# SMALL SOLUTIONS OF $ax_1 \cdots x_k + bx_{k+1} \cdots x_{2k} \equiv c \pmod m$ UNDER THE LINDELÖF HYPOTHESIS

**Todd Cochrane**
*Department of Mathematics, Kansas State University, Manhattan, Kansas*
cochrane@math.ksu.edu

**Sanying Shi**
*School of Mathematics, Hefei University of Technology, Hefei, P.R. China*
vera123_99@hotmail.com

*Received: 3/23/21, Accepted: 9/22/21, Published: 10/8/21*

**Abstract**

For $k, m \in \mathbb{N}$, and integers $a, b, c$ with $(ab, m) = 1$, we prove under the assumption of the Lindelöf Hypothesis that the congruence

$$ax_1x_2 \cdots x_k + bx_{k+1}x_{k+2} \cdots x_{2k} \equiv c \pmod m,$$

has a solution in positive integers $x_i$ with

$$1 \le x_i \ll_{\varepsilon,k} m^{\frac{1}{k}+\varepsilon}.$$

The estimate is best possible aside from the possible removal of the $\varepsilon$. For $k = 1$ we obtain, unconditionally, a solution $x, y$ of integers coprime to $m$ in any interval of length $\frac{m}{1+\kappa}(1 + o(m))$, with $\kappa = \prod_{p|m, p\nmid c} \frac{p-2}{p-1}$.

## 1. Introduction

For $k, m \in \mathbb{N}$, and integers $a, b, c$ with $(ab, m) = 1$ we seek small solutions to the congruence

$$ax_1x_2 \cdots x_k + bx_{k+1}x_{k+2} \cdots x_{2k} \equiv c \pmod m. \tag{1}$$

It was proven in [2] that for prime moduli $m = p$ with $p \nmid c$, there is a solution of (1) with

$$1 \le x_i \ll_{\varepsilon} p^{\frac{3}{2k}+\varepsilon}.$$

For general moduli, let $r = \omega(m)$, the number of distinct prime factors of $m$ and $E$ denote the maximum multiplicity of any prime factor of $m$. The authors established [6] that for $c$ relatively prime to $m$, (1) has a solution with $1 \le x_i \le m^{2/k}$, for

$m \geq C(k, E, r)$, a constant depending on $k, E$ and $r$, and conjectured that this could be improved to

$$1 \leq x_i \ll_{\varepsilon,k} m^{\frac{1}{k}+\varepsilon}, \tag{2}$$

uniformly in $E$ and $r$. This estimate is best possible up to the possible removal of the $\varepsilon$ in the exponent; consider for example the case where $a = b = 1$ and $\frac{m}{2} < c \leq m$. Here we prove the conjecture under the assumption of the generalized Lindelöf Hypothesis:

$$L\left(\tfrac{1}{2} + it, \chi\right) \ll_{\varepsilon} \left((1 + |t|)m\right)^{\varepsilon},$$

uniformly for all Dirichlet characters $\chi$ of conductor $m$. It is well known that the generalized Riemann Hypothesis implies the generalized Lindelöf Hypothesis.

**Theorem 1.** *Under the assumption of the generalized Lindelöf Hypothesis, for any positive integer $k$, integers $a, b, c$ with $(ab, m) = 1$ and any $\varepsilon > 0$, there is a solution of (1) satisfying (2). For odd $m$, or even $m$ and even $c$, such a solution exists with $(x_i, m) = 1$, $1 \leq i \leq 2k$, while for $m$ even and $c$ odd, such a solution exists with $(x_1, m) = 2$, $(x_i, m) = 1$, $2 \leq i \leq 2k$.*

**Remark 1.** i) We note that when $m$ is even and $c$ is odd, there is no solution to (1) at all with all $(x_i, m) = 1$. Thus the parity conditions in the theorem are necessary.

ii) Whereas the earlier works on this problem [5], [3] required $c$ to be coprime to $m$, Theorem 1 allows for arbitrary $c$.

