#A72 INTEGERS 20 (2020)

SUM-PRODUCTS MOD M AND THE CONGRUENCE $ax_1x_2\cdots x_k + bx_{k+1}x_{k+2}\cdots x_{2k} \equiv c \pmod{m}$

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: 1/21/20, Accepted: 8/28/20, Published: 9/11/20

Abstract

For $m \in \mathbb{N}$, and integers a, b, c with $(abc, m) = 1$, we show 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 with $1 \le x_i \ll m^{2/k}$, with the implied constant depending on the number of prime factors $\omega(m)$ of m and their maximum multiplicity, generalizing a similar result for prime moduli. More precise results are given in special cases. We also establish that if $\mathcal{A}_1, \mathcal{A}_2, \mathcal{B}_1, \mathcal{B}_2$ are subsets of $\mathbb{Z}_m$, the ring of integers mod m, with $|\mathcal{A}_1||\mathcal{A}_2||\mathcal{B}_1||\mathcal{B}_2| > 16\,\omega(m)^2 m^4/p^*$, where p^* is the minimal prime divisor of m, then $\mathcal{A}_1\mathcal{B}_1 + \mathcal{A}_2\mathcal{B}_2 \supseteq \mathbb{Z}_m^*$, the group of units mod m, generalizing a result of Hart and Iosevich for prime moduli.

1. Introduction

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

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

For prime moduli, it was proven in [2] that there is a solution of (1) with $1 \le x_i \ll_\varepsilon m^{\frac{3}{2k}+\varepsilon}$. Let $r = \omega(m)$, the number of distinct prime factors of m, and let E denote the maximum multiplicity of any prime factor of m. Here we prove the following.

Theorem 1. *For any positive integers E, k, r there is a constant $c(E, k, r)$ such that for $m > c(E, k, r)$ and any integers a, b, c with $(abc, m) = 1$, there exists a solution of (1) with*

$$1 \le x_i \le 2\,m^{2/k}, \qquad 1 \le i \le 2k.$$

Thus, by taking k sufficiently large, we obtain solutions of (1) with $1 \le x_i < m^{\varepsilon}$, for any $\varepsilon > 0$. We conjecture that there is in fact a solution of (1) with

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

uniformly in E and r. Such a bound is optimal aside from the possible removal of the ε. Theorem 1 is useful for classes of integers m where r and E are bounded in size. It is desirable to be able to replace the constant $c(E,k,r)$ with a value depending only on k.

Ayyad and the authors [3] established that for arbitrary m, any cube of edge length B contains a solution of (1) provided that

$$B \gg_{\varepsilon} m^{\frac{1}{4}+\frac{1}{2\sqrt{k}+3.9}+\varepsilon}. \tag{2}$$

For $k > 5$ this is a weaker bound than what is given in Theorem 1, however it applies to cubes in arbitrary position. For prime moduli $m = p$, Garaev [4, Theorem 1] improved (2) to $B \gg_{\varepsilon} p^{\frac{1}{4}+\varepsilon}$ for $k \ge 7$.

For $k = 4, 5$ it was shown in [3] that any cube of edge length $B \gg_{\varepsilon} m^{\frac{3}{8}+\varepsilon}$, $m^{\frac{31}{84}+\varepsilon}$ respectively, contains a solution of (1).

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 $B \ge 2\sqrt{m} + 1$ for prime power m, $B \gg m^{\frac{1}{2}} \log^2 m$, for general m. For prime moduli, Garaev and Garcia [5, Theorem 4] proved a result of the same strength for boxes with edges of different lengths.

Throughout the paper we let $\mathbb{Z}_m$ denote the ring of integers mod m, and $\mathbb{Z}_m^*$ the group of units mod m.

2. Sums of Products

The key to proving the result for prime moduli p in [2] was a theorem of Hart and Iosevich [6, Remark 1.3] stating that if $\mathcal{A}_1, \mathcal{A}_2, \mathcal{B}_1, \mathcal{B}_2$ are subsets of $\mathbb{Z}_p$, with

$$|\mathcal{A}_1||\mathcal{A}_2||\mathcal{B}_1||\mathcal{B}_2| > p^3,$$

then $\mathcal{A}_1\mathcal{B}_1 + \mathcal{A}_2\mathcal{B}_2 \supseteq \mathbb{Z}_p^*$. Let us start by investigating to what extent such a result can be extended to a general modulus.

