THE DISTRIBUTION OF SOLUTIONS
OF THE CONGRUENCE $x_1x_2x_3\ldots x_n \equiv c \pmod{p}$

ANWAR AYYAD

(Communicated by Dennis A. Hejhal)

Abstract. For a cube $B$ of size $B$, we obtain a lower bound on $B$ so that $B \cap V$ is nonempty, where $V$ is the algebraic subset of $\mathbb{F}_p^n$ defined by

$$x_1x_2x_3\ldots x_n \equiv c \pmod{p},$$

$n$ a positive integer and $c$ an integer not divisible by $p$. For $n = 3$ we obtain that $B \cap V$ is nonempty if $B \gg p^3 \log p$, for $n = 4$ we obtain that $B \cap V$ is nonempty if $B \gg \sqrt{p} \log p$, and for $n \geq 5$ we obtain that $B \cap V$ is nonempty if $B \gg p^{\frac{8}{3} + \frac{8}{n(n+1)}} \log p$. Using the assumption of the Grand Riemann Hypothesis we obtain $B \cap V$ is nonempty if $B \gg_p p^{\frac{3}{2} + \epsilon}$.

1. Introduction

We use multiplicative characters to study the congruence

$$x_1x_2x_3\ldots x_n \equiv c \pmod{p},$$

where $c$ is an integer not divisible by $p$, and $n > 2$ is a positive integer. In particular if $V$ is the algebraic subset of $\mathbb{F}_p^n$ defined by (1), and $B$ the cube of size $B$ defined by

$$B = \{x \in \mathbb{F}_p^n : a_i + 1 \leq x_i \leq a_i + B, 1 \leq i \leq n\},$$

we find how large $B$ must be to guarantee that $B \cap V$ is nonempty. More generally, if $B$ is a box having sides of arbitrary lengths,

$$B = \{x \in \mathbb{F}_p^n : a_i + 1 \leq x_i \leq a_i + B_i, 1 \leq i \leq n\},$$

then our interest is in finding how large the cardinality $|B|$ of $B$ must be to guarantee $B \cap V$ is nonempty. For $n = 2$ it is known for a cube of type (2) that $B \cap V$ is nonempty if $B \gg p^4$. This follows from Weil’s bound on the Kloosterman sum. R. A. Smith [4] conjectured that for a cube centered at the origin, $B \cap V$ is nonempty if $B \gg p^2$. He was able to prove this result on the assumption of a conjecture of Hooley.

In this paper we consider larger values of $n$, and we have the following main theorems.

Received by the editors May 9, 1997.
1991 Mathematics Subject Classification. Primary 11D79, 11L40.
Key words and phrases. Distribution, congruences, solutions.
Theorem 1. Let $\mathcal{B}$ be a box of type (3), and $V$ the algebraic subset of $\mathbb{F}_p^n$ defined by (1). Then

(i) For $n = 3$, $\mathcal{B} \cap V$ is nonempty if $|\mathcal{B}| \gg p^2 \log^2 p$. In particular if $\mathcal{B}$ is a cube of size $\mathcal{B}$, then $\mathcal{B} \cap V$ is nonempty if $\mathcal{B} \gg p^{3/2} \log p$.

(ii) For $n = 4$, $\mathcal{B} \cap V$ is nonempty if $|\mathcal{B}| \gg p^2 \log^2 p$. In particular if $\mathcal{B}$ is a cube of size $\mathcal{B}$, then $\mathcal{B} \cap V$ is nonempty if $\mathcal{B} \gg \sqrt{\log p}$.

With extra work using other methods we can obtain a slight saving in this theorem. When $n = 3$ we can show that for a box of type (3), $\mathcal{B} \cap V$ is nonempty if $|\mathcal{B}| \gg p^{2}$. For $n = 4$ we can save a factor of $\sqrt{\log p}$ on the size $\mathcal{B}$, and show that for any cube $\mathcal{B}$ of type (2), $\mathcal{B} \cap V$ is nonempty if $\mathcal{B} \gg \sqrt{p \log p}$. The details will appear in forthcoming work.