The theorem was proven in [2] for the case of prime moduli $m = p$. The strategy was to show that the set of products $\{x_1 \cdots x_k \pmod p : 1 \leq x_i \leq B\}$ has cardinality exceeding $p/2$ for $B \gg p^{\frac{1}{k}+\varepsilon}$. Thus, by a simple application of the box principle, the sum of two such sets hits every residue class mod $p$. For a general modulus the problem is more subtle since the set of products with the $(x_i, m) = 1$ has cardinality at most $\phi(m)$ which in general is less than $m/2$.

When $k = 1$, Theorem 1 is trivial. In this case (1) is just a linear congruence

$$ax + by \equiv c \pmod m, \tag{3}$$

with $(ab, m) = 1$. If $x, y$ are restricted to values coprime to $m$, then plainly there is no solution if $m$ is even and $c$ is odd. Otherwise, there exist such solutions $(x, y)$, and the total number is readily seen to be

$$\phi(m) \prod_{p|m, p\nmid c} \frac{p-2}{p-1},$$

by counting solutions modulo prime powers. It is an interesting question whether one can obtain such a solution with the variables restricted to an interval $1 \leq x, y < B$, for some value $B$ less than $m$. Plainly, one will need at least $B > m/2$ to have any hope of a solution for a general value $c$ (consider eg. $x + y \equiv -1 \bmod m$). Here we obtain a nontrivial result holding for $x, y$ belonging to an interval in arbitrary position.

**Theorem 2.** *Suppose that $m$ is odd or that $m$ is even and $c$ is even. In any interval $I = [A+1, A+B]$ of integers of length $B$ there exist integers $x, y$ coprime to $m$ satisfying* (3)*, provided that*

$$B \geq \frac{m}{1+\kappa} + O_\varepsilon\left(m^{\frac{1}{2}+\varepsilon}\right).$$

*where*

$$\kappa := \prod_{p|m, p\nmid c} \frac{p-2}{p-1}. \tag{4}$$

*Here, $\kappa := 1$ if the product over $p$ is empty.*

For example if $m = p^e$, a prime power, then $\kappa = 1$ if $p|c$, $\kappa = \frac{p-2}{p-1}$ if $p \nmid c$. The estimate in the theorem is best possible ($B \gtrsim \frac{m}{2}$), whenever $\kappa \approx 1$. The theorem is presented in a more explicit form in Section 4; see (16).

For $k = 2$ it was shown [1, Theorem 3] that there is a solution of the congruence,

$$x_1x_2 + x_3x_4 \equiv c \pmod{m}$$

in any cube of edge length $B \geq 2\sqrt{m} + 1$ for prime power $m$, $B \gg m^{\frac{1}{2}} \log^2 m$, for general $m$. We conjecture that a result of the same strength is available for the general congruence

$$ax_1x_2 + bx_3x_4 \equiv c \pmod{m}, \tag{5}$$

with $(ab, m) = 1$. This was established for prime moduli by Garaev and Garcia [9, Theorem 4], who proved the existence of a solution of (5) for $m = p$ in any cube of edge length $4\sqrt{p}$.

For $k = 3$, using the Burgess character sum estimate, Garaev [8, Theorem 1] showed that the set

$$S_3 := \{x_1x_2x_3 \pmod{m} : 1 \leq x_i \leq m^{\frac{1}{3}+\varepsilon}\}$$

has cardinality $|S_3| = m + O(m^{1-\delta})$, for some $\delta = \delta(\varepsilon)$. Thus, for $m$ sufficiently large and any integers $a, b, c$, with $(ab, m) = 1$, the sets $aS_3$ and $c - bS_3$ each have cardinality exceeding $m/2$, implying a solution of (1) with $1 \leq x_i \leq m^{\frac{1}{3}+\varepsilon}$, but without the constraint $(x_i, m) = 1$ given in Theorem 1. For $k = 4$, [8, Theorem 2] yields an analogous result with $1 \leq x_i \leq m^{\frac{1}{4}+\varepsilon}$ for cube-free moduli.