Example 1. Let m be a positive even integer, H be the subgroup of $\mathbb{Z}_m^*$ consisting of residue classes that are congruent to 1 mod 2, so that $|H| = m/2$ and $\mathcal{A}_1 = \mathcal{B}_1 = \mathcal{A}_2 = \mathcal{B}_2 = H$. Then

$$|\mathcal{A}_1||\mathcal{A}_2||\mathcal{B}_1||\mathcal{B}_2| = \frac{m^4}{16}$$

and $\mathcal{A}_1\mathcal{B}_1 + \mathcal{A}_2\mathcal{B}_2 = 2\mathbb{Z}_m$. In particular, the sum-product set contains no element of $\mathbb{Z}_m^*$.

Example 2. Let m be any odd positive integer, p^* be the minimal prime divisor of m, H be the subgroup of $\mathbb{Z}_m^*$ consisting of residue classes that are squares (mod p^*), so that $|H| = \phi(m)/2$. Let $\mathcal{A}_1 = p^*\mathbb{Z}_m$, $\mathcal{B}_1 = \mathbb{Z}_m$, $\mathcal{A}_2 = \mathcal{B}_2 = H$. Then $|H| = \frac{m}{2}\prod_{p|m}(1-\frac{1}{p})$,

$$|\mathcal{A}_1||\mathcal{A}_2||\mathcal{B}_1||\mathcal{B}_2| > \frac{m^4}{4p^*}\prod_{p|m}(1-\tfrac{1}{p})^2,$$

and $\mathcal{A}_1\mathcal{B}_1 + \mathcal{A}_2\mathcal{B}_2 = H$. In particular, the sum-product set does not contain $\mathbb{Z}_m^*$.

Here we establish the following.

Theorem 2. *Let p^* denote the minimal prime divisor of m and let $r = \omega(m)$. If $\mathcal{A}_1, \mathcal{A}_2, \mathcal{B}_1, \mathcal{B}_2$ are subsets of $\mathbb{Z}_m$ with*

$$|\mathcal{A}_1||\mathcal{A}_2||\mathcal{B}_1||\mathcal{B}_2| > 16r^2\frac{m^4}{p^*},$$

then

$$\mathcal{A}_1\mathcal{B}_1 + \mathcal{A}_2\mathcal{B}_2 \supseteq \mathbb{Z}_m^*. \tag{3}$$

The preceding examples indicate that without further constraints on the sets $\mathcal{A}_i, \mathcal{B}_i$, the lower bound on the product of cardinalities, of order m^4/p^*, is best possible. It may be possible to remove the dependence on r however.

Remark 1. A stronger conclusion, namely that $\mathcal{A}_1\mathcal{B}_1 + \mathcal{A}_2\mathcal{B}_2 \supseteq \mathbb{Z}_m$ or $\mathbb{Z}_m \setminus \{0\}$ is not possible under the hypotheses of Theorem 2, as the following example indicates. Suppose that m has an odd prime divisor p with $p^2|m$. Let λ be a quadratic nonresidue mod p, H be the set of residue classes mod m that are squares mod p, $\mathcal{A}_1 = -\lambda H$, $\mathcal{A}_2 = \mathcal{B}_1 = \mathcal{B}_2 = H$. Then $|\mathcal{A}_1||\mathcal{A}_2||\mathcal{B}_1||\mathcal{B}_2| > \frac{m^4}{16}$ but $p \notin \mathcal{A}_1\mathcal{B}_1+\mathcal{A}_2\mathcal{B}_2$.

3. A More Precise Formulation of Theorem 2

Theorem 2 follows readily from the more precise statement:

Proposition 1. *Let $\mathcal{A}_1, \mathcal{A}_2, \mathcal{B}_1, \mathcal{B}_2$ be subsets of $\mathbb{Z}_m$ such that*

$$|\mathcal{A}_1||\mathcal{A}_2||\mathcal{B}_1||\mathcal{B}_2| > m^4\left[\prod_{p|m}\left(1+\frac{\sqrt{2-\frac{1}{p}}}{\sqrt{p}-1}\right)-1\right]^2.$$

Then

$$\mathcal{A}_1\mathcal{B}_1 + \mathcal{A}_2\mathcal{B}_2 \supseteq \mathbb{Z}_m^*. \tag{4}$$

