JOURNAL OF NUMBER THEORY 59, 398–413 (1996)
ARTICLE NO. 0105

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

Anwar Ayyad and Todd Cochrane*

Kansas State University, Manhattan, Kansas 66506

and

Zhiyong Zheng

Zhongshan University, Guangzhou 510275, People's Republic of China

We obtain the asymptotic formulae $|\mathscr{B} \cap V| = (|\mathscr{B}|/p) + O(\sqrt{|\mathscr{B}|}\log^2 p)$ for the number of solutions of the congruence $x_1x_2 \equiv x_3x_4 \pmod p$ in a box $\mathscr{B}$ of arbitrary size and position, and $N(B) = (12/\pi^2)B^2 \log B + CB^2 + O(B^{19/13}\log^{7/13} B)$, with C given explicitly, for the number of solutions of the diophantine equation $x_1x_2 = x_3x_4$ with $1 \leqslant x_i \leqslant B$. We also obtain the upper bound for fourth order character sum moments, $1/(p-1)\sum_{\chi \neq \chi_o} |\sum_{x=a+1}^{a+B} \chi(x)|^4 \ll B^2 \log^2 p$.

1. INTRODUCTION

The distribution of solutions of the congruence

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

where p is a prime, arises naturally in the study of certain character sums. For any integers a_i, B_i, with $1 \leqslant B_i < p$, $1 \leqslant i \leqslant 4$ let $\mathscr{B}$ be the box of points

$$\mathscr{B} = \{\mathbf{x} \in \mathbb{Z}^4 : a_i \leqslant x_i < a_i + B_i\}, \tag{2}$$

of cardinality $|\mathscr{B}| = B_1B_2B_3B_4$, and $V \subset \mathbb{Z}^4$ denote the set of integer solutions of (1). We may also view $\mathscr{B}$ and V as subsets of $\mathbb{F}_p^4$. Solutions of (1) with some $x_i \equiv 0 \pmod p$ may be readily dealt with and so we assume henceforth that $\mathscr{B}$ does not meet any of the coordinate planes

* E-mail address: cochrane@math.ksu.edu.

0022-314X/96 $18.00

$x_i \equiv 0 \pmod p$. For such boxes the number of solutions of (1) in $\mathscr{B}$ may be easily expressed in terms of a character sum:

$$|\mathscr{B} \cap V| = \frac{|\mathscr{B}|}{p-1} + \frac{1}{p-1} \sum_{\chi \neq \chi_o} \sum_{\mathbf{x} \in \mathscr{B}} \chi(x_1x_2x_3^{-1}x_4^{-1}) \tag{3}$$

where χ runs through the set of multiplicative characters on $\mathbb{F}_p$ and χ_o denotes the principal character. In particular, taking all the $a_i = a+1$ and all of the $B_i = B$ we have

$$|\mathscr{B} \cap V| = \frac{|\mathscr{B}|}{p-1} + \frac{1}{p-1} \sum_{\chi \neq \chi_o} \left| \sum_{x=a+1}^{a+B} \chi(x) \right|^4. \tag{4}$$

Our main theorems are

THEOREM 1. *Suppose that $\mathscr{B}$ is a box of the type* (2) *not meeting any coordinate plane. Then*

$$|\mathscr{B} \cap V| = \frac{|\mathscr{B}|}{p} + O(\sqrt{|\mathscr{B}|} \log^2 p). \tag{5}$$

In particular, if $|\mathscr{B}| \gg p^2 \log^4 p$ then $\mathscr{B}$ contains a solution of (1).

One would hope to be able to replace $\log^2 p$ with $\log p$ on the right-hand side of (5), which in lieu of Theorem 3 below would be best possible. The second statement in Theorem 1 is nearly best possible in the sense that there are boxes of cardinality $\approx p^2$ containing no solution of (1); for example $1 \leqslant x_1,\ x_2 \leqslant \sqrt{p}/2,\ \sqrt{p}/2 < x_3,\ x_4 < \sqrt{p}$. One may ask this time whether the factor $\log^4 p$ can be removed altogether.

In the special cases, $B_1 = B_2$, $B_3 = B_4$ and $B_1 = B_3$, $B_2 = B_4$, we can save the factor of $\log p$ in (5) at the expense of an asymptotic formula. Specifically, we shall prove

$$|\mathscr{B} \cap V| \approx \frac{|\mathscr{B}|}{p} + O(\sqrt{|\mathscr{B}|} \log p). \tag{6}$$

Further cases where the savings of $\log p$ can be had are given at the end of Section 3. Friedlander and Iwaniec [3, Lemma] had established the upper bound in (6) for the box $1 \leqslant x_1,\ x_3 \leqslant B_1,\ a \leqslant x_2,\ x_4 \leqslant a + B_2$, with $B_1 < B_2$ and $2B_1B_2 < p$.

Immediate consequences of (4), (5) and (6) are parts (i) and (ii) of

THEOREM 2. *For any integers a, B with $B > 0$ we have*

(i) $$\frac{1}{p-1} \sum_{\chi \neq \chi_o} \left| \sum_{x=a+1}^{a+B} \chi(x) \right|^4 \ll B^2 \log^2 p. \tag{7}$$

(ii) *If* $B \ll \sqrt{p \log p}$, *then*

$$\frac{1}{p-1} \sum_{\chi \neq \chi_o} \left| \sum_{x=a+1}^{a+B} \chi(x) \right|^4 \ll B^2 \log p, \tag{8}$$

(iii) *If* $B \leqslant \sqrt{p}$ *and* $a = 0$ *then*

$$\frac{1}{p-1} \sum_{\chi \neq \chi_o} \left| \sum_{x=1}^{B} \chi(x) \right|^4 = \frac{12}{\pi^2} B^2 \log B + \left(C - \frac{B^2}{p} \right) B^2 + O(B^{19/13} \log^{7/13} B), \tag{9}$$

where $C = -.511317447\cdots$ *is the constant in Theorem* 3.