**Remark 2.** Regarding the modular hyperbola

$$x_1x_2 \cdots x_k \equiv c \pmod{m}, \tag{6}$$

with $(c, m) = 1$, we conjecture that there is always a solution with (2) holding, but even with the assumption of the Lindelöf Hypothesis we have been unable to obtain this. What we do show, Lemma 2, is that the number of reduced residues $c$ represented as in (6) with $1 \leq x_i \leq m^{\frac{1}{k}+\varepsilon}$, is

$$\phi(m) + O_\varepsilon\left(m^{1-k\varepsilon/2}\right).$$

## 2. Lemmas

Let $B$ be a positive integer with $1 \le B \le m$ and $B'$ denote the number of integers $x \in [1, B]$ with $(x, m) = 1$. By [3, Lemma 3.3], and the estimate of Robin [14] for $\omega(m)$,

$$B' = \frac{\phi(m)}{m} B + \theta 2^{\omega(m)} = \frac{\phi(m)}{m} B + \theta' m^{.96/\log\log m}, \tag{7}$$

for some $\theta, \theta'$ with $|\theta|, |\theta'| < 1$. For a given $\varepsilon > 0$ we may assume $B > m^{\varepsilon}$ (else the results of this section are trivial) and so (7) gives in particular

$$B' \gg_{\varepsilon} \frac{B}{\log\log m}. \tag{8}$$

Indeed, by the work of Iwaniec [10], the lower bound (8) holds for $B \gg (\log m)^2$.

Let $N$ denote the number of solutions of

$$x_1 \cdots x_k \equiv y_1 \cdots y_k \pmod{m}, \tag{9}$$

with $1 \le x_i, y_i \le B$, $(x_i, m) = (y_i, m) = 1$, $1 \le i \le k$, and for any divisor $d$ of $m$ and integer $\lambda$ coprime to $d$, let $N(\lambda, d)$ denote the number of those solutions satisfying the additional constraint

$$x_1 \cdots x_k \equiv \lambda \pmod{d}. \tag{10}$$

Finally, let $H(\lambda, d)$ denote the number of solutions of (10) alone with $1 \le x_i \le B$, $(x_i, m) = 1$, $1 \le i \le k$.

**Lemma 1.** *Under the assumption of the Lindelöf Hypothesis, for any $d|m$ and integer $\lambda$ with $(\lambda, d) = 1$, we have*

*i)* $$N(\lambda, d) = \frac{B'^{2k}}{\phi(m)\phi(d)} \left(1 + O_{\varepsilon}\left(\frac{\phi(d) m^{k\varepsilon}}{B^{k/2}} + \frac{m^{1+k\varepsilon}\phi(d)}{B^k}\right)\right).$$

*ii)* $$N = \frac{B'^{2k}}{\phi(m)} \left(1 + O_{\varepsilon}\left(\frac{m^{1+k\varepsilon}}{B^k}\right)\right).$$

*iii)* $$H(\lambda, d) = \frac{B'^{k}}{\phi(d)} + O_{\varepsilon}\left(B^{k/2} m^{k\varepsilon}\right).$$

*Proof.* It follows from the Lindelöf Hypothesis that

$$\sum_{x=1}^{B} \chi(x) \ll_{\varepsilon} B^{\frac{1}{2}} m^{\varepsilon}, \tag{11}$$

uniformly for all non-principal Dirichlet characters $\chi$ mod $m$, as noted for example in [12, (13.2)], [13, p. 71], or [11, (5.61)].

