THE CONGRUENCE \( x_1 x_2 \equiv x_3 x_4 \pmod{p} \), THE EQUATION \( x_1 x_2 = x_3 x_4 \) AND MEAN VALUES OF CHARACTER SUMS

ANWAR AYYAD, TODD COCHRANE, ZHIYONG ZHENG

Kansas State University, Kansas State University and Zhongshan University

ABSTRACT. We obtain the asymptotic formulae, \( |B \cap V| = \frac{|B|}{p} + O(\sqrt{|B|} \log^2 p) \), for the number of solutions of the congruence \( x_1 x_2 \equiv x_3 x_4 \pmod{p} \) in a box \( B \) of arbitrary size and position, and \( N(B) = \frac{12}{5} B^2 \log B + CB^2 + O(B^{1+\varepsilon} \log^{13} B) \), with \( C \) given explicitly, for the number of solutions of the diophantine equation \( x_1 x_2 = x_3 x_4 \) with \( 1 \leq x_i \leq B \). We also obtain the upper bound for fourth order character sum moments, \( \frac{1}{p-1} \sum_{x \neq x_0} \left| \sum_{x=x_0+1}^{x+a+B} \chi(x) \right|^4 \ll B^2 \log^2 p \).

The distribution of solutions of the congruence
\[
x_1 x_2 \equiv x_3 x_4 \pmod{p},
\]
where \( p \) is a prime, arises naturally in the study of certain character sums. For any integers \( a_i, B_i \), with \( 1 \leq B_i < p \), \( 1 \leq i \leq 4 \) let \( B \) be the box of points
\[
B = \{ x \in \mathbb{Z}^4 : a_i \leq x_i < a_i + B_i \},
\]
of cardinality \( |B| = B_1 B_2 B_3 B_4 \), and \( V \subset \mathbb{Z}^4 \) denote the set of integer solutions of \( (1) \). We may also view \( B \) 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 \( B \) does not meet any of the coordinate planes \( x_i \equiv 0 \pmod{p} \). For such boxes the number of solutions of \( (1) \) in \( B \) may be easily expressed in terms of a character sum:
\[
|B \cap V| = \frac{|B|}{p-1} + \frac{1}{p-1} \sum_{x \neq x_0} \sum_{x \in B} \chi(x_1 x_2 x_3^{-1} x_4^{-1})
\]
where \( \chi \) runs through the set of multiplicative characters on \( \mathbb{F}_p \) and \( \chi_0 \) denotes the principal character. In particular, taking all the \( a_i = a + 1 \) and all of the \( B_i = B \) we have
\[
|B \cap V| = \frac{|B|}{p-1} + \frac{1}{p-1} \sum_{x \neq x_0} \left| \sum_{x=a+1}^{a+B} \chi(x) \right|^4.
\]

Our main theorems are

\[1991 \text{ Mathematics Subject Classification.} \text{ 11D79, 11L40.}\]
\[\text{Key words and phrases.} \text{ congruences, character sums.}\]
Theorem 1. Suppose that $B$ is a box of the type (2) not meeting any coordinate plane. Then

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

(5)

In particular, if $|B| \gg p^2 \log^4 p$ then $B$ 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 $1 \leq x_1, x_2 \leq \sqrt{p}/2$, $\sqrt{p}/2 < x_3, x_4 < \sqrt{p}$. 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

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

(6)

Further cases where the savings of $\log p$ can be had are given at the end of section 3. Friedlander and Iwaniec (1993, Lemma) had established the upper bound in (6) for the box $1 \leq x_1, x_3 \leq B_1, a \leq x_2, x_4 \leq a + B_2$, 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

$$\frac{1}{p-1} \sum_{x \neq x_0} \sum_{x = a+1}^{a+B} \chi(x)^4 \ll B^2 \log^2 p.$$  

(7)

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

$$\frac{1}{p-1} \sum_{x \neq x_0} \sum_{x = a+1}^{a+B} \chi(x)^4 \ll B^2 \log p,$$

(8)

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

$$\frac{1}{p-1} \sum_{x \neq x_0} \sum_{x = 1}^{B} \chi(x)^4 = \frac{12}{\pi^2} B^2 \log B + \left( C - \frac{B^2}{p} \right) B^2 + O(B^{\frac{15}{13}} \log \frac{7}{13} B),$$

(9)

where $C = -.511317447 \ldots$ 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 (1985, 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 (1979, Theorem 1),

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

and the result of Burgess (1986, Lemma 1),

$$\sum_{\chi \neq \chi_0} \sum_{x=1}^{p} \left| \sum_{m=1}^{B} \chi(x + m) \right|^4 \leq 6p^2B^2.$$

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 $x_1x_2 = x_3x_4$, and establish a precise asymptotic formula for the number of solutions in a cube cornered at the origin.