Part (iii) is an immediate corollary of Theorem 3 as explained below. Also, it follows from Theorem 3 that the upper bound in (8) is best possible for $a = 0$ and $B \ll \sqrt{p \log p}$. The upper bound in (7) sharpens the result of Friedlander and Iwaniec [2, Lemma 3]. They had $\log^6 p$ instead of $\log^2 p$ on the righthand side. Their result has the advantage that it holds for a general modulus, but it only applies when $a = 0$ and the proof requires a substantial amount of analytic machinery pertaining to L-functions. Our proof of (7) is elementary. The upper bounds in (7) and (8) may also be compared with the result of Montgomery and Vaughan [6, Theorem 1],

$$\frac{1}{p-1} \sum_{\chi \neq \chi_o} \max_{B} \left| \sum_{x=1}^{B} \chi(x) \right|^4 \ll p^2,$$

and the result of Burgess [1, Lemma 1],

$$\sum_{\chi \neq \chi_o} \sum_{x=1}^{p} \left| \sum_{m=1}^{B} \chi(x+m) \right|^4 \leqslant 6p^2 B^2.$$

The inequality of Montgomery and Vaughan yields a sharper inequality in (7) for values of B close to p, while the result of Burgess indicates that on averaging with respect to a, one saves the factor of $\log^2 p$ in (7).

We turn now to the diophantine equation $x_1 x_2 = x_3 x_4$, and establish a precise asymptotic formula for the number of solutions in a cube concerned at the origin.

THEOREM 3. *The number* $N(B)$ *of integer solutions of the equation* $x_1 x_2 = x_3 x_4$ *with* $1 \leqslant x_i \leqslant B$, $1 \leqslant i \leqslant 4$, *is given by*

$$N(B) = \frac{12}{\pi^2} B^2 \log B + CB^2 + O(B^{19/13} \log^{7/13} B), \tag{10}$$

where $C = 2/\pi^2(12\gamma_o - (36/\pi^2)\,\zeta'(2) - 3) - 2 = -.511317447\cdots$, γ_o *is Euler's constant and* $\zeta'(2) = \sum_{n=1}^{\infty} (\log n/n^2)$.

Let $A(B) = (12/\pi^2)\,B^2 \log B + CB^2$ denote the approximation to $N(B)$ provided by Theorem 3. The following table illustrates the accuracy of the formula. (The values given are approximations.)

B	$N(B)$	$A(B)$	$\lvert N(B) - A(B)\rvert / N(B)$
10^2	52160	50878	.024
10^3	7.899×10^6	7.887×10^6	.0016
10^4	1.0690×10^9	1.0687×10^9	.00029
10^5	1.348687×10^{11}	1.348672×10^{11}	.000011
10^6	1.628652×10^{13}	1.628633×10^{13}	.000011

If $B \leqslant \sqrt{p}$ then the equation $x_1x_2 = x_3x_4$ and the congruence (1) are identical and so (10) is also a formula for $|\mathscr{B} \cap V|$. This observation, together with (4), yields part (iii) of Theorem 2.

Another easy consequence of (6) is

COROLLARY 2. *If* $\mathscr{B}$ *is a box of the type* (2) *not meeting any coordinate plane then the number* $N(\mathscr{B})$ *of integer solutions of the equation* $x_1x_2 = x_3x_4$ *with coordinates in* $\mathscr{B}$ *is bounded by*

$$N(\mathscr{B}) \ll \sqrt{|\mathscr{B}|}\,\log(|\mathscr{B}|). \tag{11}$$

Theorem 3 and Corollary 2 are proven in Sections 4 and 5 respectively.

The proof of Theorem 1 makes use of three different ways of counting the solutions of (1). The first method is the most elementary. Here we fix two of the coordinates, say x_1 and x_3, and count the number of solutions of the linear diophantine equations $x_1x_2 - x_3x_4 = jp$ for the appropriate range of values of j. Upon summing over x_1 and x_3 we obtain the upper bound in Lemma 2,

$$|\mathscr{B} \cap V| \ll \frac{|\mathscr{B}|}{p} + \sqrt{|\mathscr{B}|}\,\log p, \tag{12}$$

for a box of the type

$$\mathscr{B} = \{\mathbf{x} \in \mathbb{Z}^4 \colon 1 \leqslant x_i \leqslant B_i,\ 1 \leqslant i \leqslant 4\},$$

with $B_1 = B_3$ and $B_2 = B_4$. This approach has two limitations. It can only be used to obtain an upper bound on the number of solutions. Also, the method runs into complications for boxes of arbitrary sizes and even more

so for boxes not cornered at the origin. This lemma will serve as a catalyst for the second method.

The second way of counting the solutions of (1) is to work over $\mathbb{F}_p$, and let α denote the characteristic function of the box $\mathscr{B}$ in (2), viewed as a subset of $\mathbb{F}_p^4$, with finite Fourier expansion

$$\alpha(\mathbf{x}) = \sum_{\mathbf{y}} a(\mathbf{y})\, e_p(\mathbf{x}\cdot\mathbf{y}).$$