Let $\lambda^{-1}$ denote the inverse of $\lambda$ mod $d$, $y_i^{-1}$ the inverse of $y_i$ mod $m$, and $\chi_0$ the principal character mod $m$. Letting $\chi$ run through the mod $m$ characters and $\psi$ run through the mod $m$ characters induced by a mod $d$ character, and writing $\sum_{x_i=1}^{B}, \sum_{y_i=1}^{B}$ for the multiple sums over $x_1, \dots, x_k$, $y_1, \dots, y_k$ respectively with the $x_i, y_i$ coprime to $m$, we have

$$\begin{aligned}\phi(m)\phi(d)N(\lambda,d) &= \sum_{x_i=1}^{B}\sum_{y_i=1}^{B}\sum_{\chi}\chi(x_1\cdots x_k y_1^{-1}\cdots y_k^{-1})\sum_{\psi}\psi(\lambda^{-1}x_1\cdots x_k)\\ &= \sum_{\psi}\sum_{\chi}\psi^{-1}(\lambda)\sum_{x_i=1}^{B}\chi\psi(x_i)\sum_{y_i=1}^{B}\chi^{-1}(y_i)\\ &= B'^{2k}+E_1+E_2+E_3,\end{aligned}$$

where, using (11),

$$E_1 := \sum_{\psi\neq\chi_0}\sum_{\chi=\chi_0}\psi^{-1}(\lambda)\sum_{x_i=1}^{B}\chi\psi(x_i)\sum_{y_i=1}^{B}\chi^{-1}(y_i) = O_\varepsilon\left(\phi(d)B'^kB^{k/2}m^{k\varepsilon}\right),$$

$$E_2 := \sum_{\psi\neq\chi_0}\sum_{\chi=\psi^{-1}}\sum_{x_i=1}^{B}\chi\psi(x_i)\sum_{y_i=1}^{B}\chi^{-1}(y_i) = O_\varepsilon\left(\phi(d)B'^kB^{k/2}m^{k\varepsilon}\right),$$

$$E_3 := \sum_{\psi}\sum_{\substack{\chi\neq\chi_0\\ \chi\neq\psi^{-1}}}\sum_{x_i=1}^{B}\chi\psi(x_i)\sum_{y_i=1}^{B}\chi^{-1}(y_i) = O_\varepsilon\left(\phi(d)\phi(m)B^km^{k\varepsilon}\right).$$

Thus

$$\begin{aligned}N(\lambda,d) &= \frac{B'^{2k}}{\phi(m)\phi(d)}+O_\varepsilon\left(\frac{B^{3k/2}m^{k\varepsilon}}{\phi(m)}+B^km^{k\varepsilon}\right)\\ &= \frac{B'^{2k}}{\phi(m)\phi(d)}\left(1+O_\varepsilon\left(\frac{\phi(d)m^{k\varepsilon}}{B^{k/2}}+\frac{m^{1+k\varepsilon}\phi(d)}{B^k}\right)\right),\end{aligned}$$

using (8).

For part (ii) we simply apply part (i) with $d = 1$ and note that in this case $E_1 = E_2 = 0$.

For part (iii), letting $\psi$ again run through the mod $m$ characters induced by a mod $d$ character, and using (11), we have

$$\begin{aligned}\phi(d)H(\lambda,d) &= \sum_{x_i=1}^{B}\sum_{\psi}\psi(\lambda^{-1}x_1\cdots x_k) = B'^k+\sum_{\psi\neq\chi_0}\psi(\lambda^{-1})\sum_{x_i=1}^{B}\psi(x_i)\\ &= B'^k+O_\varepsilon\left(\phi(d)B^{k/2}m^{k\varepsilon}\right),\end{aligned}$$

completing the proof. □

Let

$$S := \{x_1 \cdots x_k \pmod m : 1 \le x_i \le B, (x_i, m) = 1, 1 \le i \le k\}, \tag{12}$$

and for any $d|m$ and integer $\lambda$ with $(\lambda, d) = 1$, let

$$S(\lambda, d) := \{s \in S : s \equiv \lambda \pmod d\}.$$

Using the estimates for $N$, $N(\lambda, d)$, $S(\lambda, d)$ in Lemma 1, the lower bound for $B'$ in (8) and the inequalities

$$|S| \ge \frac{B'^{2k}}{N}, \qquad |S(\lambda, d)| \ge \frac{H(\lambda, d)^2}{N(\lambda, d)},$$

we deduce the following.