**Theorem 3.** The number $N(B)$ of integer solutions of the equation $x_1x_2 = x_3x_4$ with $1 \leq x_i \leq B$, $1 \leq i \leq 4$, is given by

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

where $C = \frac{\gamma}{\pi^2}(12\gamma - \frac{36}{\pi^2}\zeta'(2) - 3) - 2 = -0.511317447\ldots$, $\gamma$ is Euler's constant and $\zeta'(2) = \sum_{n=1}^{\infty} \frac{\log n}{n^2}$.

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

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

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

**Another easy consequence of (6) is**

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

$$N(B) \ll \sqrt{|B| \log(|B|)}.$$  \quad (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 \( x_1 x_2 - x_3 x_4 = j p \) for the appropriate range of values of \( j \). Upon summing over \( x_1 \) and \( x_3 \) we obtain the upper bound in Lemma 2,

\[
|B \cap V| \ll \frac{|B|}{p} + \sqrt{|B|} \log p,
\]

for a box of the type

\[
B = \{ x \in \mathbb{Z}^4 : 1 \leq x_i \leq B_i, 1 \leq i \leq 4 \},
\]

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 \( \alpha \) denote the characteristic function of the box \( B \) in (2), viewed as a subset of \( \mathbb{F}_p^4 \), with finite Fourier expansion

\[
\alpha(x) = \sum_y a(y)e_p(x \cdot y).
\]

Here, \( e_p(x) = e^{2\pi i x/p} \) and \( x \cdot y = x_1 y_1 + x_2 y_2 + x_3 y_3 + x_4 y_4 \), and \( \sum_y \) denotes the complete sum over \( y \in \mathbb{F}_p^4 \). Then

\[
|B \cap V| = \sum_{x_1 x_2 x_3 x_4 \atop x_i \neq 0} \alpha(x) = \frac{1}{p-1} \sum_x \alpha(x) \sum_x \chi(x_1 x_2 x_3^{-1} x_4^{-1}),
\]

\[
= \frac{1}{p-1} \sum_x \alpha(x) + \frac{1}{p-1} \sum_{x \neq x, x_i \neq 0} \sum_x \alpha(x) \chi(x_1 x_2 x_3^{-1} x_4^{-1})
\]

\[
= \frac{1}{p-1} \sum_x \alpha(x) + \frac{1}{p-1} \sum_y \alpha(y) \sum_{x \neq x, x_i \neq 0} \chi(x_1 x_2 x_3^{-1} x_4^{-1}) e_p(x \cdot y).
\]

Now if any \( y_i = 0 \) then the sum over \( \chi \) and \( x \) is zero. If all of the \( y_i \) are nonzero then the sum over \( x \) is just

\[
\Pi_{i=1}^2 \sum_{x_i \neq 0} \chi(x_i) e_p(x_i y_i) \Pi_{i=3}^4 \sum_{x_i \neq 0} \chi(x_i^{-1}) e_p(x_i y_i).
\]

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

\[
= \chi(y_1^{-1} y_2^{-1} y_3 y_4) G(\chi) G(\chi^{-1}) = p^2 \chi(y_1^{-1} y_2^{-1} y_3 y_4),
\]

since \( G(\chi^{-1}) = \chi(-1) G(\overline{\chi}) \) and \( |G(\chi)|^2 = p \) for \( \chi \neq \chi_0 \). Summing over \( \chi \) we obtain the fundamental identity,
Fundamental Identity.

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

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 $B$ we shall apply it to a weighted function $\alpha$ 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,

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

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.