Here, $e_p(*) = e^{(2\pi i/p)*}$ and $\mathbf{x}\cdot\mathbf{y} = x_1y_1 + x_2y_2 + x_3y_3 + x_4y_4$, and $\sum_{\mathbf{y}}$ denotes the complete sum over $\mathbf{y}\in\mathbb{F}_p^4$. Then

$$\begin{aligned}
|\mathscr{B}\cap V| &= \sum_{\substack{x_1x_2 = x_3x_4\\ x_i\neq 0}} \alpha(\mathbf{x}) = \frac{1}{p-1}\sum_{\substack{\mathbf{x}\\ x_i\neq 0}} \alpha(\mathbf{x}) \sum_{\chi} \chi(x_1x_2x_3^{-1}x_4^{-1}),\\
&= \frac{1}{p-1}\sum_{\substack{\mathbf{x}\\ x_i\neq 0}} \alpha(\mathbf{x}) + \frac{1}{p-1}\sum_{\chi\neq\chi_o}\ \sum_{\substack{\mathbf{x}\\ x_i\neq 0}} \alpha(\mathbf{x})\,\chi(x_1x_2x_3^{-1}x_4^{-1}) \quad (13)\\
&= \frac{1}{p-1}\sum_{\substack{\mathbf{x}\\ x_i\neq 0}} \alpha(\mathbf{x})\\
&\quad + \frac{1}{p-1}\sum_{y} a(\mathbf{y}) \sum_{\chi\neq\chi_o}\ \sum_{\substack{\mathbf{x}\\ x_i\neq 0}} \chi(x_1x_2x_3^{-1}x_4^{-1})\, e_p(\mathbf{x}\cdot\mathbf{y}). \quad (14)
\end{aligned}$$

Now if any $y_i = 0$ then the sum over χ and $\mathbf{x}$ is zero. If all of the y_i are non-zero then the sum over $\mathbf{x}$ is just

$$\Pi_{i=1}^2 \sum_{x_i\neq 0} \chi(x_i)\, e_p(x_iy_i)\, \Pi_{i=3}^4 \sum_{x_i\neq 0} \chi(x_i^{-1})\, e_p(x_iy_i).$$

Letting $G(\chi)$ denote the Gaussian sum $G(\chi) = \sum_{x_i\neq 0}\chi(x_i)\, e_p(x_i)$, this is just

$$= \chi(y_1^{-1}y_2^{-1}y_3y_4)\, G(\chi)^2\, G(\chi^{-1})^2 = p^2\chi(y_1^{-1}y_2^{-1}y_3y_4),$$

since $G(\chi^{-1}) = \chi(-1)\,\overline{G(\chi)}$ and $|G(\chi)|^2 = p$ for $\chi\neq\chi_o$. Summing over χ we obtain the fundamental identity,

Fundamental Identity.

$$\sum_{\substack{x_1x_2 = x_3x_4\\ x_i\neq 0}} \alpha(\mathbf{x}) = \frac{1}{p-1}\sum_{\substack{\mathbf{x}\\ x_i\neq 0}} \alpha(\mathbf{x}) + p^2 \sum_{\substack{y_1y_2 = y_3y_4\\ y_i\neq 0}} a(\mathbf{y}) - \frac{p^2}{p-1}\sum_{y_i\neq 0} a(\mathbf{y}). \quad (15)$$

Now, in order to control the error term in (15) one is brought back to the problem of determining a good upper bound on the number of solutions of (1) in a box centered at the origin. Rather than applying (15) directly to the characteristic function of $\mathscr{B}$ we shall apply it to a weighted function α having rapidly decaying Fourier coefficients. This will allow us to control the error term in (15) and to generalize the upper bound in (12). For an arbitrary box we shall obtain, Lemma 3,

$$|\mathscr{B} \cap V| \ll \frac{|\mathscr{B}|}{p} + (p + B_1B_2 \log p)^{1/2} (p + B_3B_4 \log p)^{1/2}. \tag{16}$$

The factor of p appearing twice on the right hand side of (16) is unavoidable if one makes a simple application of the Fundamental Identity. Nevertheless, the bound in (16) is strong enough for a successful application of our third method which is taken up in Section 3.

2. LEMMAS

LEMMA 1. *Let $x_1, x_3, a_2, a_4, B_2, B_4$ be positive integers with x_1, x_3 nonzero* $(\mathrm{mod}\, p)$ *and d the greatest common divisor of x_1 and x_3. Then*

$$\#\{(x_2, x_4) \in \mathbb{Z}^2 : x_1x_2 \equiv x_3x_4 \pmod p,\ a_2 \leqslant x_2 < a_2 + B_2,\ a_4 \leqslant x_4 < a_4 + B_4\}$$
$$\leqslant \left(\frac{B_2x_1}{dp} + \frac{B_4x_3}{dp} + 1\right) \min\left(\frac{B_2d}{x_3} + 1, \frac{B_4d}{x_1} + 1\right).$$

Proof. We must solve the linear diophantine equation

$$x_1x_2 - x_3x_4 = jp \tag{17}$$

with $j \in \mathbb{Z}$. Now, since

$$x_1a_2 - x_3(a_4 + B_4) < x_1x_2 - x_3x_4 < x_1(a_2 + B_2) - x_3a_4,$$

it follows that jp runs through an interval of length $B_2x_1 + B_4x_3$. Any solution of (17) must have $d \mid j$, and so there are at most

$$\left(\frac{B_2x_1}{dp} + \frac{B_4x_3}{dp} + 1\right)$$

choices for j. For any fixed j the solution set of (17) is given by

$$x_2 = x_{20} + \lambda x_3/d, \qquad x_4 = x_{40} + \lambda x_1/d,$$

with $\lambda \in \mathbb{Z}$. Since x_2 and x_4 run through intervals of lengths B_2 and B_4 respectively, there are at most

$$\min\left(\frac{B_2 d}{x_3}+1, \frac{B_4 d}{x_1}+1\right),$$

choices for λ, and the lemma follows.

