Proof of Theorem 4

Let $\mathcal{H}$ be the set of all distinct elements of the form $(d_1 + d_2)(b_1 + b_2)^*$, where

$$d_1 \in \mathcal{D}, \qquad d_2 \in \mathcal{D}, \qquad b_1 \in \mathcal{B}, \qquad b_2 \in \mathcal{B}, \qquad b_1 + b_2 \neq 0. \tag{23}$$

Lemma 5. *The following bound holds*:

$$|\mathcal{H}| \geqslant p - \frac{p^2}{|\mathcal{B}||\mathcal{D}| - p}.$$

Proof. The proof of Lemma 5 follows the same lines as the proof of Theorem 3. Let

$$\mathcal{R} = \mathbb{F}_p \setminus \mathcal{H}.$$

Then the equation

$$d_1 + d_2 - (b_1 + b_2)h = 0 \tag{24}$$

has no solutions with $h \in \mathcal{R}$ and d_1, d_2, b_1, b_2 subject to the conditions given by (23). Therefore, since $b_1 + b_2 = 0$ implies that $d_1 + d_2 = 0$, Eq. (24) has at most $|\mathcal{B}||\mathcal{D}||\mathcal{R}|$ solutions subject to

$$d_1 \in \mathcal{D}, \qquad d_2 \in \mathcal{D}, \qquad b_1 \in \mathcal{B}, \qquad b_2 \in \mathcal{B}, \qquad h \in \mathcal{R}.$$

Thus,

$$\frac{1}{p}\sum_{a=0}^{p-1}\sum_{h\in\mathcal{R}}\sum_{\substack{d_1\in\mathcal{D}\\ d_2\in\mathcal{D}}}\sum_{\substack{b_1\in\mathcal{B}\\ b_2\in\mathcal{B}}}\mathbf{e}_p\big(a\big(d_1+d_2-(b_1+b_2)h\big)\big) \leqslant |\mathcal{B}||\mathcal{D}||\mathcal{R}|.$$

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

$$\frac{1}{p}|\mathcal{R}||\mathcal{D}|^2|\mathcal{B}|^2 \leqslant |\mathcal{B}||\mathcal{D}||\mathcal{R}| + \frac{1}{p}\sum_{a=1}^{p-1}\sum_{h=0}^{p-1}\left|\sum_{d\in\mathcal{D}}\mathbf{e}_p(ad)\right|^2\left|\sum_{b\in\mathcal{B}}\mathbf{e}_p(ahb)\right|^2.$$

Thus,

$$|\mathcal{R}||\mathcal{D}|^2|\mathcal{B}|^2 \leqslant |\mathcal{B}||\mathcal{D}||\mathcal{R}|p + |\mathcal{D}||\mathcal{B}|p^2,$$

which implies that

$$|\mathcal{H}| = p - |\mathcal{R}| \geqslant p - \frac{p^2}{|\mathcal{B}||\mathcal{D}| - p}. \qquad \square$$

To prove Theorem 4, denote by T the number of solutions of the equation

$$a_1 + \lambda c_1 = a_2 + \lambda c_2, \quad a_1 \in \mathcal{A},\ a_2 \in \mathcal{A},\ c_1 \in \mathcal{C},\ c_2 \in \mathcal{C},\ \lambda \in \mathcal{H}.$$

If $c_1 = c_2$, then $a_1 = a_2$ and λ can be an arbitrary element of $\mathcal{H}$. Otherwise, for given a_1, a_2, c_1, c_2 with $c_1 \neq c_2$ we have at most one possible value for λ. Thus,

$$T \leqslant |\mathcal{A}||\mathcal{C}||\mathcal{H}| + |\mathcal{A}|^2|\mathcal{C}|^2.$$

Hence, there exists an element $\lambda \in \mathcal{H}$ such that

$$I \leqslant |\mathcal{A}||\mathcal{C}| + \frac{|\mathcal{A}|^2|\mathcal{C}|^2}{|\mathcal{H}|},$$

where I denotes the number of solutions of the equation

$$a_1 + \lambda c_1 = a_2 + \lambda c_2, \quad a_1 \in \mathcal{A},\ a_2 \in \mathcal{A},\ c_1 \in \mathcal{A},\ c_2 \in \mathcal{C}.$$

From this we get, by Lemma 3,

$$\#\{a+\lambda c\colon\ a\in\mathcal{A},\ c\in\mathcal{C}\}\geqslant\frac{|\mathcal{A}|^2|\mathcal{C}|^2}{I}\geqslant\frac{|\mathcal{A}||\mathcal{C}||\mathcal{H}|}{|\mathcal{A}||\mathcal{C}|+|\mathcal{H}|}. \tag{25}$$