For larger values of $n$ we use the result of Burgess [2] and prove

Theorem 2. Let $\mathcal{B}$ be a cube of type (2), and $V$ the algebraic subset of $\mathbb{F}_p^n$ defined by (1) with $n \geq 5$. Then $\mathcal{B} \cap V$ is nonempty if

$$\mathcal{B} \gg p^{1/4} + (\log p)^{3/2}.$$  

On the assumption of the generalized Lindelöf hypothesis we are able to sharpen the result of Theorem 2 and prove

Theorem 3. For any cube $\mathcal{B}$ of type (2), and algebraic set $V$ defined by (1) with $n \geq 5$, $\mathcal{B} \cap V$ is nonempty if $\mathcal{B} \gg p^{1/4} + \epsilon$.

2. Lemmas

For any prime $p$, we let $\sum_{\chi \neq \chi_0}^\chi(a + B)\sum_{x=a+1}^{a+B}\chi(x)$ denote a sum over all multiplicative characters $\chi \pmod{p}$ with $\chi \neq \chi_0$, the principal character.

Lemma 1.  

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

This is just Theorem 2 of Ayyad, Cochrane, and Zheng [1].

Lemma 2.  

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

Proof.  

$$\sum_{\chi \neq \chi_0} \left| \sum_{x=a+1}^{a+B} \chi(x) \right|^2 = \sum_{\chi \neq \chi_0} \left( \sum_{x=a+1}^{a+B} \chi(x) \sum_{y=a+1}^{a+B} \chi(y) \right)$$

$$= \sum_{x,y=a+1}^{a+B} \left( \sum_{\chi \neq \chi_0} \chi(xy^{-1}) \right)$$

$$\leq \sum_{x,y=a+1}^{a+B} \left( \sum_{\chi \neq \chi_0} \chi(xy^{-1}) \right)$$

$$\leq (p-1)B.$$
To obtain results for values of \( n \geq 5 \) we need the following result of Burgess.

**Lemma 3** (Burgess [2]). For any positive integer \( r \geq 2 \), and nonprincipal character \( \chi \),

\[
\sum_{x=a+1}^{a+B} \chi(x) \ll B^{\frac{1}{r}} p^{rac{r+1}{r^2}} (\log p)^{\frac{3}{4r^2}}.
\]

**Lemma 4.** For every integer \( n \geq 5 \) there exists an integer \( r \geq 2 \) such that

\[
\frac{2r^2 + n - 4}{r(8r + 4n - 16)} < \frac{1}{\sqrt{2(n + 4)}}.
\]

**Proof.** For any integer \( n \geq 5 \) and positive real number \( x \) we have

\[
\frac{2x^2 + n - 4}{x(8x + 4n - 16)} < \frac{1}{\sqrt{2(n + 4)}}
\]

\[
\iff x^2 + \frac{2(n - 4)x}{4 - \sqrt{2(n + 4)}} - \frac{(n - 4)\sqrt{2(n + 4)}}{2(4 - \sqrt{2(n + 4)})} < 0.
\]

The graph of the quadratic function

\[
f(x) = ax^2 + bx + c =: x^2 + \frac{2(n - 4)x}{4 - \sqrt{2(n + 4)}} - \frac{(n - 4)\sqrt{2(n + 4)}}{2(4 - \sqrt{2(n + 4)})}
\]

is a parabola opening upwards. Now

\[
b^2 - 4ac = \frac{4(n - 4)^2}{(4 - \sqrt{2(n + 4)})^2} - \frac{2(4 - n)\sqrt{2(n + 4)}}{4 - \sqrt{2(n + 4)}}
\]

\[
= \frac{128 - 32n - 8(4 - n)\sqrt{2(n + 4)}}{(4 - \sqrt{2(n + 4)})^2}.
\]