LEMMA 2. *Suppose that $\mathscr{B}$ is a box of the type*

$$\mathscr{B} = \{\mathbf{x} \in \mathbb{Z}^4 : 1 \leqslant x_1 \leqslant H,\ a_2 \leqslant x_2 < a_2 + K,\ 1 \leqslant x_3 \leqslant K,\ a_4 \leqslant x_4 < a_4 + H\},$$

where a_2, a_4, H, K are integers with $0 < H,\ K < p$. Then

$$|\mathscr{B} \cap V| \ll \frac{|\mathscr{B}|}{p} + \sqrt{|\mathscr{B}|}\log p. \tag{18}$$

Proof. For any fixed x_1, x_3 let $N(x_1, x_3)$ denote the number of solutions (x_2, x_4) of the congruence $x_1 x_2 \equiv x_3 x_4 \pmod p$ in the desired interval. Then by Lemma 1 we have

$$\begin{aligned}
|\mathscr{B} \cap V| &= \sum_{d \leqslant H} \sum_{x_1=1}^{H} \sum_{\substack{x_3=1 \\ (x_1, x_3)=d}}^{K} N(x_1, x_3) \\
&\leqslant \sum_{d \leqslant H} \Bigg[\sum_{\substack{x_1=1 \\ (x_1, x_3)=d}}^{H} \sum_{\substack{x_3=1 \\ Kx_1 \leqslant Hx_3}}^{K} \left(\frac{Hx_3}{dp}+1\right)\left(\frac{Kd}{x_3}+1\right) \\
&\quad + \sum_{\substack{x_1=1 \\ (x_1, x_3)=d}}^{H} \sum_{\substack{x_3=1 \\ Kx_1 \geqslant Hx_3}}^{K} \left(\frac{Kx_1}{dp}+1\right)\left(\frac{Hd}{x_1}+1\right)\Bigg] \\
&= \frac{H^2K^2}{p} + HK + \sum_{d \leqslant H} \sum_{\substack{x_1, x_3 \\ Kx_1 \leqslant Hx_3}} \left(\frac{Hx_3}{dp}+\frac{Kd}{x_3}\right) \\
&\quad + \sum_{d \leqslant H} \sum_{\substack{x_1, x_3 \\ Kx_1 \geqslant Hx_3}} \left(\frac{Kx_1}{dp}+\frac{Hd}{x_1}\right).
\end{aligned}$$

Letting $x_1 = du_1$ and $x_3 = du_3$ the above is

$$\begin{aligned}
&\leqslant \frac{H^2K^2}{p} + HK + \sum_{d \leqslant H} \sum_{u_3 \leqslant K/d} \left(\frac{H^2u_3^2}{pK}+H\right) + \sum_{d \leqslant H} \sum_{u_1 \leqslant H/d} \left(\frac{K^2u_1^2}{Hp}+K\right) \\
&\ll \frac{H^2K^2}{p} + HK\log p.
\end{aligned}$$

LEMMA 3. *Suppose that $\mathscr{B}$ is any box of the type* (2) *not meeting any coordinate plane. Then*

$$|\mathscr{B} \cap V| \ll \frac{|\mathscr{B}|}{p} + (p + B_1B_2 \log p)^{1/2} (p + B_3B_4 \log p)^{1/2}. \tag{19}$$

Moreover, the inequality in (19) *holds if the products B_1B_2 and B_3B_4 are replaced with any other pairing of the B_i.*

Proof. Suppose first that $B_1 = B_3$ and $B_2 = B_4$. Our strategy is to choose a weighted function α so that the error term

$$E(\alpha) := p^2 \sum_{\substack{y_1y_2 = y_3y_4 \\ y_i \neq 0}} a(\mathbf{y}) - \frac{p^2}{p-1} \sum_{y_i \neq 0} a(\mathbf{y})$$

in the fundamental identity (15), admits a good upper bound. We may assume that $\mathscr{B}$ is a box of the type

$$\mathscr{B} = \{\mathbf{x} \in \mathbb{Z}^4 : |x_i - c_i| < B_i/2,\ 1 \leqslant i \leqslant 4\},$$

for some integers c_i. Let V be the set of solutions of (1), $\mathscr{B}_0 = \{\mathbf{x} \in \mathbb{Z}^4 : |x_i| < B_i/2\}$ and

$$\alpha = \frac{1}{|\mathscr{B}|^4} \chi_{\mathscr{B}_0} * \chi_{\mathscr{B}_0} * \chi_{\mathscr{B}_0} * \chi_{\mathscr{B}_0} * \chi_{\mathscr{B}},$$

a normalized five-fold convolution of the characteristic functions of $\mathscr{B}_0$ and $\mathscr{B}$. Then

$$\sum_{\substack{x_1x_2 = x_3x_4 \\ x_i \neq 0}} \alpha(\mathbf{x}) \gg |\mathscr{B} \cap V|, \tag{20}$$

$$\sum_{x_i \neq 0} \alpha(\mathbf{x}) \ll |\mathscr{B}|, \tag{21}$$

and the Fourier coefficients $a(\mathbf{y})$ of α satisfy

$$|a(\mathbf{y})| \ll p^{-4} |\mathscr{B}|^{-4} \Pi_{i=1}^4 \min\left(B_i^5, \frac{p^5}{|y_i|^5}\right), \qquad (|y_i| < p/2).$$

Thus, letting the y_i run through the intervals $0 < |y_i| \leqslant p/B_i$ and $2^{k_i}p/B_i < |y_i| \leqslant 2^{k_i+1}p/B_i$ for $k_i = 0, 1, 2\ldots$, we have

$$\sum_{\substack{y_1y_2 = y_3y_4 \\ y_i \neq 0}} |a(\mathbf{y})| \ll p^{-4} |\mathscr{B}|^{-4} \sum_{k_1=0} \sum_{k_2=0} \sum_{k_3=0} \sum_{k_4=0} \sum_{\substack{y_1y_2 = y_3y_4 \\ 0 < |y_i| \leqslant 2^{k_i}p/B_i}} |\mathscr{B}|^5 \Pi_{i=1}^4 2^{-5k_i}.$$

