PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 127, Number 4, April 1999, Pages 943–950
S 0002-9939(99)05124-2

THE DISTRIBUTION OF SOLUTIONS OF THE CONGRUENCE $x_1x_2x_3\dots x_n \equiv c \pmod p$

ANWAR AYYAD

(Communicated by Dennis A. Hejhal)

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

$$x_1x_2x_3\dots x_n \equiv c \pmod p,$$

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

1. Introduction

We use multiplicative characters to study the congruence

$$x_1x_2x_3\dots x_n \equiv c \pmod p, \tag{1}$$

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 $\mathcal{B}$ the cube of size B defined by

$$\mathcal{B} = \{\mathbf{x}\in\mathbb{F}_p^n : a_i+1\leq x_i\leq a_i+B, 1\leq i\leq n\}, \tag{2}$$

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

$$\mathcal{B} = \{\mathbf{x}\in\mathbb{F}_p^n : a_i+1\leq x_i\leq a_i+B_i, 1\leq i\leq n\}, \tag{3}$$

then our interest is in finding how large the cardinality $|\mathcal{B}|$ of $\mathcal{B}$ must be to guarantee $\mathcal{B}\cap V$ is nonempty. For $n=2$ it is known for a cube of type (2) that $\mathcal{B}\cap V$ is nonempty if $B\gg p^{\frac{3}{4}}$. This follows from Weil's bound on the Kloosterman sum. R. A. Smith [4] conjectured that for a cube centered at the origin, $\mathcal{B}\cap V$ is nonempty if $B\gg p^{\frac{2}{3}}$. 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 B, then $\mathcal{B} \cap V$ is nonempty if $B \gg p^{\frac{2}{3}} (\log p)^{\frac{2}{3}}$.

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

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 B, and show that for any cube $\mathcal{B}$ of type (2), $\mathcal{B} \cap V$ is nonempty if $B \gg \sqrt{p \log p}$. 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*

$$B \gg p^{\frac{1}{4} + \frac{1}{\sqrt{2(n+4)}}} (\log p)^{\frac{3}{2}}.$$

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 $B \gg_\epsilon p^{\frac{2}{n} + \epsilon}$.*

2. Lemmas

For any prime p, we let $\sum_{\chi \neq \chi_o}$ denote a sum over all multiplicative characters $\chi \pmod p$ with $\chi \neq \chi_o$, the principal character.

Lemma 1.

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

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

Lemma 2.

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

Proof.

$$\begin{aligned}
\sum_{\chi \neq \chi_o} \Big| \sum_{x=a+1}^{a+B} \chi(x) \Big|^2 &= \sum_{\chi \neq \chi_o} \left(\sum_{x=a+1}^{a+B} \chi(x) \sum_{y=a+1}^{a+B} \overline{\chi(y)} \right) \\
&= \sum_{x,y=a+1}^{a+B} \left(\sum_{\chi \neq \chi_o} \chi(xy^{-1}) \right) \\
&\leq \sum_{\substack{x,y=a+1 \\ x=y}}^{a+B} \left(\sum_{\chi \neq \chi_o} \chi(xy^{-1}) \right) \\
&\leq (p-1)B.
\end{aligned}$$

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 χ,*

$$\Big|\sum_{x=a+1}^{a+B} \chi(x)\Big| \ll B^{1-\frac{1}{r}} p^{\frac{r+1}{4r^2}} (\log p)^{\frac{3}{2r}}. \tag{4}$$

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

$$\begin{aligned} &\frac{2x^2+n-4}{x(8x+4n-16)} < \frac{1}{\sqrt{2(n+4)}} \\ &\iff x^2 + \frac{2(n-4)x}{4-\sqrt{2(n+4)}} - \frac{(n-4)\sqrt{2(n+4)}}{2(4-\sqrt{2(n+4)})} < 0. \end{aligned} \tag{5}$$

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

$$\begin{aligned} b^2-4ac &= \frac{4(n-4)^2}{(4-\sqrt{2(n+4)})^2} - \frac{2(4-n)\sqrt{2(n+4)}}{4-\sqrt{2(n+4)}} \\ &= \frac{128-32n-8(4-n)\sqrt{2(n+4)}}{(4-\sqrt{2(n+4)})^2}. \end{aligned}$$

We also have

$$\begin{aligned} &128-32n-8(4-n)\sqrt{2(n+4)} > (4-\sqrt{2(n+4)})^2 \\ &\iff (8n-24)\sqrt{2(n+4)} > 34n-104. \end{aligned}$$