We also have

\[
128 - 32n - 8(4 - n)\sqrt{2(n + 4)} > (4 - \sqrt{2(n + 4)})^2
\]

\[
\iff (8n - 24)\sqrt{2(n + 4)} > 34n - 104.
\]

Since the last inequality holds true for \( n \geq 5 \) we see that \( b^2 - 4ac > 1 \). Therefore \( f(x) \) has real roots \( x_1 < x_2 \), with \( x_2 - x_1 = \sqrt{b^2 - 4ac} > 1 \). Moreover,

\[
x_2 = \frac{-b + \sqrt{b^2 - 4ac}}{2} > \frac{n - 4}{\sqrt{2(n + 4)} - 4} + \frac{1}{2} > 2,
\]

for \( n \geq 5 \). Since \( x_2 - x_1 > 1 \) and \( x_2 > 2 \), there exists an integer \( r \geq 2 \) with \( x_1 < r < x_2 \). Also, since \( f(x) < 0 \) on the interval \( (x_1, x_2) \), we have \( f(r) < 0 \). Thus \( r \) satisfies (5) and so

\[
\frac{2r^2 + n - 4}{r(8r + 4n - 16)} < \frac{1}{\sqrt{2(n + 4)}}.
\]
3. Proof of Theorem 1

Suppose that \( n = 3 \) and that \( \mathcal{B} \) is a box of type (3). Then

\[
|\mathcal{B} \cap V| = \sum_{x \in \mathcal{B}} 1 = \sum_{x_1 x_2 x_3 = c} 1
\]

\[
= \frac{1}{p-1} \sum_{\chi} \left( \sum_{a_i} \chi(x_1) \chi(x_2) \chi(x_3) \right)
\]

(6)

\[
= \frac{|\mathcal{B}|}{p-1} + \frac{1}{p-1} \sum_{\chi \neq \chi_0} \chi(c^{-1}) \sum_{a_i} \chi(x_1) \chi(x_2) \chi(x_3).
\]

Using the Cauchy-Schwarz inequality we bound the error term in (6) as follows:

\[
|\sum_{\chi \neq \chi_0} \chi(c^{-1}) \sum_{a_i} \chi(x_1) \chi(x_2) \chi(x_3)|
\]

\[
\leq \sum_{\chi \neq \chi_0} \left( \sum_{x_1 = a_1 + 1}^{a_1 + B_1} \chi(x_1) \cdot \sum_{x_2 = a_2 + 1}^{a_2 + B_2} \chi(x_2) \cdot \sum_{x_3 = a_3 + 1}^{a_3 + B_3} \chi(x_3) \right)
\]

\[
\leq \left( \sum_{\chi \neq \chi_0} \left( \sum_{x_1 = a_1 + 1}^{a_1 + B_1} \chi(x_1)^2 \right) \cdot \left( \sum_{\chi \neq \chi_0} \left( \sum_{x_2 = a_2 + 1}^{a_2 + B_2} \chi(x_2)^2 \cdot \sum_{x_3 = a_3 + 1}^{a_3 + B_3} \chi(x_3)^2 \right) \right)^{\frac{1}{2}}
\]

\[
\leq \left( \sum_{\chi \neq \chi_0} \left( \sum_{x_1 = a_1 + 1}^{a_1 + B_1} \chi(x_1)^2 \right) \cdot \prod_{i=2}^{3} \left( \sum_{\chi \neq \chi_0} \left( \sum_{x_i = a_i + 1}^{a_i + B_i} \chi(x_i) \right)^4 \right)^{\frac{1}{4}}.
\]

Now by Lemma 1 and Lemma 2 we obtain the following bound on the error term in (6):

\[
|\text{error}| \ll \frac{1}{p-1} \sqrt{(p-1)B_1} \cdot \prod_{i=2}^{3} ((p-1)B_i^2 \log^2 p)^{\frac{1}{2}}
\]

\[
\ll |\mathcal{B}|^{\frac{1}{2}} \log p.
\]