For any choice of k_i let $K = \max(k_1, k_2, k_3, k_4)$, and enlarge the range of summation of the y_i to the box (with coordinate planes omitted),

$$0 < |y_1|, |y_3| \leqslant 2^K p/B_1, \qquad 0 < |y_2|, |y_4| \leqslant 2^K p/B_2.$$

Here we have used our assumption that $B_1 = B_3$ and $B_2 = B_4$. On applying Lemma 2, we obtain

$$\sum_{\substack{y_1 y_2 = y_3 y_4 \\ y_i \neq 0}} |a(\mathbf{y})| \ll p^{-4} |\mathscr{B}| \sum_{k_1} \cdots \sum_{k_4} \Pi_{i=1}^4 2^{-5k_i} \left(\frac{2^{4K} p^3}{|\mathscr{B}|} + \frac{2^{2K} p^2 \log p}{B_1 B_2} \right)$$

$$\ll \frac{1}{p} + p^{-2} |\mathscr{B}|^{1/2} \log p,$$

and in a similar manner one obtains $\sum_{y_i \neq 0} |a(\mathbf{y})| \ll 1$. Thus

$$E(\alpha) \ll p + |\mathscr{B}|^{1/2} \log p. \tag{22}$$

Suppose now that B_1, B_2, B_3 and B_4 are arbitrary. Write

$$\alpha(\mathbf{x}) = \alpha_1(x_1)\, \alpha_2(x_2)\, \alpha_3(x_3)\, \alpha_4(x_4).$$

By (13) the error term $E(\alpha)$ may be expressed

$$\begin{aligned}
|E(\alpha)| &= |E(\alpha_1(x_1)\, \alpha_2(x_2)\, \alpha_3(x_3)\, \alpha_4(x_4))| \\
&= \frac{1}{p-1} \left| \sum_{\chi \neq \chi_o} \sum_{\substack{\mathbf{x} \\ x_i \neq 0}} \alpha(\mathbf{x})\, \chi(x_1 x_2 x_3^{-1} x_4^{-1}) \right| \\
&= \frac{1}{p-1} \left| \sum_{\chi \neq \chi_o} \left(\Pi_{i=1}^2 \sum_{x_i \neq 0} \alpha_i(x_i)\, \chi(x_i) \right) \left(\Pi_{i=3}^4 \sum_{x_i \neq 0} \alpha_i(x_i)\, \chi(x_i^{-1}) \right) \right| \\
&\leqslant \frac{1}{p-1} \left(\sum_{\chi \neq \chi_o} \left| \Pi_{i=1}^2 \sum_{x_i \neq 0} \alpha_i(x_i)\, \chi(x_i) \right|^2 \right)^{1/2} \\
&\quad \times \left(\sum_{\chi \neq \chi_o} \left| \Pi_{i=3}^4 \sum_{x_i \neq 0} \alpha_i(x_i)\, \chi(x_i^{-1}) \right|^2 \right)^{1/2} \\
&= E(\alpha_1(x_1)\, \alpha_2(x_2)\, \alpha_1(x_3)\, \alpha_2(x_4))^{1/2}\, E(\alpha_3(x_1)\, \alpha_4(x_2)\, \alpha_3(x_3)\, \alpha_4(x_4))^{1/2} \\
&\ll (p + B_1 B_2 \log p)^{1/2}\, (p + B_3 B_4 \log p)^{1/2},
\end{aligned}$$

by the first case, (22). Applying Cauchy's inequality in the preceding argument to a different pairing of the B_i allows us to replace the products B_1B_2 and B_3B_4 in the statement of Lemma 3 with any other pairing of the B_i.

3. PROOF OF THEOREM 1

The third method for counting the solutions of (1) in $\mathscr{B}$ is to again view the congruence as an equation over $\mathbb{F}_p$ and write,

$$\sum_{\substack{x_1x_2 = x_3x_4 \\ a_i \leqslant x_i < a_i + B_i}} 1 = \sum_{a_i \leqslant x_i < a_i + B_i,\ 1 \leqslant i \leqslant 3} \alpha(x_1x_2x_3^{-1}),$$

where α is the characteristic function of the interval $a_4 \leqslant x_4 < a_4 + B_4$. Letting $\alpha(x) = \sum_y a(y)\, e_p(xy)$ be the finite Fourier expansion of α we obtain,

$$|\mathscr{B} \cap V| = \frac{|\mathscr{B}|}{p} + \sum_{y \neq 0} a(y) \sum_{a_i \leqslant x_i < a_i + B_i,\ 1 \leqslant i \leqslant 3} e_p(x_1x_2x_3^{-1}y). \tag{23}$$

To bound the error term in (23) we sum over x_2 to obtain

$$\begin{aligned} |\text{Error}| &\leqslant \sum_{y \neq 0} |a(y)| \sum_{a_i \leqslant x_i < a_i + B_i,\ i = 1, 3} \left| \frac{\sin(\pi x_1 x_3^{-1} y B_2/p)}{\sin(\pi x_1 x_3^{-1} y/p)} \right| \\ &= \sum_{y \neq 0} |a(y)| \sum_{l \neq 0} \left| \frac{\sin(\pi l B_2/p)}{\sin(\pi l/p)} \right| \sum_{\substack{a_i \leqslant x_i < a_i + B_i,\ i = 1, 3 \\ x_1 y = x_3 l}} 1 \\ &\ll p^{-1} \sum_{y \neq 0} \min\left(B_4, \frac{p}{|y|}\right) \sum_{l \neq 0} \min\left(B_2, \frac{p}{|l|}\right) \sum_{\substack{a_i \leqslant x_i < a_i + B_i,\ i = 1, 3 \\ x_1 y = x_3 l}} 1. \end{aligned}$$