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

$$\begin{aligned}|\mathcal{B}\cap V| &= \sum_{\substack{\mathbf{x}\in\mathcal{B}\\ x_1x_2x_3=c}} 1 = \sum_{\substack{\mathbf{x}\in\mathcal{B}\\ x_1x_2x_3c^{-1}=1}} 1\\ &= \frac{1}{p-1}\sum_{\chi}\left(\sum_{\substack{x_i=a_i+1\\ i=1,2,3}}^{a_i+B_i}\chi(x_1x_2x_3c^{-1})\right) \qquad (6)\\ &= \frac{|\mathcal{B}|}{p-1}+\frac{1}{p-1}\sum_{\chi\neq\chi_o}\chi(c^{-1})\sum_{\substack{x_i=a_i+1\\ i=1,2,3}}^{a_i+B_i}\chi(x_1)\chi(x_2)\chi(x_3).\end{aligned}$$

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

$$\begin{aligned}&|\sum_{\chi\neq\chi_o}\chi(c^{-1})\sum_{\substack{x_i=a_i+1\\ i=1,2,3}}^{a_i+B_i}\chi(x_1)\chi(x_2)\chi(x_3)|\\ &\le \sum_{\chi\neq\chi_o}\left(|\sum_{x_1=a_1+1}^{a_1+B_1}\chi(x_1)||\sum_{x_2=a_2+1}^{a_2+B_2}\chi(x_2)\cdot\sum_{x_3=a_3+1}^{a_3+B_3}\chi(x_3)|\right)\\ &\le \left(\sum_{\chi\neq\chi_o}|\sum_{x_1=a_1+1}^{a_1+B_1}\chi(x_1)|^2\right)^{\frac12}\left(\sum_{\chi\neq\chi_o}|\sum_{x_2=a_2+1}^{a_2+B_2}\chi(x_2)|^2\cdot|\sum_{x_3=a_3+1}^{a_3+B_3}\chi(x_3)|^2\right)^{\frac12}\\ &\le \left(\sum_{\chi\neq\chi_o}|\sum_{x_1=a_1+1}^{a_1+B_1}\chi(x_1)|^2\right)^{\frac12}\cdot\prod_{i=2}^{3}\left(\sum_{\chi\neq\chi_o}|\sum_{x_i=a_i+1}^{a_i+B_i}\chi(x_i)|^4\right)^{\frac14}.\end{aligned}$$

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

$$\begin{aligned}|\text{error}| &\ll \frac{1}{p-1}\sqrt{(p-1)B_1}\cdot\prod_{i=2}^{3}((p-1)B_i^2\log^2 p)^{\frac14}\\ &\ll |\mathcal{B}|^{\frac12}\log p.\end{aligned}$$

Thus

$$|\mathcal{B}\cap V| = \frac{|\mathcal{B}|^3}{p-1}+O\left(|\mathcal{B}|^{\frac12}\log p\right).$$

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

$$\frac{|\mathcal{B}|^3}{p-1}\gg|\mathcal{B}|^{\frac12}\log p,$$

that is,

$$|\mathcal{B}|\gg p^2\log^2 p.$$

When $n = 4$, we proceed in a similar manner to obtain

$$|\mathcal{B} \cap V| = \frac{|\mathcal{B}|}{p-1} + \frac{1}{p-1} \sum_{\chi \neq \chi_o} \chi(c^{-1}) \sum_{\substack{x_i = a_i+1 \\ i=1,2,3,4}}^{a_i+B_i} \chi(x_1)\chi(x_2)\chi(x_3)\chi(x_4). \tag{7}$$