**Lemma 2.** *For $d|m$ and integer $\lambda$ with $(\lambda, d) = 1$ we have*

$$i) \quad |S(\lambda, d)| \ge \frac{\phi(m)}{\phi(d)} - O_\varepsilon\left(\frac{m^{1+k\varepsilon}}{B^{k/2}} + \frac{m^{2+k\varepsilon}}{B^k}\right).$$

$$ii) \quad |S| \ge \phi(m)\left(1 - O_\varepsilon\left(\frac{m^{1+k\varepsilon}}{B^k}\right)\right).$$

An upper bound on $S(\lambda, d)$ is obtained from the lemma as follows.

$$\begin{aligned} |S(\lambda, d)| &= |S| - \sum_{\substack{y=1 \\ (y,d)=1, y \not\equiv \lambda \pmod d}}^{d} |S(y, d)| \\ &\le \phi(m) - (\phi(d) - 1)\frac{\phi(m)}{\phi(d)} + O_\varepsilon\left(\frac{dm^{1+k\varepsilon}}{B^{k/2}} + \frac{m^{2+k\varepsilon}d}{B^k}\right) \\ &= \frac{\phi(m)}{\phi(d)} + O_\varepsilon\left(\frac{dm^{1+k\varepsilon}}{B^{k/2}} + \frac{m^{2+k\varepsilon}d}{B^k}\right). \end{aligned}$$

Combining the lower bound of the lemma with this upper bound we obtain

**Lemma 3.** *Suppose that $\varepsilon < \frac{1}{2k}$ and that $B > m^{\frac{1}{k}+2\varepsilon}$. Then for any $d|m$ and integer $\lambda$ with $(\lambda, d) = 1$ we have*

$$|S(\lambda, d)| = \frac{\phi(m)}{\phi(d)} + O_\varepsilon\left(dm^{1-k\varepsilon}\right).$$

## 3. Proof of Theorem 1

Let $a, b, c$ be integers with $(ab, m) = 1$, $S$ be the set of products as in (12) and $\varepsilon$ be a given positive real. We may assume $\varepsilon < \frac{1}{2k}$. The strategy to solve (1) is to show that the sets $c - aS$ and $bS$ have a nonempty intersection. Let

$$T := (c - aS) \cap \mathbb{Z}_m^* = \{c - as : s \in S, (c - as, m) = 1\}. \tag{13}$$

Since $T$ and $bS$ are both subsets of $\mathbb{Z}_m^*$ we are done if we can show that $|T|+|bS| > \phi(m)$. Now

$$\begin{aligned}|T| &= \sum_{\substack{s\in S\\(c-as,m)=1}} 1 = \sum_{s\in S}\sum_{d|(c-as,m)}\mu(d)\\ &= \sum_{d|m}\mu(d)\sum_{\substack{s\in S\\ d|c-as}} 1 = \sum_{\substack{d|m\\(d,c)=1}}\mu(d)|S(a^{-1}c,d)|,\end{aligned}$$

where $a^{-1}$ is the inverse of $a$ mod $d$, noting that if $(d,c)>1$ the sum $\sum_{s\in S, d|c-as} 1$ is empty. Using the estimate in Lemma 3 for $d < m^{\varepsilon/2}$ and the trivial estimate $|S(a^{-1}c,d)| \le m/d$ for $d \ge m^{\varepsilon/2}$, we get for $B > m^{\frac{1}{k}+2\varepsilon}$,

$$\begin{aligned}|T| &= \sum_{\substack{d|m,(d,c)=1\\ d<m^{\frac{\varepsilon}{2}}}}\mu(d)\left(\frac{\phi(m)}{\phi(d)} + O_\varepsilon\left(dm^{1-k\varepsilon}\right)\right) + O_\varepsilon\left(\sum_{\substack{d|m\\ d>m^{\frac{\varepsilon}{2}}}} m/d\right)\\ &= \sum_{\substack{d|m,(d,c)=1\\ d<m^{\frac{\varepsilon}{2}}}}\mu(d)\frac{\phi(m)}{\phi(d)} + O_\varepsilon\left(m^{1-k\varepsilon}m^{\varepsilon/2}\tau(m) + m^{1-\varepsilon/2}\tau(m)\right)\\ &= \phi(m)\sum_{\substack{d|m\\(d,c)=1}}\frac{\mu(d)}{\phi(d)} + O_\varepsilon\left(m^{1-\frac{\varepsilon}{3}}\right)\\ &= \phi(m)\prod_{\substack{p|m\\ p\nmid c}}\left(1-\frac{1}{p-1}\right) + O_\varepsilon(m^{1-\frac{\varepsilon}{3}}).\end{aligned}$$