Letting y run through the intervals $0 < |y| \leqslant p/B_4$ and $2^i p/B_4 < |y| \leqslant 2^{i+1} p/B_4$ for $i = 0, 1, 2...$, stopping as soon as $2^i > B_4/4$, and doing the same thing for l we obtain

$$|\text{Error}| \ll p^{-1} B_2 B_4 \sum_{i=0} \sum_{j=0} 2^{-i-j} |\mathscr{B}_{ij} \cap V| \tag{24}$$

where for any i and j,

$$\begin{aligned} \mathscr{B}_{ij} = \{(x_1, y, x_3, l) \in \mathbb{Z}^4 &: a_k \leqslant x_k < a_k + B_k,\ k = 1, 3, \\ &0 < |y| \leqslant 2^i p/B_4,\ 0 < |l| \leqslant 2^j p/B_2\}. \end{aligned}$$

If we assume that $B_1 \geqslant B_2$ and $B_3 \geqslant B_4$ then for any i, j, we have by Lemma 3 that

$$|\mathscr{B}_{ij} \cap V| \ll \frac{2^{i+j} B_1 B_3 p}{B_2 B_4} + (p + 2^j p B_1 \log p/B_2)^{1/2} (p + 2^i p B_3 \log p/B_4)^{1/2}$$
$$\ll \frac{2^{i+j} B_1 B_3 p}{B_2 B_4} + 2^{(i+j)/2} p \log p \sqrt{\frac{B_1 B_3}{B_2 B_4}}.$$

Inserting this into (24) and realizing that i and j each run through an interval of length $< \log p$ yields

$$|\text{Error}| \ll B_1 B_3 \log^2 p + \sqrt{B_1 B_2 B_3 B_4} \log p \ll B_1 B_3 \log^2 p. \tag{25}$$

If $B_1 \geqslant B_4$ and $B_3 \geqslant B_2$ then for any i, j we have $B_1 2^i p/B_4 \geqslant p$ and $B_3 2^j p/B_2 \geqslant p$ and so we can again apply Lemma 3 and obtain (25). Thus for any box $\mathscr{B}$ with B_1 the largest dimension and $B_3 \geqslant \min(B_2, B_4)$ it follows from (23) that

$$|\mathscr{B} \cap V| = \frac{|\mathscr{B}|}{p} + O(B_1 B_3 \log^2 p).$$

In particular, we have established Theorem 1 for Cubes, that is, for boxes with all of the B_i equal. This is enough to establish Theorem 2(i). One can then obtain Theorem 1 for a general box by a simple application of Cauchy's inequality. Indeed, from (3) we have

$$\left| |\mathscr{B} \cap V| - \frac{\mathscr{B}}{p-1} \right| \ll \frac{1}{p-1} \left(\Pi_{i=1}^4 \sum_{\chi \neq \chi_o} \left| \sum_{a_i \leqslant x_i < a_i + B_i} \chi(x_i) \right|^4 \right)^{1/4}$$
$$\ll \Pi_{i=1}^4 B_i^{1/2} \log^2 p.$$

We turn now to the proof of the approximation formula

$$|\mathscr{B} \cap V| \approx \frac{|\mathscr{B}|}{p} + O(\sqrt{|\mathscr{B}|} \log p), \tag{26}$$

in a number of special cases.

PROPOSITION. *Suppose that $\mathscr{B}$ is a box not meeting any coordinate plane with B_1 the largest dimension and $B_3 \geqslant \min(B_2, B_4)$. Then*

$$|\mathscr{B} \cap V| \approx \frac{|\mathscr{B}|}{p} + O(B_1 B_3 \log p). \tag{27}$$

Proof. We proceed as in the proof of Theorem 1 above, only this time we replace α with the appropriate weighted functions having Fourier coefficients $a(y)$ satisfying

$$|a(y)| \ll p^{-1} \min\left(B_4^2, \frac{p^2}{|y|^2}\right).$$

In this case, the inequality in (24) becomes

$$|\text{Error}| \ll p^{-1} B_2 B_4 \sum_{i=0} \sum_{j=0} 2^{-2i-j} |\mathscr{B}_{ij} \cap V|, \tag{28}$$

and so we save a factor of $\log p$ in the sum over i.

The proposition establishes (26) in the special cases $B_1 = B_2$, $B_3 = B_4$ and $B_1 = B_3$, $B_2 = B_4$. Another special case where (26) can be proved is when the B_i can be paired so that both products are $\gg p/\log p$. The upper bound

$$|\mathscr{B} \cap V| \ll \frac{|\mathscr{B}|}{p} + O(\sqrt{|\mathscr{B}|} \log p),$$

is just a consequence of Lemma 3. The lower bound can be obtained in an analogous manner by choosing a slightly different weighted function α.