Section 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 $\pmod{p}$ and $d$ the greatest common divisor of $x_1$ and $x_3$. Then

$$\# \{(x_2, x_4) \in \mathbb{Z}^2 : x_1x_2 \equiv x_3x_4 \pmod{p}, a_2 \leq x_2 < a_2 + B_2, a_4 \leq x_4 < a_4 + B_4 \}$$

$$\leq \left( \frac{B_2x_1}{dp} + \frac{B_4x_3}{dp} + 1 \right) \min \left( \frac{B_2d}{x_3} + 1, \frac{B_4d}{x_1} + 1 \right).$$

**Proof.** We must solve the linear diophantine equation

$$x_1x_2 - x_3x_4 = jp \quad (17)$$

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 $d|j$, 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

$$x_2 = x_20 + \lambda x_3/d, \quad x_4 = x_40 + \lambda x_1/d,$$

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

$$\min \left( \frac{B_2d}{x_3} + 1, \frac{B_4d}{x_1} + 1 \right),$$

choices for $\lambda$, and the lemma follows.
Lemma 2. Suppose that $B$ is a box of the type

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

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

$$|B \cap V| \ll \frac{|B|}{p} + \sqrt{|B|} \log p, \quad (18)$$

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

$$|B \cap V| = \sum_{d \leq H} \sum_{x_1 = 1}^{H} \sum_{x_3 = 1}^{K} N(x_1, x_3) \left( \frac{Hx_3}{dp} + 1 \right) \left( \frac{Kd}{x_3} + 1 \right)$$

$$\leq \sum_{d \leq H} \sum_{x_1 = 1}^{H} \sum_{x_3 = 1}^{K} \left( \frac{Hx_3}{dp} + 1 \right) \left( \frac{Kd}{x_3} + 1 \right) + \sum_{d \leq H} \sum_{x_1 = 1}^{H} \sum_{x_3 = 1}^{K} \left( \frac{Kx_1}{dp} + 1 \right) \left( \frac{Hd}{x_1} + 1 \right)$$

$$= \frac{H^2 K^2}{p} + HK + \sum_{d \leq H} \sum_{Kx_1 \leq Hx_3} \left( \frac{Hx_3}{dp} + \frac{Kd}{x_3} \right) + \sum_{d \leq H} \sum_{Kx_1 \geq Hx_3} \left( \frac{Kx_1}{dp} + \frac{Hd}{x_1} \right)$$

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

$$\leq \frac{H^2 K^2}{p} + HK + \sum_{d \leq H} \sum_{u_2 \leq K/d} \left( \frac{H^2 u_2^2}{pK} + H \right) + \sum_{d \leq H} \sum_{u_1 \leq H/d} \left( \frac{K^2 u_1^2}{Hp} + K \right)$$

$$\ll \frac{H^2 K^2}{p} + HK \log p.$$

Lemma 3. Suppose that $B$ is any box of the type (2) not meeting any coordinate plane. Then

$$|B \cap V| \ll \frac{|B|}{p} + (p + B_1 B_2 \log p)^{1/2} (p + B_3 B_4 \log p)^{1/2}, \quad (19)$$

Moreover, the inequality in (19) holds if the products $B_1 B_2$ and $B_3 B_4$ 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 $\alpha$ so that the error term