Thus

\[
|\mathcal{B} \cap V| = \frac{|\mathcal{B}|^3}{p-1} + O \left( |\mathcal{B}|^{\frac{1}{2}} \log p \right).
\]

For \( \mathcal{B} \cap V \) not to be empty it suffices that

\[
\frac{|\mathcal{B}|^3}{p-1} \gg |\mathcal{B}|^{\frac{1}{2}} \log p,
\]

that is,

\[
|\mathcal{B}| \gg p^2 \log^2 p.
\]
When \( n = 4 \), we proceed in a similar manner to obtain
\[
|B \cap V| = \frac{|B|}{p - 1} + \frac{1}{p - 1} \sum_{\chi \neq \chi_0} \chi(c^{-1}) \sum_{x_i = a_i + 1}^{a_i + B_1} \chi(x_1) \chi(x_2) \chi(x_3) \chi(x_4).
\]

Using the Cauchy-Schwarz inequality we obtain
\[
|\sum_{\chi \neq \chi_0} \chi(c^{-1}) \sum_{x_i = a_i + 1}^{a_i + B_1} \chi(x_1) \chi(x_2) \chi(x_3) \chi(x_4)|
\leq \sum_{\chi \neq \chi_0} \left| \sum_{x_1 = a_1 + 1}^{a_1 + B_2} \chi(x_1) \sum_{x_2 = a_2 + 1}^{a_2 + B_3} \chi(x_2) \sum_{x_3 = a_3 + 1}^{a_3 + B_3} \chi(x_3) \sum_{x_4 = a_4 + 1}^{a_4 + B_4} \chi(x_4) \right|^2
\leq \sum_{\chi \neq \chi_0} \left( \sum_{x_1 = a_1 + 1}^{a_1 + B_1} \chi(x_1) \right)^2 \left( \sum_{i=1}^{4} \chi(x_i) \right)^4
\leq \frac{4}{p - 1} \left( \sum_{x_1 = a_1 + 1}^{a_1 + B_1} \chi(x_1) \right)^4.
\]

Now by Lemma 2 we obtain the following bound on the error term in (7):
\[
|\text{error}| \ll \frac{1}{p - 1} \prod_{i=1}^{4} (pB_i^2 \log^2 p)^{\frac{1}{2}}
\ll \sqrt{B_1 B_2 B_3 B_4} \log^2 p = |B| \frac{1}{2} \log^2 p.
\]

Therefore we obtain
\[
|B \cap V| = \frac{|B|}{p - 1} + O \left( |B| \frac{1}{2} \log^2 p \right).
\]

Thus for \( B \cap V \) not to be empty it suffices that
\[
\frac{|B|}{p - 1} \gg |B| \frac{1}{2} \log^2 p,
\]
that is,
\[
|B| \gg p^2 \log^4 p.
\]

4. Proof of Theorem 2

For any cube \( B \) of size \( B \) we have
\[
|B \cap V| = \frac{B^n}{p - 1} + \frac{1}{p - 1} \sum_{\chi \neq \chi_0} \chi(c^{-1}) \sum_{x_i = a_i + 1}^{a_i + B} \chi(x_1) \chi(x_2) \ldots \chi(x_n).
\]

The error term in (9) is bounded above by
\[
\frac{1}{p - 1} \sum_{\chi \neq \chi_0} \left( \prod_{i=1}^{n} \sum_{x_i = a_i + 1}^{a_i + B} \chi(x_i) \right).
\]
Thus
\begin{align*}
|B \cap V| &\geq \frac{B^n}{p-1} - \frac{1}{p-1} \sum_{\chi \neq \chi_0} \left( \prod_{i=1}^{n} \sum_{x_i = a_i + 1}^{a_i + B} \chi(x_i) \right).
\end{align*}