Finally, if the B_i can be paired in such a manner that both products are $\ll p \log p$ then we can again establish (26). In this case (26) is just equivalent to

$$|\mathscr{B} \cap V| \ll \sqrt{|\mathscr{B}|} \log p. \tag{29}$$

To obtain (29) suppose, without loss of generality, that $B_1B_4 \ll p \log p$ and $B_2B_3 \ll p \log p$. By an application of Cauchy's inequality we have,

$$\begin{aligned}
|\mathscr{B} \cap V| &= \sum_{\substack{x_1x_2 = x_3x_4 \\ a_i \leqslant x_i < a_i + B_i}} 1 = \sum_{\beta=1}^{p-1} \Bigg(\sum_{\substack{x_1, x_4 \\ x_1/x_4 = \beta}} 1 \Bigg) \Bigg(\sum_{\substack{x_2, x_3 \\ x_3/x_2 = \beta}} 1 \Bigg) \\
&\leqslant \Bigg[\sum_{\beta} \Bigg(\sum_{\substack{x_1, x_4 \\ x_1/x_4 = \beta}} 1 \Bigg)^2 \Bigg]^{1/2} \Bigg[\sum_{\beta} \Bigg(\sum_{\substack{x_2, x_3 \\ x_3/x_2 = \beta}} 1 \Bigg)^2 \Bigg]^{1/2} \\
&= \Bigg[\sum_{\substack{x_1u_4 = u_1x_4 \\ a_1 \leqslant x_1,\, u_1 < a_1 + B_1 \\ a_4 \leqslant x_4,\, u_4 < a_4 + B_4}} 1 \Bigg]^{1/2} \Bigg[\sum_{\substack{x_2u_3 = u_2x_3 \\ a_2 \leqslant x_2,\, u_2 < a_2 + B_2 \\ a_3 \leqslant x_3,\, u_3 < a_3 + B_3}} 1 \Bigg]^{1/2} \\
&\ll (\sqrt{B_1B_4 \log p})(\sqrt{B_2B_3 \log p}),
\end{aligned}$$

the last inequality following from the above proposition.

4. PROOF OF THEOREM 3

We have

$$N(B) := \sum_{\substack{x_1x_2 = x_3x_4 \\ 1 \leqslant x_i \leqslant B}} 1 = \sum_{\substack{(a,b)=1 \\ 1 \leqslant a,b \leqslant B}} \left(\sum_{(x_1/x_3)=(a/b)} 1 \right)^2.$$

The contribution coming from $a = b = 1$ is just B^2, and so by symmetry the above is

$$= B^2 + 2 \sum_{\substack{(a,b)=1 \\ 1 \leqslant a < b \leqslant B}} \left(\sum_{(x_1/x_3)=(a/b)} 1 \right)^2 = B^2 + 2 \sum_{\substack{(a,b)=1 \\ 1 \leqslant a < b \leqslant B}} \left[\frac{B}{b} \right]^2$$

$$= B^2 + 2 \sum_{b=2}^{B} \phi(b) \left[\frac{B}{b} \right]^2. \tag{30}$$

Thus, it is sufficient to show that

$$\sum_{n \leqslant x} \phi(x) \left[\frac{x}{n} \right]^2 = \frac{6}{\pi^2} x^2 \log x + C'x^2 + O(x^{19/13} \log^{7/13} x) \tag{31}$$

for the appropriate constant C'.

LEMMA 4. *Let $\gamma_o = .57721...$ denote Euler's constant and $\{x\} = x - [x]$. Then*

(i) $$\gamma_1 := \sum_{n=1}^{\infty} \frac{\mu(n)}{n^2} \log n = \frac{\zeta'(2)}{\zeta^2(2)} = \frac{36}{\pi^4} \zeta'(2), \tag{32}$$

(ii) $$\gamma_2 := \int_1^{\infty} \frac{\{y\}^2}{y^3} dy = \frac{3}{2} - \gamma_o - \frac{\pi^2}{12}. \tag{33}$$

Proof. Part (i) follows from $\zeta^{-1}(s) = \sum_{n=1}^{\infty} (\mu(n)/n^s)$. For part (ii) we write

$$\gamma_2 = \sum_{n=1}^{\infty} \int_n^{n+1} \frac{(y-n)^2}{y^3} dy = \sum_{n=1}^{\infty} \int_n^{n+1} \frac{1}{y} - \frac{2n}{y^2} + \frac{n^2}{y^3} dy$$

$$= \sum_{n=1}^{\infty} \log(n+1) - \log(n) - \frac{1}{n+1} - \frac{1}{2(n+1)^2},$$

and use $\sum_{n=1}^{x} (1/n) = \log x + \gamma_o + O(1/x)$.

LEMMA 5. *We have*

$$\text{(i)} \qquad \sum_{n \leqslant x} \frac{\phi(n)}{n^2} = \frac{6}{\pi^2} \log x + \left(\frac{6}{\pi^2} \gamma_o - \gamma_1 \right) + O\left(\frac{\log x}{x} \right), \tag{34}$$

$$\text{(ii)} \qquad \sum_{n \leqslant x} \left\{ \frac{x}{n} \right\} = (1 - \gamma_o)\, x + O(x^{(7/22)+\varepsilon}), \tag{35}$$

and

$$\text{(iii)} \qquad \sum_{n \leqslant x} n \left\{ \frac{x}{n} \right\}^2 = \gamma_2 x^2 + O(x^{19/13} \log^{7/13} x). \tag{36}$$

Proof. Part (i) is readily obtained upon inserting $\phi(n) = n \sum_{d \mid n} (\mu(d)/d)$ into the sum on the left-hand side of (34). For part (ii) let $d(n)$ denote the divisor function. Then

$$\sum_{n \leqslant x} d(n) = x \log x + (2\gamma_o - 1)\, x + \Delta(x),$$

where by the work of Iwaniec and Mozzochi (1988), $\Delta(x) \ll x^{(7/22)+\varepsilon}$. On the other hand,

$$\sum_{n \leqslant x} d(n) = \sum_{a \leqslant x} \left[\frac{x}{a} \right] = x \sum_{a \leqslant x} \frac{1}{a} - \sum_{a \leqslant x} \left\{ \frac{x}{a} \right\},$$

and so we obtain (35). To prove part (iii) we write

$$\begin{aligned} \sum_{n \leqslant x} n \left\{ \frac{x}{n} \right\}^2 &= \sum_{n \leqslant x} n \left\{ \frac{x}{n} \right\}^2 + \gamma_2 x^2 - \int_1^x u \left\{ \frac{x}{u} \right\}^2 du + O(1) \\ &= \gamma_2 x^2 + \int_0^1 \sum_{n \leqslant x} \left(n \left\{ \frac{x}{n} \right\}^2 - (n+u) \left\{ \frac{x}{n+u} \right\}^2 \right) du + O(x). \end{aligned}$$

Inserting the bound of Kolesnik (1982),

$$\sum_{n \leqslant x} \left(n \left\{ \frac{x}{n} \right\}^2 - (n+u) \left\{ \frac{x}{n+u} \right\}^2 \right) \ll x^{1+(6/13)} \log^{7/13} x$$

for $0 \leqslant u \leqslant 1$, yields (36).