$$E(\alpha) := p^2 \sum_{\substack{y_1 y_2 = y_3 y_4 \ y_i \neq 0}} a(y),$$
in the fundamental identity (15), admits a good upper bound. We may assume that \( B \) is a box of the type
\[
B = \{ x \in \mathbb{Z}^4 : |x_i - c_i| < B_i/2, 1 \leq i \leq 4 \},
\]
for some integers \( c_i \). Let \( V \) be the set of solutions of (1), \( B_0 = \{ x \in \mathbb{Z}^4 : |x_i| < B_i/2 \} \) and
\[
\alpha = \frac{1}{|B|^4} \chi B_0 \ast \chi B_0 \ast \chi B_0 \ast \chi B_0 \ast \chi B,
\]
a normalized five-fold convolution of the characteristic functions of \( B_0 \) and \( B \). Then
\[
\sum_{x_1 x_2 = x_3 x_4 \atop x_i \neq 0} \alpha(x) \gg |B \cap V|, \tag{20}
\]
\[
\sum_{x_i \neq 0} \alpha(x) \ll |B|, \tag{21}
\]
and the Fourier coefficients \( a(y) \) of \( \alpha \) satisfy
\[
|a(y)| \ll p^{-4} |B|^{-4} \Pi_{i=1}^{4} \min \left( B_i^5, \frac{p^5}{|y_i|^5} \right), \quad (|y_i| < p/2).
\]
Thus, letting the \( y_i \) run through the intervals \( 0 < |y_i| \leq p/B_i \) and \( 2^{k_i+1}p/B_i < |y_i| \leq 2^{k_i+1}p/B_i \) for \( k_i = 0, 1, 2, \ldots \), we have
\[
\sum_{y_1 y_2 = y_3 y_4 \atop y_i \neq 0} |a(y)| \ll p^{-4} |B|^{-4} \sum_{k_1=0}^{K} \sum_{k_2=0}^{K} \sum_{k_3=0}^{K} \sum_{k_4=0}^{K} \sum_{0 < |y_i| \leq 2^{k_i}p/B_i} |B|^5 \Pi_{i=1}^{4} 2^{-5k_i}.
\]
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),
\[
0 < |y_1|, |y_3| \leq 2K p/B_1, \quad 0 < |y_2|, |y_4| \leq 2K p/B_2.
\]
Here we have used our assumption that \( B_1 = B_3 \) and \( B_2 = B_4 \). On applying Lemma 2, we obtain
\[
\sum_{y_1 y_2 = y_3 y_4 \atop y_i \neq 0} |a(y)| \ll p^{-4} |B| \sum_{k_1}^{K} \cdots \sum_{k_4}^{K} \Pi_{i=1}^{4} 2^{-5k_i} \left( \frac{2^4Kp^3}{|B|} + \frac{2^2Kp^2 \log p}{B_1B_2} \right)
\]
\[
\ll \frac{1}{p} + p^{-2} |B|^{1/2} \log p,
\]
and so
\[
E(\alpha) \ll p + |B|^{1/2} \log p. \tag{22}
\]
Suppose now that $B_1, B_2, B_3$ and $B_4$ are arbitrary. Write
\[
\alpha(x) = \alpha_1(x_1)\alpha_2(x_2)\alpha_3(x_3)\alpha_4(x_4).
\]
By (13) the error term $E(\alpha)$ may be expressed
\[
|E(\alpha)| = |E(\alpha_1(x_1)\alpha_2(x_2)\alpha_3(x_3)\alpha_4(x_4))| = \frac{1}{p-1} \left| \sum_{x \neq x_0} \sum_{x_i \neq 0} \alpha(x) \chi(x_1 x_2 x_3^{-1} x_4^{-1}) \right|
\]
\[
= \frac{1}{p-1} \left| \sum_{x \neq x_0} \left( \prod_{i=1}^{2} \sum_{x_i \neq 0} \alpha_i(x_i) \chi(x_i) \right) \left( \prod_{i=3}^{4} \sum_{x_i \neq 0} \alpha_i(x_i) \chi(x_i^{-1}) \right) \right|
\]
\[
\leq \frac{1}{p-1} \left( \sum_{x \neq x_0} \left| \prod_{i=1}^{2} \sum_{x_i \neq 0} \alpha_i(x_i) \chi(x_i) \right|^2 \right)^{1/2} \left( \sum_{x \neq x_0} \left| \prod_{i=3}^{4} \sum_{x_i \neq 0} \alpha_i(x_i) \chi(x_i^{-1}) \right|^2 \right)^{1/2}
\]
\[
= E(\alpha_1(x_1)\alpha_2(x_2)\alpha_1(x_3)\alpha_2(x_4))^{1/2} E(\alpha_3(x_1)\alpha_4(x_2)\alpha_3(x_3)\alpha_4(x_4))^{1/2}
\]
\[
\ll (p + B_1 B_2 \log p)^{1/2} (p + B_3 B_4 \log p)^{1/2},
\]
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 $B_1 B_2$ and $B_3 B_4$ in the statement of Lemma 3 with any other pairing of the $B_i$.