Proof. For $a \in \mathbb{Z}_m^*$, let N be the number of solutions of the equation $x_1y_1+x_2y_2 = a$ with $x_i \in \mathcal{A}_i, y_i \in \mathcal{B}_i, i = 1, 2$. Then

$$\begin{aligned}
mN &= \sum_{\lambda} \sum_{\substack{x_i\in\mathcal{A}_i\\ y_i\in\mathcal{B}_i}} e_m(\lambda(x_1y_1 + x_2y_2 - a)) \\
&= \sum_{d|m} \sum_{\substack{\lambda=1\\ (\lambda,m)=d}}^{m} \sum_{\substack{x_i\in\mathcal{A}_i\\ y_i\in\mathcal{B}_i}} e_m(\lambda(x_1y_1 + x_2y_2 - a)) \\
&= \sum_{d|m} \sum_{\substack{\lambda=1\\ (\lambda',m/d)=1}}^{m/d} \sum_{\substack{x_i\in\mathcal{A}_i\\ y_i\in\mathcal{B}_i}} e_{m/d}(\lambda'(x_1y_1 + x_2y_2 - a)) \\
&= \sum_{d|m} \sum_{\substack{\lambda=1\\ (\lambda,d)=1}}^{d} \sum_{\substack{x_i\in\mathcal{A}_i\\ y_i\in\mathcal{B}_i}} e_d(\lambda(x_1y_1 + x_2y_2 - a)) \\
&= \prod_{i=1}^{2} |\mathcal{A}_i||\mathcal{B}_i| + Error
\end{aligned}$$

say, with

$$Error := \sum_{\substack{d|m\\ d>1}} \sum_{\substack{\lambda=1\\ (\lambda,d)=1}}^{d} \sum_{\substack{x_i\in\mathcal{A}_i\\ y_i\in\mathcal{B}_i}} e_d(\lambda(x_1y_1 + x_2y_2 - a)). \tag{5}$$

Applying the Cauchy-Schwarz inequality and then extending the range of summation for the y_i, we obtain that

$$\begin{aligned}
|Error| &\le \sum_{\substack{d|m\\ d>1}} \Big(\sum_{y_i\in\mathcal{B}_i} 1\Big)^{1/2} \Big(\sum_{y_i\in\mathcal{B}_i} \Big| \sum_{\substack{\lambda=1\\ (\lambda,d)=1}}^{d} \sum_{x_i\in\mathcal{A}_i} e_d(\lambda(x_1y_1 + x_2y_2 - a))\Big|^2\Big)^{1/2} \\
&\le \sum_{\substack{d|m\\ d>1}} \prod_{i=1}^{2} |\mathcal{B}_i|^{1/2} \Bigg(\sum_{y_1\in\mathbb{Z}_m} \sum_{y_2\in\mathbb{Z}_m} \sum_{\substack{\lambda=1\\ (\lambda,d)=1}}^{d} \sum_{\substack{\lambda'=1\\ (\lambda',d)=1}}^{d} \\
&\quad \sum_{x_i,x_i'\in\mathcal{A}_i} e_d\big(\lambda(x_1y_1 + x_2y_2 - a) - \lambda'(x_1'y_1 + x_2'y_2 - a)\big)\Bigg)^{1/2},
\end{aligned}$$

and so

$$|Error| \leq \sum_{\substack{d|m \\ d>1}} \prod_{i=1}^{2} |\mathcal{B}_i|^{1/2} \left(\sum_{\substack{\lambda=1 \\ (\lambda,d)=1}}^{d} \sum_{\substack{\lambda'=1 \\ (\lambda',d)=1}}^{d} e_d\big(a(\lambda'-\lambda)\big) \right.$$

$$\left. \sum_{x_i,x_i' \in \mathcal{A}_i} \sum_{y_1 \in \mathbb{Z}_m} e_d\big(y_1(\lambda x_1 - \lambda' x_2)\big) \sum_{y_2 \in \mathbb{Z}_m} e_d\big(y_2(\lambda x_2 - \lambda' x_2')\big) \right)^{1/2}$$

$$= m \prod_{i=1}^{2} |\mathcal{B}_i|^{1/2} \sum_{\substack{d|m \\ d>1}} E_d^{1/2}$$