The term
\begin{align*}
\frac{1}{p-1} \sum_{\chi \neq \chi_0} \left( \prod_{i=1}^{n} \sum_{x_i = a_i + 1}^{a_i + B} \chi(x_i) \right)
\end{align*}
in (10) may be bounded as follows:
\begin{align*}
&\leq \frac{n}{p-1} \sum_{\chi \neq \chi_0} \left( \max_{i=1}^{n} \sum_{x_i = a_i + 1}^{a_i + B} \chi(x_i) \right) \cdot \frac{1}{p-1} \sum_{\chi \neq \chi_0} \left( \prod_{i=1}^{4} \sum_{x_i = a_i + 1}^{a_i + B} \chi(x_i) \right).
\end{align*}

Inserting the upper bound of Burgess, Lemma 3, and the upper bound in (8) we obtain
\begin{align*}
&\leq \left( B^{1-n} \frac{\log p}{p} \right)^{n-4} \frac{1}{p-1} \sum_{\chi \neq \chi_0} \left( \prod_{i=1}^{4} \sum_{x_i = a_i + 1}^{a_i + B} \chi(x_i) \right).
\end{align*}

Therefore
\begin{align*}
|B \cap V| = \frac{B^n}{p-1} + O \left( B^{2+ \frac{n-4r-n+4}{r} + 4} \frac{\log p}{p} \right)^{4} \frac{4r+3n-12}{2r}
\end{align*}

Thus $B \cap V$ is nonempty if
\begin{align*}
\frac{B^n}{p-1} \gg B^{2+ \frac{n-4r-n+4}{r} + 4} \frac{\log p}{p} \left( \log p \right)^{4} \frac{4r+3n-12}{2r},
\end{align*}

that is,
\begin{align*}
(11) \quad B \gg p^{\frac{4r+3n-12}{8r^2+4rn-16r}} \left( \log p \right)^{\frac{4r+3n-12}{4r+2n-8}}.
\end{align*}

Now the power of $p$ in (11) is
\begin{align*}
\frac{4r^2 + rn + n - 4r - 4}{8r^2 + 4rn - 16r} = \frac{1}{4} + \frac{2r^2 + n - 4}{r(8r + 4n - 16)}.
\end{align*}

By Lemma 4 for any integer $n \geq 5$ there exists an integer $r \geq 2$ such that
\begin{align*}
\frac{2r^2 + n - 4}{r(8r + 4n - 16)} < \frac{1}{\sqrt{2(n+4)}}.
\end{align*}

For such choice of $r$ the power of $p$ in (11) satisfies
\begin{align*}
\frac{4r^2 + rn + n - 4r - 4}{8r^2 + 4rn - 16r} < \frac{1}{4} + \frac{1}{\sqrt{2(n+4)}}.
\end{align*}

Since the power of $\log p$ in (11) satisfies
\begin{align*}
\frac{4r + 3n - 12}{4r + 2n - 8} < \frac{3}{2},
\end{align*}
we have that $B \cap V$ is nonempty if
\[ B \gg p^{\frac{1}{2} + \frac{1}{\sqrt{2n+1}} (\log p)^{\frac{3}{2}}}. \]

**The optimal choice of $r$ in (11).** The best choice of $r$ is that integer which minimizes the power of $p$ in (11). Using calculus it is easy to see that the power of $p$ in (11) is minimal when
\[
(8r^2 + 4rn - 16)(8r + n - 4) - (4r^2 + nr - 4r + n - 4)(16r + 4n - 16) = 0,
\]
that is,
\[ r^2(2n - 8) + r(16 - 4n) + n(8 - n) - 16 = 0. \]
Therefore for $n \geq 5$ we take $r$ to be
\[
 r = \left[ 1 + \frac{\sqrt{2n^3 - 20n^2 + 64n - 64}}{2n - 8} \right] \text{ or } \left[ 1 + \frac{\sqrt{2n^3 - 20n^2 + 64n - 64}}{2n - 8} \right] + 1.
\]

The following table gives the optimal choice of $r$ for various values of $n$. We also include the corresponding power of $p$ in (11).