**Section 3. Proof of Theorem 1.**

The third method for counting the solutions of (1) in $B$ is to again view the congruence as an equation over $\mathbb{F}_p$ and write,
\[
\sum_{\substack{x_1 x_2 = x_3 x_4 \equiv x \pmod{p} \\ a_i \leq x_i < a_i + B_i, 1 \leq i \leq 3}} 1 = \sum_{a_i \leq x_i < a_i + B_i, 1 \leq i \leq 3} \alpha(x_1 x_2 x_3^{-1}),
\]
where $\alpha$ is the characteristic function of the interval $a_4 \leq x_4 < a_4 + B_4$. Letting $\alpha(x) = \sum_y a(y) e_p(xy)$ be the finite Fourier expansion of $\alpha$ we obtain,
\[
|B \cap V| = \frac{|B|}{p} + \sum_{y \neq 0} a(y) \sum_{a_i \leq x_i < a_i + B_i, 1 \leq i \leq 3} e_p(x_1 x_2 x_3^{-1} y).
\]

(23)

To bound the error term in (23) we sum over $x_2$ to obtain
\[
|\text{Error}| \leq \sum_{y \neq 0} |a(y)| \sum_{a_i \leq x_i < a_i + B_i, i=1,3} \left| \frac{\sin(\pi x_1 x_3^{-1} y B_2 / p)}{\sin(\pi x_1 x_3^{-1} y / p)} \right| 
\]
\[
= \sum_{y \neq 0} |a(y)| \sum_{\ell \neq 0} \left| \frac{\sin(\pi \ell B_2 / p)}{\sin(\pi \ell / p)} \right| \sum_{x_1 y = x_3 \ell} 1.
\]
\[ p^{-1} \sum_{y \neq 0} \min(B_4, \frac{p}{|y|}) \sum_{\ell \neq 0} \min(B_2, \frac{p}{|\ell|}) \sum_{\substack{a_i \leq x_i < a_i + B_i, i = 1, 3 \atop x_1 y = x_2 \ell}} 1. \]

Letting \( y \) run through the intervals \( 0 < |y| \leq p/B_4 \) and \( 2^i p/B_4 < |y| \leq 2^{i+1} p/B_4 \) for \( i = 0, 1, 2, \ldots \), stopping as soon as \( 2^i > B_4/4 \), and doing the same thing for \( \ell \) we obtain

\[ |\text{Error}| \ll p^{-1} B_2 B_4 \sum_{i=0}^{2^{i+1}} \sum_{j=0}^{2^{i-j}} 2^{-i-j} |B_{ij} \cap V| \quad (24) \]

where for any \( i \) and \( j \),

\[ B_{ij} = \{(x_1, y, x_3, \ell) \in \mathbb{Z}^4 : a_k \leq x_k < a_k + B_k, k = 1, 3, 0 < |y| \leq 2^i p/B_4, 0 < |\ell| \leq 2^i p/B_2 \}. \]

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

\[ |B_{ij} \cap V| \ll \frac{2^{i+j} B_1 B_3 p}{B_2 B_4} + (p + 2^i p B_1 \log p/B_2)^{1/2} \left( p + 2^i p B_3 \log p/B_4 \right)^{1/2} \]

\[ \ll \frac{2^{i+j} B_1 B_3 p}{B_2 B_4} + 2 i^2 p \log p \sqrt{B_1 B_3 / B_2 B_4}. \]

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

\[ |\text{Error}| \ll B_1 B_3 \log^2 p + \sqrt{B_1 B_2 B_3 B_4} \log p \ll B_1 B_3 \log^2 p. \quad (25) \]

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

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

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

\[ |B \cap V| - B / p - 1| \ll \frac{1}{p - 1} \left( \Pi_{i=1}^{4} \sum_{\chi \neq \chi_0} \sum_{a_i \leq x_i < a_i + B_i} \chi(x_i)^4 \right)^{1/4} \]

\[ \ll \Pi_{i=1}^{4} B_i^{1/2} \log^2 p. \]

We turn now to the proof of the approximation formula

\[ |B \cap V| \approx \frac{|B|}{p} + O(\sqrt{|B|} \log p), \quad (26) \]

in a number of special cases.
Proposition. Suppose that $B$ is a box not meeting any coordinate plane with $B_1$ the largest dimension and $B_3 \geq \min(B_2, B_4)$. Then

$$|B \cap V| \approx \frac{|B|}{p} + O(B_1 B_3 \log p).$$  \hspace{1cm} (27)

Proof. We proceed as in the proof of Theorem 1 above, only this time we replace $\alpha$ 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

$$|\text{Error}| \ll p^{-1} B_2 B_4 \sum_{i=0} \sum_{j=0} 2^{-2i-j} |B_{ij} \cap V|,$$  \hspace{1cm} (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

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

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

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

$$|B \cap V| \ll \sqrt{|B|} \log p.$$  \hspace{1cm} (29)