say, where

$$E_d := \sum_{\substack{\lambda=1 \\ (\lambda,d)=1}}^{d} \sum_{\substack{\lambda'=1 \\ (\lambda',d)=1}}^{d} e_d(a(\lambda'-\lambda)) \prod_{i=1}^{2} \sum_{\substack{x_i,x_i' \in \mathcal{A}_i \\ \lambda x_i \equiv \lambda' x_i' \pmod{d}}} 1$$

$$= \sum_{\substack{\nu=1 \\ (\nu,d)=1}}^{d} \left(\sum_{\substack{\lambda=1 \\ (\lambda,d)=1}}^{d} e_d(a\lambda(\nu-1)) \right) \prod_{i=1}^{2} \sum_{\substack{x_i,x_i' \in \mathcal{A}_i \\ x_i \equiv \nu x_i' \pmod{d}}} 1.$$

The sum over λ is a Ramanujan sum, which for any $m \in \mathbb{N}, x \in \mathbb{Z}$, satisfies

$$\sum_{\substack{\lambda=1 \\ (\lambda,m)=1}}^{m} e_m(\lambda x) = \mu\left(\frac{m}{(m,x)}\right) \frac{\phi(m)}{\phi\left(m/(m,x)\right)}.$$

Since $(a,d)=1$, and so $(d, a(\nu-1)) = (d, \nu-1)$, we obtain

$$E_d = \sum_{\substack{\nu=1 \\ (\nu,d)=1}}^{d} \mu\left(\frac{d}{(\nu-1,d)}\right) \frac{\phi(d)}{\phi\left(d/(\nu-1,d)\right)} \prod_{i=1}^{2} \sum_{\substack{x_i,x_i' \in \mathcal{A}_i \\ x_i \equiv \nu x_i' \pmod{d}}} 1$$

$$= \sum_{e|d} \frac{\mu(\frac{d}{e})\phi(d)}{\phi(d/e)} \sum_{\substack{\nu=1,(\nu,d)=1 \\ (\nu-1,d)=e}}^{d} \prod_{i=1}^{2} \sum_{\substack{x_i,x_i' \in \mathcal{A}_i \\ x_i \equiv \nu x_i' \pmod{d}}} 1 \tag{6}$$

$$\leq \sum_{e|d} \frac{|\mu(\frac{d}{e})|\phi(d)}{\phi(\frac{d}{e})} \sum_{\substack{\nu=1,(\nu,d)=1 \\ \nu \equiv 1 \pmod{e}}}^{d} \prod_{i=1}^{2} \sum_{\substack{x_i,x_i' \in \mathcal{A}_i \\ x_i \equiv \nu x_i' \pmod{d}}} 1.$$

Now, for any choice of x_1', x_2' and ν, there are at most m/d choices for x_1 and m/d choices for x_2. Also, the number of choices for ν is the number of t with

$1 \le t \le d/e$ and $(1+te, d) = 1$, which is $\phi(d)/\phi(e)$. Thus, altogether, there are at most $|\mathcal{A}_1||\mathcal{A}_2|\frac{\phi(d)}{\phi(e)}\frac{m^2}{d^2}$ choices for $\nu, x_1, x_2, x_1', x_2'$, and so

$$E_d \le \sum_{e|d} \frac{|\mu(\frac{d}{e})|\phi(d)}{\phi(\frac{d}{e})}|\mathcal{A}_1||\mathcal{A}_2|\frac{\phi(d)}{\phi(e)}\frac{m^2}{d^2},$$

and

$$\begin{aligned} |Error| &< m^2 \prod_{i=1}^{2} |\mathcal{A}_i|^{1/2}|\mathcal{B}_i|^{1/2} \sum_{\substack{d|m \\ d>1}} \frac{\phi(d)}{d}\Big(\sum_{e|d}\frac{|\mu(\frac{d}{e})|}{\phi(\frac{d}{e})\phi(e)}\Big)^{1/2} \\ &= m^2 \prod_{i=1}^{2} |\mathcal{A}_i|^{1/2}|\mathcal{B}_i|^{1/2} \sum_{\substack{d|m \\ d>1}} \frac{\phi(d)}{d} G(d)^{1/2}, \end{aligned} \tag{7}$$

where

$$G(d) := \sum_{e|d} \frac{|\mu(e)|}{\phi(e)\phi(\frac{d}{e})}. \tag{8}$$

Plainly, $G(d)$ is a multiplicative function with

$$G(p^j) = \frac{2p-1}{p}\frac{p^j}{\phi(p^j)^2},$$

$$G(d) = \frac{d}{\phi(d)^2}\prod_{p|d}\left(2 - \frac{1}{p}\right).$$

Thus, we obtain

$$|Error| < m^2 \prod_{i=1}^{2} |A_i|^{1/2}|B_i|^{1/2} \sum_{\substack{d|m \\ d>1}} \frac{1}{\sqrt{d}} \prod_{p|d}\left(2 - \frac{1}{p}\right)^{1/2}.$$