Using the Cauchy-Schwarz inequality we obtain

$$\begin{aligned}
&|\sum_{\chi \neq \chi_o} \chi(c^{-1}) \sum_{\substack{x_i = a_i+1 \\ i=1,2,3,4}}^{a_i+B_i} \chi(x_1)\chi(x_2)\chi(x_3)\chi(x_4)| \\
&\leq \sum_{\chi \neq \chi_o} \left(|\sum_{x_1=a_1+1}^{a_1+B_1} \chi(x_1) \sum_{x_2=a_2+1}^{a_2+B_2} \chi(x_2)| \cdot |\sum_{x_3=a_3+1}^{a_3+B_3} \chi(x_3) \sum_{x_4=a_4+1}^{a_4+B_4} \chi(x_4)| \right) \\
&\leq \left(\sum_{\chi \neq \chi_o} |\prod_{i=1}^{2} \sum_{x_i=a_i+1}^{a_i+B_i} \chi(x_i)|^2 \right)^{\frac{1}{2}} \left(\sum_{\chi \neq \chi_o} |\prod_{i=3}^{4} \sum_{x_i=a_i+1}^{a_i+B_i} \chi(x_i)|^2 \right)^{\frac{1}{2}} \\
&\leq \prod_{i=1}^{4} \left(\sum_{\chi \neq \chi_o} |\sum_{x_i=a_i+1}^{a_i+B_i} \chi(x_i)|^4 \right)^{\frac{1}{4}}.
\end{aligned}$$

Now by Lemma 2 we obtain the following bound on the error term in (7):

$$\begin{aligned}
|\text{error}| &\ll \frac{1}{p-1} \prod_{i=1}^{4} (pB_i^2 \log^2 p)^{\frac{1}{4}} \\
&\ll \sqrt{B_1B_2B_3B_4} \log^2 p = |\mathcal{B}|^{\frac{1}{2}} \log^2 p.
\end{aligned} \tag{8}$$

Therefore we obtain

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

Thus for $\mathcal{B} \cap V$ not to be empty it suffices that

$$\frac{|\mathcal{B}|}{p-1} \gg |\mathcal{B}|^{\frac{1}{2}} \log^2 p,$$

that is,

$$|\mathcal{B}| \gg p^2 \log^4 p.$$

4. Proof of Theorem 2

For any cube $\mathcal{B}$ of size B we have

$$|\mathcal{B} \cap V| = \frac{B^n}{p-1} + \frac{1}{p-1} \sum_{\chi \neq \chi_o} \chi(c^{-1}) \sum_{\substack{x_i = a_i+1 \\ i=1,2,\dots,n}}^{a_i+B} \chi(x_1)\chi(x_2)\dots\chi(x_n). \tag{9}$$

The error term in (9) is bounded above by

$$\frac{1}{p-1} \sum_{\chi \neq \chi_o} \left(\prod_{i=1}^{n} |\sum_{x_i=a_i+1}^{a_i+B} \chi(x_i)| \right).$$

Thus

$$|\mathcal{B}\cap V| \geq \frac{B^n}{p-1} - \frac{1}{p-1}\sum_{\chi\neq\chi_o}\left(\prod_{i=1}^{n}|\sum_{x_i=a_i+1}^{a_i+B}\chi(x_i)|\right). \tag{10}$$

The term

$$\frac{1}{p-1}\sum_{\chi\neq\chi_o}\left(\prod_{i=1}^{n}|\sum_{x_i=a_i+1}^{a_i+B}\chi(x_i)|\right)$$

in (10) may be bounded as follows:

$$\begin{aligned}&\frac{1}{p-1}\sum_{\chi\neq\chi_o}\left(\prod_{i=1}^{n}|\sum_{x_i=a_i+1}^{a_i+B}\chi(x_i)|^n\right)\\ &\leq \prod_{i=5}^{n}\left(\max_{\chi\neq\chi_o}|\sum_{x_i=a_i+1}^{a_i+B}\chi(x_i)|\right)\cdot\frac{1}{p-1}\sum_{\chi\neq\chi_o}\left(\prod_{i=1}^{4}|\sum_{x_i=a_i+1}^{a_i+B}\chi(x_i)|\right).\end{aligned}$$

Inserting the upper bound of Burgess, Lemma 3, and the upper bound in (8) we obtain

$$\begin{aligned}\frac{1}{p-1}\sum_{\chi\neq\chi_o}\left(\prod_{i=1}^{n}|\sum_{x_i=a_i+1}^{a_i+B}\chi(x)|\right) &\ll \left(B^{1-\frac{1}{r}}p^{\frac{r+1}{4r^2}}(\log p)^{\frac{3}{2r}}\right)^{n-4}B^2\log^2 p\\ &= B^{2+\frac{nr-4r-n+4}{r}}p^{\frac{nr+n-4r-4}{4r^2}}(\log p)^{\frac{4r+3n-12}{2r}}.\end{aligned}$$

Therefore

$$|\mathcal{B}\cap V| = \frac{B^n}{p-1} + O\left(B^{2+\frac{nr-4r-n+4}{r}}p^{\frac{nr+n-4r-4}{4r^2}}(\log p)^{\frac{4r+3n-12}{2r}}\right).$$