To obtain (29) suppose, without loss of generality, that $B_1 B_4 \ll p \log p$ and $B_2 B_3 \ll p \log p$. By an application of Cauchy's inequality we have,

$$|B \cap V| = \sum_{\substack{x_1 x_2 = x_3 x_4 \atop a_1 \leq x_1 < a_1 + B_1}} \sum_{\substack{x_1 x_4 = x_2 \atop x_1/x_4 = \beta}} \left( \sum_{x_2, x_3 \atop x_3/x_2 = \beta} 1 \right) \left( \sum_{x_2, x_3 \atop x_3/x_2 = \beta} 1 \right) \cdots \ll \left( \sum_{x_1 x_4 = u_1 x_4 \atop a_1 \leq x_1 < a_1 + B_1} \sum_{x_1 x_4 = u_1 x_4 \atop a_4 \leq x_4 < a_4 + B_4} 1 \right)^{1/2} \left( \sum_{x_2 x_3 = u_2 x_3 \atop a_2 \leq x_2 < a_2 + B_2} \sum_{x_2 x_3 = u_2 x_3 \atop a_3 \leq x_3 < a_3 + B_3} 1 \right)^{1/2} \ll (\sqrt{B_1 B_4 \log p})(\sqrt{B_2 B_3 \log p}),$$

the last inequality following from the above Proposition.
Section 4. Proof of Theorem 3. We have

$$N(B) := \sum_{\substack{x_1 x_2 = x_3 x_4 \leq B \leq \ell \leq B}} 1 = \sum_{\substack{1 \leq a, b \leq B \leq \ell \leq B}} \left( \sum_{\substack{\frac{x_1}{x_2} = \frac{a}{b}}} 1 \right)^2.$$  

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

$$= B^2 + 2 \sum_{\substack{1 \leq a < b \leq B \leq \ell \leq B}} \left( \sum_{\substack{\frac{x_1}{x_2} = \frac{a}{b}}} 1 \right)^2 = B^2 + 2 \sum_{\substack{1 \leq a < b \leq B \leq \ell \leq B}} \left[ \frac{B}{b} \right]^2.$$  

Thus, it is sufficient to show that

$$\sum_{n \leq x} \phi(x) \left[ \frac{x}{n} \right]^2 = \frac{6}{\pi^2} x^2 \log x + C' x^2 + O(x^{10} \log^{13} x)$$  

for the appropriate constant $C'$.

Lemma 4. Let $\gamma_0 = .57721 \ldots$ denote Euler’s constant and $\{x\} = x - [x]$. Then

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

$$(ii) \quad \gamma_2 := \int_1^{\infty} \frac{\{y\}^2}{y^3} dy = \frac{3}{2} - \gamma_0 - \frac{\pi^2}{12}$$

Proof. Part (i) follows from $\zeta^{-1}(s) = \sum_{n=1}^{\infty} \frac{\mu(n)}{n^s}$. 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 $\sum_{n=1}^{x} \frac{1}{n} = \log x + \gamma_0 + O(1/x).$
Lemma 5. We have

\begin{equation}
(i) \quad \sum_{n \leq 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}
\end{equation}

\begin{equation}
(ii) \quad \sum_{n \leq x} \left\{ \frac{x}{n} \right\} = (1 - \gamma_o) x + O\left( x^{\frac{7}{32} + \epsilon} \right), \tag{35}
\end{equation}

and

\begin{equation}
(iii) \quad \sum_{n \leq x} n\left\{ \frac{x}{n} \right\}^2 = \gamma_2 x^2 + O\left( x^{\frac{19}{13}} \log^{\frac{17}{13}} x \right). \tag{36}
\end{equation}

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

\[ \sum_{n \leq x} d(n) = x \log x + (2 \gamma_o - 1) x + \Delta(x), \]

where by the work of Iwaniec and Mozzochi (1988), \( \Delta(x) \ll x^{\frac{7}{32} + \epsilon} \). On the other hand,

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

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

\[ \sum_{n \leq x} n\left\{ \frac{x}{n} \right\}^2 = \sum_{n \leq x} n\left\{ \frac{x}{n} \right\}^2 + \gamma_2 x^2 - \int_1^x u \left\{ \frac{x}{u} \right\}^2 du + O(1) \]

\[ = \gamma_2 x^2 + \int_0^1 \sum_{n \leq x} \left( n\left\{ \frac{x}{n} \right\}^2 - (n + u)\left\{ \frac{x}{n + u} \right\}^2 \right) du + O(x). \]

Inserting the bound of Kolesnik (1982),

\[ \sum_{n \leq x} \left( n\left\{ \frac{x}{n} \right\}^2 - (n + u)\left\{ \frac{x}{n + u} \right\}^2 \right) \ll x^{1 + \frac{6}{13}} \log^{\frac{17}{13}} x \]

for \( 0 \leq u \leq 1 \), yields (36).