If we include $d = 1$, the sum over d on the right-hand side,

$$H(m) := \sum_{d|m} \frac{1}{\sqrt{d}} \prod_{p|d}\left(2 - \frac{1}{p}\right)^{1/2},$$

is a multiplicative function with

$$H(p^j) = 1 + \sqrt{2 - \frac{1}{p}}\frac{1}{\sqrt{p}}\left(1 + \frac{1}{\sqrt{p}} + \frac{1}{p} + \cdots + \frac{1}{(\sqrt{p})^{j-1}}\right) \le 1 + \sqrt{2 - \frac{1}{p}}\frac{1}{\sqrt{p}-1}.$$

Thus,

$$|Error| < m^2 \prod_{i=1}^{2} |A_i|^{1/2}|B_i|^{1/2}\left[\prod_{p|m}\left(1 + \frac{\sqrt{2-\frac{1}{p}}}{\sqrt{p}-1}\right) - 1\right],$$

which is less than the main term $\prod_{i=1}^{2} |A_i||B_i|$ under the hypothesis of the proposition. □

4. Proof of Theorem 2

The result is vacuously true for $p^* \le 16r^2$, and so we may assume $p^* > 16r^2$. It follows that $p^* \ge (2\sqrt{2}\, r+1)^2$, and so

$$\frac{\sqrt{p^*}-1}{\sqrt{2}} \ge 2r. \tag{9}$$

Now, for any $x \ge 2r$, we have

$$\left(1+\frac{1}{x}\right)^r \le e^{r/x} \le 1+\frac{2r}{x}, \tag{10}$$

and so letting $x = (\sqrt{p^*}-1)/\sqrt{2}$, we have by (9) and (10),

$$\prod_{p|m}\left(1+\frac{\sqrt{2}}{\sqrt{p}-1}\right) \le \left(1+\frac{\sqrt{2}}{\sqrt{p^*}-1}\right)^r \le 1+\frac{2\sqrt{2}\, r}{\sqrt{p^*}-1},$$

and

$$\left[\prod_{p|m}\left(1+\frac{\sqrt{2-\frac{1}{p}}}{\sqrt{p}-1}\right)-1\right]^2 \le \left(\frac{2\sqrt{2}\, r}{\sqrt{p^*}-1}\right)^2 \le \frac{16r^2}{p^*},$$

the latter inequality holding for $p^* > 16$, which we have assumed. The theorem now follows immediately from Proposition 1.

Remark 2. For special classes of moduli, more precise versions of the proposition are available. We give a couple of examples here, prime power moduli and moduli that are products of two distinct primes.

Proposition 2. *For any prime power $m = p^l$, we have*

$$\mathcal{A}_1\mathcal{B}_1 + \mathcal{A}_2\mathcal{B}_2 \supseteq \mathbb{Z}_m^*, \tag{11}$$

provided that

$$|\mathcal{A}_1||\mathcal{A}_2||\mathcal{B}_1||\mathcal{B}_2| > m^4\frac{p-1}{(p-\sqrt{p})^2}.$$

Proof. Let $Error$ denote the error term in (5). For $m = p^l$, the only positive contribution to E_d in (6) occurs when $e = d$, and so we obtain

$$\begin{aligned}
|Error| &< m^2\prod_{i=1}^{2}|A_i|^{1/2}|B_i|^{1/2}\sum_{j=1}^{l}\frac{\phi(p^j)}{p^j}\frac{1}{\sqrt{\phi(p^j)}}\\
&= m^2\prod_{i=1}^{2}|A_i|^{1/2}|B_i|^{1/2}\sqrt{1-\frac{1}{p}}\sum_{j=1}^{l}\frac{1}{p^{j/2}}\\
&\le \frac{\sqrt{p-1}}{p-\sqrt{p}}\; m^2\prod_{i=1}^{2}|A_i|^{1/2}|B_i|^{1/2},
\end{aligned}$$

yielding the result. □

Proposition 3. *For $m = pq$, with primes $p < q$, we have*

$$\mathcal{A}_1\mathcal{B}_1 + \mathcal{A}_2\mathcal{B}_2 \supseteq \mathbb{Z}_m^*, \tag{12}$$

provided that

$$|\mathcal{A}_1||\mathcal{A}_2||\mathcal{B}_1||\mathcal{B}_2| > 2m^3(\sqrt{p} + \sqrt{q} + \sqrt{2})^2.$$