Now, for $B > m^{\frac{1}{k}+2\varepsilon}$, we get from Lemma 3 (with $d=1$),

$$|bS| = \phi(m) + O_\varepsilon\left(m^{1-k\varepsilon}\right),$$

and so

$$|bS|+|T| \ge \phi(m) - O_\varepsilon\left(m^{1-k\varepsilon}\right) + \phi(m)\prod_{\substack{p|m\\ p\nmid c}}\left(1-\frac{1}{p-1}\right) - O_\varepsilon(m^{1-\varepsilon/3}). \quad (14)$$

If $m$ is odd, or $m$ is even and $c$ is even, then

$$\prod_{\substack{p|m\\ p\nmid c}}\left(1-\frac{1}{p-1}\right) > \prod_{p|m}\left(1-\frac{1}{p}\right)^2 = (\phi(m)/m)^2$$

and so

$$\phi(m)\prod_{\substack{p|m\\ p\nmid c}}\left(1-\frac{1}{p-1}\right) > \frac{\phi(m)^3}{m^2} > \frac{m}{27(\log\log m)^3}$$

for $m > 30$ (using the estimate for $\phi(m)$ in [15]). Thus for $m$ sufficiently large this term dominates the error terms in (14), and we see that for $m > C(\varepsilon, k)$, $|bS| + |T| > \phi(m)$ as desired.

If $m$ is even and $c$ is odd, the product over $p$ in (14) is zero and thus we fail to obtain a solution of (1) (as was already noted in the introduction.) In this case we replace $x_1$ with $2x_1'$ and allow $x_1'$ to run through a set of reduced residues mod $m$. This time we set $T = (c - 2aS) \cap \mathbb{Z}_m^*$, let $(2a)^{-1}$ denote the inverse of $2a$ mod $d$, and obtain as above that

$$\begin{aligned} |T| &= \sum_{d|m} \mu(d) \sum_{\substack{s \in S \\ d|(c-2as)}} 1 = \sum_{\substack{d|m \\ (d,2c)=1}} \mu(d)|S((2a)^{-1}c, d)| \\ &= \phi(m) \prod_{\substack{p|m \\ p\nmid 2c}} \left(1 - \frac{1}{p-1}\right) + O(m^{1-\frac{\varepsilon}{3}}). \end{aligned}$$

Thus for $m$ sufficiently large we again conclude that $|T| + |bS| > \phi(m)$.

## 4. Proof of Theorem 2

We start with the Polya-Vinogradov estimate for character sums, stated for arbitrary characters.

**Lemma 4.** *There is an absolute constant $c_o$ such that for any mod $m$ character $\chi$ of conductor $d > 1$, and any positive integer $B$,*

$$\left| \sum_{x=1}^{B} \chi(x) \right| \leq c_o \sqrt{d}\, \tau^*(m/d) \log d,$$

*where $\tau^*(m/d)$ denotes the number of square-free divisors of $m/d$.*

By the work of Frolenkov and Soundararajan [7], we can take $c_o = .21$ for $q > 1200$. Further improvements in $c_o$ are available for odd characters and for larger $q$ using estimates in [7] or the results of Bordignon and Kerr [4].