Since λ is a fixed element of $\mathcal{H}$, there exist fixed elements d_0', d_0'' of $\mathcal{D}$ and fixed elements b_0', b_0'' of $\mathcal{B}$ such that

$$\lambda=\big(d_0'+d_0''\big)\big(b_0'+b_0''\big)^*.$$

Therefore, from (25) we derive that

$$\#\big\{a\big(b_0'+b_0''\big)+c\big(d_0'+d_0''\big)\colon\ a\in\mathcal{A},\ c\in\mathcal{C}\big\}\geqslant\frac{|\mathcal{A}||\mathcal{C}||\mathcal{H}|}{|\mathcal{A}||\mathcal{C}|+|\mathcal{H}|}.$$

Recalling the inequalities $|\mathcal{A}||\mathcal{C}|>(2+\sqrt{2})p$, $|\mathcal{B}||\mathcal{D}|>(2+\sqrt{2})p$ and using Lemma 5, we get

$$\frac{|\mathcal{A}||\mathcal{C}||\mathcal{H}|}{|\mathcal{A}||\mathcal{C}|+|\mathcal{H}|}>p/2.$$

Hence, from the pigeon-hole principle we conclude that

$$\big\{(a_1+a_2)\big(b_0'+b_0''\big)+(c_1+c_2)\big(d_0'+d_0''\big)\colon\ a_1\in\mathcal{A},\ a_2\in\mathcal{A},\ c_1\in\mathcal{C},\ c_2\in\mathcal{C}\big\}=\mathbb{F}_p.$$

Acknowledgments

The authors are thankful to the referee for careful reading the paper and useful remarks. The authors were supported by the Project PAPIIT IN 100307 from UNAM.

References

[1] A. Ayyad, T. Cochrane, Zh. Zheng, The congruence $x_1x_2\equiv x_3x_4 \pmod p$, the equation $x_1x_2=x_3x_4$, and mean values of character sums, J. Number Theory 59 (1996) 398–413.
[2] J. Bourgain, N. Katz, T. Tao, A sum-product estimate in finite fields and their applications, Geom. Funct. Anal. 14 (2004) 27–57.
[3] J. Bourgain, A.A. Glibichuk, S.V. Konyagin, Estimates for the number of sums and products and for exponential sums in fields of prime order, J. London Math. Soc. (2) 73 (2006) 380–398.
[4] D.A. Burgess, Mean values of character sums, Mathematika 33 (1986) 1–5.
[5] T. Cochrane, Zh. Zheng, Small solutions of the congruence $a_1x_1^2+a_2x_2^2+a_3x_3^2+a_4x_4^2\equiv c \pmod p$, Acta Math. Sinica (N.S.) 14 (1998) 175–182.
[6] J.B. Friedlander, H. Iwaniec, The divisor problem for arithmetic progressions, Acta Arith. 45 (1985) 273–277.
[7] J.B. Friedlander, H. Iwaniec, Estimates for character sums, Proc. Amer. Math. Soc. 119 (1993) 365–372.
[8] M.Z. Garaev, On the logarithmic factor in error term estimates in certain additive congruence problems, Acta Arith. 124 (2006) 27–39.
[9] M.Z. Garaev, A.A. Karatsuba, The representation of residue classes by products of small integers, Proc. Edinb. Math. Soc. (2) 50 (2007) 363–375.
[10] 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.
[11] G. Harman, Diophantine approximation with square-free integers, Math. Proc. Cambridge Philos. Soc. 95 (1984) 381–388.
[12] H.L. Montgomery, R.C. Vaughan, Mean values of character sums, Canad. J. Math. 31 (3) (1979) 476–487.

[13] I.E. Shparlinski, Distribution of points on modular hyperbolas, in: Sailing on the Sea of Number Theory: Proc. 4th China–Japan Seminar on Number Theory, Weihai, 2006, World Scientific, 2007, pp. 155–189.
[14] I.E. Shparlinski, Distribution of inverses and multiples of small integers and the Sato–Tate conjecture on average, Michigan Math. J., in press.
[15] G. Tenenbaum, Sur la probabilité qu'un entier possède un diviseur dans un intervalle donné, Compos. Math. 51 (2) (1984) 243–263 (in French).
[16] R.C. Vaughan, Diophantine approximation by prime numbers, III, Proc. London Math. Soc. 33 (1976) 177–192.