It is now a simple matter to obtain (31). By parts (ii) and (iii) of Lemma 5 it is easily seen that

$$\sum_{n \leqslant x} \frac{\phi(n)}{n} \left\{ \frac{x}{n} \right\} = \frac{6}{\pi^2} (1 - \gamma_o) x + O(x^{(7/22)+\varepsilon}), \tag{37}$$

and

$$\sum_{n \leqslant x} \phi(n) \left\{\frac{x}{n}\right\}^2 = \frac{6}{\pi^2} \gamma_2 x^2 + O(x^{1+(6/13)} \log^{7/13} x). \tag{38}$$

By (34), (37) and (38) we have

$$\begin{aligned}\sum_{n \leqslant x} \phi(n) \left[\frac{x}{n}\right]^2 &= x^2 \sum_{n \leqslant x} \frac{\phi(n)}{n^2} - 2x \sum_{n \leqslant x} \frac{\phi(n)}{n} \left\{\frac{x}{n}\right\} + \sum_{n \leqslant x} \phi(n) \left\{\frac{x}{n}\right\}^2 \\ &= \frac{6}{\pi^2} x^2 \log x + \left(\frac{18}{\pi^2} \gamma_o - \gamma_1 + \frac{6}{\pi^2} \gamma_2 - \frac{12}{\pi^2}\right) x^2 \\ &\quad + O(x^{19/13} \log^{7/13} x).\end{aligned}$$

The theorem now follows from (30) and the formulae in Lemma 4.

5. PROOF OF COROLLARY 2

Suppose first that $\mathscr{B}$ is a box with $B_1 = B_3$ and $B_2 = B_4$, so that by (6)

$$|\mathscr{B} \cap V| \ll \frac{|\mathscr{B}|}{p} + O(B_1 B_2 \log p),$$

for any prime p. Choose p so that $B_1 B_2 < p < 2B_1 B_2$. Then,

$$N(\mathscr{B}) \leqslant |\mathscr{B} \cap V| \ll B_1 B_2 \log(B_1 B_2).$$

Now let $\mathscr{B}$ be a box with sides of arbitrary lengths. Then

$$\begin{aligned}N(\mathscr{B}) &= \sum_{\lambda=1}^{\infty} \Bigg(\sum_{\substack{x_1 x_2 = \lambda \\ a_i \leqslant x_i < a_i + B_i}} 1 \Bigg) \Bigg(\sum_{\substack{x_3 x_4 = \lambda \\ a_i \leqslant x_i < a_i + B_i}} 1 \Bigg) \\ &\leqslant \Bigg[\sum_{\lambda=1}^{\infty} \Bigg(\sum_{\substack{x_1 x_2 = \lambda \\ a_i \leqslant x_i < a_i + B_i}} 1 \Bigg)^2 \Bigg]^{1/2} \Bigg[\sum_{\lambda=1}^{\infty} \Bigg(\sum_{\substack{x_3 x_4 = \lambda \\ a_i \leqslant x_i < a_i + B_i}} 1 \Bigg)^2 \Bigg]^{1/2} \\ &\ll \sqrt{B_1 B_2 \log(B_1 B_2)} \sqrt{B_3 B_4 \log(B_3 B_4)}.\end{aligned}$$

Remark. Our method of proving Theorem 1 can be applied to a more general set of points V satisfying

$$a x_1 x_2 + b x_3 x_4 \equiv f(x_1, x_3) \pmod p,$$

where a, b are any nonzero integers $(\mathrm{mod}\, p)$, and $f(x_1, x_3)$ is any integer valued function defined over $\mathbb{Z}^2$. One obtains the same result as in

Theorem 1. It is desirable to be able to prove Theorem 1 for the set of points V satisfying

$$L_1(\mathbf{x})\, L_2(\mathbf{x}) \equiv L_3(\mathbf{x})\, L_4(\mathbf{x}) \pmod p,$$

where the L_i are linear forms $L_i(\mathbf{x}) = \sum_{i=1}^{4} a_{ij} x_i$ and the matrix $[a_{ij}]$ is nonsingular $(\mathrm{mod}\, p)$.

ACKNOWLEDGMENTS

The third author thanks the second author and Kansas State University for the invitation to Kansas State University.

REFERENCES

1. D. A. Burgess, Mean values of character sums, *Mathematika* **33**, No. 1 (1986), 1–5.
2. J. B. Friedlander and H. Iwaniec, The divisor problem for arithmetic progressions, *Acta Arith.* **45**, No. 3 (1985), 273–277.
3. J. B. Friedlander and H. Iwaniec, Estimates for character sums, *Proc. Amer. Math. Soc.* **119**, No. 2 (1993), 365–372.
4. H. Iwaniec and C. J. Mozzochi, *J. Number Theory* **29** (1988), 60–93.
5. G. Kolesnik, *Notices Amer. Math. Soc.* **29** (1982), 327.
6. H. L. Montgomery and R. C. Vaughan, Mean values of character sums, *Canad. J. Math.* **31**, No. 3 (1979), 476–487.