*Proof.* The lemma is a well known consequence of the Polya-Vinogradov bound

$$\left| \sum_{x=1}^{B} \chi(x) \right| \leq c_o \sqrt{m}\, \log m, \tag{15}$$

for primitive characters. Suppose $\chi$ is a mod $m$ character induced by a primitive mod $d$ character $\chi_d$ with $d > 1$. Then

$$\sum_{x=1}^{B} \chi(x) = \sum_{x=1}^{B} \chi_d(x) \left( \sum_{e|(x,m)} \mu(e) \right) = \sum_{e|m} \mu(e) \sum_{x=1, e|x}^{B} \chi_d(x).$$

If $(e,d)>1$ the sum over $x$ is zero. Thus,

$$\sum_{x=1}^{B}\chi(x)=\sum_{\substack{e\mid m\\(e,d)=1}}\mu(e)\chi_d(e)\sum_{1\le y\le B/e}\chi_d(y).$$

Inserting the estimate (15) for the sum over $y$, and letting $\sum^*$ denote a sum over square-free divisors, we obtain

$$\left|\sum_{x=1}^{B}\chi(x)\right|\le\sum_{e\mid(m/d)}^{*}c_o\sqrt{d}\,\log d,$$

the upper bound of the lemma. □

We proceed to solve the linear congruence $ax+by\equiv c \bmod m$ with $x,y\in[1,B]$. At the end of the proof, we comment on generalizing it to a displaced interval $[A+1,A+B]$. Let

$$S:=\{x\in\mathbb{Z}:1\le x\le B,(x,m)=1\}.$$

Once again our goal is to show $|T|+|bS|>\phi(m)$, where $T$ is the set in (13). Letting $S(\lambda,d)$ denote the set of $x\in[1,B]$ coprime to $m$ with $x\equiv\lambda \bmod d$, we have (letting $\psi$ again run through the mod $m$ characters induced by a mod $d$ character),

$$\begin{aligned}|S(\lambda,d)|&=\frac{1}{\phi(d)}\sum_{\substack{x=1\\(x,m)=1}}^{B}\sum_{\psi}\psi(\lambda^{-1}x)\\&=\frac{1}{\phi(d)}B'+\frac{1}{\phi(d)}\sum_{\psi\neq\chi_0}\psi(\lambda^{-1})\sum_{x=1}^{B}\psi(x)=\frac{1}{\phi(d)}B'+E(\lambda,d),\end{aligned}$$

say where setting $e$ equal to the conductor of $\psi$, and using Lemma 4,

$$\begin{aligned}|E(\lambda,d)|&\le\frac{1}{\phi(d)}\sum_{e\mid d}c_o\phi(e)\sqrt{e}\,\tau^*(m/e)\log e\\&\le c_o\frac{\tau^*(m)\log d}{\phi(d)}\sum_{e\mid d}\phi(e)\sqrt{e}\le c_o\frac{\tau^*(m)\log d}{\phi(d)}\,d^{3/2}.\end{aligned}$$

Following the proof of Theorem 1 we then obtain

$$\begin{aligned}|T|&=\sum_{\substack{s\in S\\(c-as,m)=1}}1=\sum_{s\in S}\sum_{d\mid(c-as,m)}\mu(d)=\sum_{\substack{d\mid m\\(d,c)=1}}\mu(d)|S(a^{-1}c,d)|\\&=B'\sum_{\substack{d\mid m\\(d,c)=1}}\frac{\mu(d)}{\phi(d)}+E=B'\prod_{\substack{p\mid m\\p\nmid c}}\left(1-\frac{1}{p-1}\right)+E,\end{aligned}$$

say, where (again letting $\sum^*$ denote a sum over square-free divisors),

$$\begin{aligned}|E| &\le c_o \sum_{\substack{d|m\\(d,c)=1}}^{*} \frac{\tau^*(m)\log d}{\phi(d)}\, d^{3/2} \le c_o\tau^*(m)\log m \sum_{\substack{d|m\\(d,c)=1}}^{*} d^{3/2}/\phi(d)\\ &\le c_o\tau^*(m)\log m \prod_{p|m,p\nmid c}\left(1+\frac{p^{3/2}}{p-1}\right)\\ &\le c_o\tau^*(m)\sqrt{m}\,\log m \prod_{p|m,p\nmid c}\left(1+\frac{1}{\sqrt{p}}+\frac{1}{p-1}\right)\\ &\le 2\,c_o\tau^*(m)^2\sqrt{m}\,\log m.\end{aligned}$$