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

\begin{equation}
\sum_{n \leq x} \frac{\phi(n)}{n} \left\{ \frac{x}{n} \right\} = \frac{6}{\pi^2} (1 - \gamma_o) x + O\left( x^{\frac{7}{32} + \epsilon} \right), \tag{37}
\end{equation}

and

\begin{equation}
\sum_{n \leq x} \phi(n) \left\{ \frac{x}{n} \right\}^2 = \frac{6}{\pi^2} \gamma_2 x^2 + O\left( x^{1 + \frac{6}{13}} \log^{\frac{17}{13}} x \right). \tag{38}
\end{equation}
By (34), (37) and (38) we have
\[
\sum_{n \leq x} \phi(n) \left( \frac{x}{n} \right)^2 = x^2 \sum_{n \leq x} \phi(n) \frac{x}{n^2} - 2x \sum_{n \leq x} \phi(n) \left\{ \frac{x}{n} \right\} + \sum_{n \leq x} \phi(n) \left\{ \frac{x}{n} \right\}^2
\]
\[
= \frac{6}{\pi^2} x^2 \log x + \left( \frac{18}{\pi^2} \gamma_0 - \gamma_1 + \frac{6}{\pi^2} \gamma_2 - \frac{12}{\pi^2} \right)x^2 + O(x^{1/2} \log^{1/3} x).
\]
The Theorem now follows from (30) and the formulae in Lemma 4.

Section 5. Proof of Corollary 2. Suppose first that \( B \) is a box with \( B_1 = B_3 \) and \( B_2 = B_4 \), so that by (6)
\[
|B \cap V| \ll \frac{|B|}{p} + O(B_1 B_2 \log p),
\]
for any prime \( p \). Choose \( p \) so that \( B_1 B_2 < p < 2B_1 B_2 \). Then,
\[
N(B) \leq |B \cap V| \ll B_1 B_2 \log(B_1 B_2).
\]
Now let \( B \) be a box with sides of arbitrary lengths. Then
\[
N(B) = \sum_{\lambda=1}^{\infty} \left( \sum_{x_1, x_2, x_3 = \lambda \atop a_i \leq x_i < a_i + B_i} 1 \right) \left( \sum_{x_2, x_4 = \lambda \atop a_i \leq x_i < a_i + B_i} 1 \right)
\]
\[
\ll \sum_{\lambda=1}^{\infty} \left( \sum_{x_1, x_2 = \lambda \atop a_i \leq x_i < a_i + B_i} 1 \right)^2 \sum_{\lambda=1}^{\infty} \left( \sum_{x_2, x_4 = \lambda \atop a_i \leq x_i < a_i + B_i} 1 \right)^2 \frac{1}{\lambda} \frac{1}{\lambda}
\]
\[
\ll \sqrt{B_1 B_2 \log(B_1 B_2)} \sqrt{B_3 B_4 \log(B_3 B_4)}.
\]

Remark. Our method of proving Theorem 1 can be applied to a more general set of points \( V \) satisfying
\[
ax_1 x_2 + bx_3 x_4 \equiv f(x_1, x_3) \pmod{p},
\]
where \( a, b \) are any nonzero integers \( \pmod{p} \), 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
\[
L_1(x) L_2(x) \equiv L_3(x) L_4(x) \pmod{p},
\]
where the \( L_i \) are linear forms \( L_i(x) = \sum_{i=1}^{4} a_{i} x_i \) and the matrix \( [a_{ij}] \) is nonsingular \( \pmod{p} \). The third author wishes to thank the second author and Kansas State University for the invitation to Kansas State University.
REFERENCES


**Kansas State University, Manhattan KS 66506, U. S. A.**

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

**Zhongshan University, Guangzhou 510275, P. R. China**