<table>
<thead>
<tr>
<th>$n$</th>
<th>$r$</th>
<th>power of $p$</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>2</td>
<td>0.4749</td>
</tr>
<tr>
<td>10</td>
<td>3</td>
<td>0.4166</td>
</tr>
<tr>
<td>20</td>
<td>4</td>
<td>0.375</td>
</tr>
<tr>
<td>100</td>
<td>8</td>
<td>0.3125</td>
</tr>
<tr>
<td>1000</td>
<td>23</td>
<td>0.2714</td>
</tr>
<tr>
<td>1000000</td>
<td>708</td>
<td>0.2507</td>
</tr>
</tbody>
</table>

5. **Proof of Theorem 3**

It is conjectured that
\[
| \sum_{n \leq x} \chi(n) | \ll_{\epsilon} x^{\frac{1}{2}} p^{\epsilon},
\]
for any nonprincipal character $\chi \pmod{p}$. As Montgomery and Vaughan [3] have pointed out, the conjecture is known to be true under the assumption of the Grand Riemann Hypothesis. It is actually a consequence of the generalized Lindelöf hypothesis. Under the assumption of (12) we can substantially sharpen the result of Theorem 2, and prove Theorem 3 as follows.

In (10) we have shown
\[
|B \cap V| \geq \frac{B^n}{p-1} - \frac{1}{p-1} \sum_{\chi \neq \chi_0} \left( \prod_{i=1}^{n} \left| \sum_{x_i = a_i + 1}^{a_i + B} \chi(x_i) \right| \right).
\]

Also
\[
\frac{1}{p-1} \sum_{\chi \neq \chi_0} \left( \prod_{i=1}^{n} \left| \sum_{x_i = a_i + 1}^{a_i + B} \chi(x_i) \right| \right) \\
\leq \prod_{i=5}^{n} \left( \max_{\chi \neq \chi_0} \left| \sum_{x_i = a_i + 1}^{a_i + B} \chi(x_i) \right| \right) \cdot \frac{1}{p-1} \sum_{\chi \neq \chi_0} \left( \prod_{i=1}^{4} \left| \sum_{x_i = a_i + 1}^{a_i + B} \chi(x_i) \right| \right).\]
Inserting the upper bounds of (12) and (8) we obtain
\[
\frac{1}{p-1} \sum_{\chi \neq \chi_0} \left( \prod_{i=1}^{n} \sum_{x_i = a_i + 1}^{a_i + B} \chi(x_i) \right) \ll \epsilon \left( B^{\frac{2}{3}} p^2 \right)^{n-4} B^2 (\log p)^2 = B^{\frac{2}{3}} p^{(n-4)\epsilon} (\log p)^2.
\]
Thus by (10) we have
\[
|B \cap V| \geq \frac{B^n}{p - 1} - c(\epsilon) B^{\frac{2}{3}} p^{(n-4)\epsilon} (\log p)^2,
\]
where \( c(\epsilon) \) is a constant depending on \( \epsilon \). Therefore \( B \cap V \) is nonempty if
\[
B \gg \epsilon_p^{\frac{2}{3} + \frac{2(n-4)}{n}} (\log p)^{\frac{2}{3}}.
\]
It suffices to take
\[
B \gg \epsilon_p^{\frac{2}{3} + \epsilon}.
\]

References

1. A. Ayyad, T. Cochrane, and Z. Zheng, 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, J. of Number Theory 59 (2) (1996), 398–413. MR 97i:11091

Department of Mathematics, Kansas State University, Manhattan, Kansas 66506
Current address: Department of Mathematics, University of Gaza, P.O. Box 1418, Gaza Strip, Via Israel
E-mail address: anwar@math.ksu.edu