Thus $\mathcal{B}\cap V$ is nonempty if

$$\frac{B^n}{p-1} \gg B^{2+\frac{nr-4r-n+4}{r}}p^{\frac{nr+n-4r-4}{4r^2}}(\log p)^{\frac{4r+3n-12}{2r}},$$

that is,

$$B \gg p^{\frac{4r^2+nr+n-4r-4}{8r^2+4rn-16r}}(\log p)^{\frac{4r+3n-12}{4r+2n-8}}. \tag{11}$$

Now the power of p in (11) is

$$\frac{4r^2+rn+n-4r-4}{8r^2+4rn-16r} = \frac{1}{4} + \frac{2r^2+n-4}{r(8r+4n-16)}.$$

By Lemma 4 for any integer $n\geq 5$ there exists an integer $r\geq 2$ such that

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

For such choice of r the power of p in (11) satisfies

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

Since the power of $\log p$ in (11) satisfies

$$\frac{4r+3n-12}{4r+2n-8} < \frac{3}{2},$$

we have that $\mathcal{B}\cap V$ is nonempty if

$$B \gg p^{\frac{1}{4}+\frac{1}{\sqrt{2(n+4)}}}(\log p)^{\frac{3}{2}}.$$

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 $n\ge 5$ 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).

n	r	power of p
5	2	0.4749
10	3	0.4166
20	4	0.375
100	8	0.3125
1000	23	0.2714
1000000	708	0.2507

5. Proof of Theorem 3

It is conjectured that

$$|\sum_{n\le x}\chi(n)| \ll_\epsilon x^{\frac{1}{2}}p^\epsilon, \tag{12}$$

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

$$|\mathcal{B}\cap V| \ge \frac{B^n}{p-1}-\frac{1}{p-1}\sum_{\chi\ne\chi_o}\left(\prod_{i=1}^{n}|\sum_{x_i=a_i+1}^{a_i+B}\chi(x_i)|\right).$$

Also

$$\frac{1}{p-1}\sum_{\chi\ne\chi_o}\left(\prod_{i=1}^{n}|\sum_{x_i=a_i+1}^{a_i+B}\chi(x_i)|\right)$$
$$\le \prod_{i=5}^{n}\left(\max_{\chi\ne\chi_o}|\sum_{x_i=a_i+1}^{a_i+B}\chi(x_i)|\right)\cdot\frac{1}{p-1}\sum_{\chi\ne\chi_o}\left(\prod_{i=1}^{4}|\sum_{x_i=a_i+1}^{a_i+B}\chi(x_i)|\right).$$

Inserting the upper bounds of (12) and (8) we obtain

$$\frac{1}{p-1}\sum_{\chi\neq\chi_o}\left(\prod_{i=1}^{n}|\sum_{x_i=a_i+1}^{a_i+B}\chi(x_i)|\right)\ll_\epsilon \left(B^{\frac{1}{2}}p^{\epsilon}\right)^{n-4}B^2(\log p)^2$$
$$= B^{\frac{n}{2}}p^{(n-4)\epsilon}(\log p)^2.$$

Thus by (10) we have

$$|\mathcal{B}\cap V|\geq \frac{B^n}{p-1}-c(\epsilon)B^{\frac{n}{2}}p^{(n-4)\epsilon}(\log p)^2,$$

where $c(\epsilon)$ is a constant depending on ϵ. Therefore $\mathcal{B}\cap V$ is nonempty if

$$B\gg_\epsilon p^{\frac{2}{n}+\frac{2\epsilon(n-4)}{n}}(\log p)^{\frac{4}{n}}.$$

It suffices to take

$$B\gg_\epsilon p^{\frac{2}{n}+\epsilon}.$$

References

1. A. Ayyad, T. Cochrane, and Z. 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. of Number Theory **59** (2) (1996), 398–413. MR **97i:**11091
2. D.A. Burgess, *On character sums and primitive roots*, Proc. London Math. Soc.(3) **12** (1962), 179–192. MR **24:**A2569
3. H.L. Montgomery and R.C. Vaughan, *Exponential sums with multiplicative coefficients*, Invent. Math. **43** (1977), 69–82. MR **56:**15579
4. R.A. Smith, *The distribution of rational points on a curve modulo q*, Rocky Mountain J. of Math. **15** (2) (1985), 589–597. MR **87h:**11055

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