We are done provided that $|S|+|T|>\phi(m)$ which is the case if

$$B'+B'\prod_{\substack{p|m\\p\nmid c}}\left(1-\frac{1}{p-1}\right) > \phi(m)+2\,c_o\tau^*(m)^2\sqrt{m}\,\log m, \tag{16}$$

that is, with $\kappa$ as defined in (4),

$$B'(1+\kappa) > \phi(m)+O_\varepsilon\left(m^{\frac{1}{2}+\varepsilon}\right).$$

The theorem now follows from the estimate for $B'$ in (7).

Noting that the estimate for $B'$ in (7), and the Polya-Vinogradov estimate in Lemma 4 with $c_o$ replaced by $2c_o$, both hold as well for a general interval $[A+1, A+B]$, the proof above holds identically for the general interval.

## References


[1] A. Ayyad and T. Cochrane, Lattices in $\mathbb{Z}^2$ and the congruence $xy+uv\equiv c \pmod m$, *Acta Arith.* **132** (2008), no. 2, 127-133.

[2] A. Ayyad and T. Cochrane, The congruence $ax_1x_2\cdots x_k + bx_{k+1}x_{k+2}\cdots x_{2k}\equiv c \pmod p$, *Proc. Amer. Math. Soc.* **145** (2017), no. 2, 467-477.

[3] A. Ayyad, T. Cochrane, S. Shi, Modular hyperbolas and the congruence $ax_1x_2\cdots x_k + bx_{k+1}x_{k+2}\cdots x_{2k}\equiv c \pmod m$, *Integers* **18** (2018), A37, 18 pp.

[4] M. Bordignon and B. Kerr, An explicit Polya-Vinogradov inequality via partial Gaussian sums, *Trans. Amer. Math. Soc.* **373** (2020), no. 9, 6503–6527.

[5] T. Cochrane and S. Shi, The congruence $x_1x_2\equiv x_3x_4 \pmod m$ and mean values of character sums, *J. Number Theory* **130** (2010), no. 3, 767-785.

[6] T. Cochrane and S. Shi, Sum-products mod $m$ and the congruence $ax_1\cdots x_k + bx_{k+1}\cdots x_{2k}\equiv c \pmod m$, *Integers* **20** (2020), A72, 13 pp.

[7] D. A. Frolenkov and K. A. Soundararajan, Generalization of the Pólya-Vinogradov inequality, *Ramanujan J.* **31** (2013), no. 3, 271-279.

[8] M. Z. Garaev, On multiplicative congruences, *Math. Z.* **272** (2012), no. 1-2, 473–482.

[9] M. Z. Garaev and V. C. Garcia, The equation $x_1x_2 = x_3x_4 + \lambda$ in fields of prime order and applications, *J. Number Theory* **128** (2008), no. 9, 2520-2537.

[10] H. Iwaniec, On the problem of Jacobsthal, *Demonstratio Math.* **11** (1978), no. 1, 225-231.

[11] H. Iwaniec and E. Kowalski, *Analytic Number Theory.* American Mathematical Society Colloquium Publications, **53**. American Mathematical Society, Providence, RI, 2004.

[12] H. L. Montgomery, *Topics in Multiplicative Number Theory.* Lecture Notes in Mathematics, **227**. Springer-Verlag, Berlin-New York, 1971.

[13] H. L. Montgomery and R. C. Vaughan, Exponential sums with multiplicative coefficients, *Invent. Math.* **43** (1977), 69-82.

[14] G. Robin, Estimate of the Chebyshev function $\theta$ on the $k$-th prime number and large values of the number of prime divisors function $\omega(n)$ of $n$, *Acta Arith.* **42** (1983), no. 4, 367-389.

[15] J. B. Rosser and L. Schoenfeld, Approximate formulas for some functions of prime numbers, *Illinois J. Math.* **6** (1962), 64-94.