Proof. In this case, with $G(d)$ as defined in (8), we obtain from (7),

$$\begin{aligned}
|Error| &< m^2 \prod_{i=1}^{2} |\mathcal{A}_i|^{1/2}|\mathcal{B}_i|^{1/2} \sum_{\substack{d|pq \\ d>1}} \frac{\phi(d)}{d} G(d)^{1/2} \\
&= m^2 \prod_{i=1}^{2} |\mathcal{A}_i|^{1/2}|\mathcal{B}_i|^{1/2} \Big(\frac{\phi(p)}{p} \frac{\sqrt{2}}{\sqrt{\phi(p)}} + \frac{\phi(q)}{q} \frac{\sqrt{2}}{\sqrt{\phi(q)}} + \frac{\phi(pq)}{pq} \frac{2}{\sqrt{\phi(pq)}} \Big) \\
&< m^2 \prod_{i=1}^{2} |\mathcal{A}_i|^{1/2}|\mathcal{B}_i|^{1/2} \Big(\frac{\sqrt{2}}{\sqrt{p}} + \frac{\sqrt{2}}{\sqrt{q}} + \frac{2}{\sqrt{pq}} \Big) \\
&= m^{\frac{3}{2}} \prod_{i=1}^{2} |\mathcal{A}_i|^{1/2}|\mathcal{B}_i|^{1/2} \Big(\sqrt{2q} + \sqrt{2p} + 2 \Big),
\end{aligned}$$

and the result follows. □

5. Lower Bounds on the Cardinality of Product Sets

Lemma 1. *Let $l, B, P, Q \in \mathbb{N}$, $a_i \in \mathbb{Z}$, with $B \le Q$, $0 \le a_i < P$, $1 \le i \le l$, $(P, Q) = 1$, and let N be the number of solutions of the congruence*

$$(a_1 + Ps_1) \cdots (a_l + Ps_l) \equiv (a_1 + Pt_1) \cdots (a_l + Pt_l) \pmod{Q}, \tag{13}$$

in integers s_i, t_i with $1 \le s_i, t_i \le B$, $1 \le i \le l$. Then, for any $\varepsilon > 0$, we have

$$N \ll_\varepsilon \left(\frac{P^l B^{2l}}{PQ} + B^l \right) (PB)^{l^2 \varepsilon}. \tag{14}$$

Proof. For a given selection of t_i, we must solve a congruence of the type

$$(a_1 + Ps_1)(a_2 + Ps_2) \cdots (a_l + Ps_l) \equiv C \pmod{Q},$$

with $0 \le s_i \le B - 1$, $1 \le i \le l$, for some nonnegative integer $C < Q$, that is,

$$(a_1 + Ps_1)(a_2 + Ps_2) \cdots (a_l + Ps_l) = C + \ell Q,$$

for some nonnegative integer $\ell \le \frac{P^l(B+1)^l}{Q}$. Note that, for any choice of s_i, we have

$$a_1 a_2 \cdots a_l \equiv C + \ell Q \pmod{P},$$

and so the value of ℓ is uniquely determined mod P. Therefore, there are at most $\frac{P^l(B+1)^l}{PQ} + 1$ choices for ℓ. For any choice of ℓ, there are at most $\tau(C+\ell Q)^{l-1} \ll_\varepsilon (PB)^{l^2\varepsilon}$ choices for the s_i, for any $\varepsilon > 0$, and thus the total number of choices for the s_i is

$$\ll_\varepsilon \left(\frac{P^l B^l}{PQ} + 1\right)(PB)^{l^2\varepsilon}.$$

Multiplying by the B^l choices for the t_i, we obtain the upper bound of the lemma. □

Lemma 2. *Under hypotheses of Lemma 1, we have*

$$\#\{(a_1+Ps_1)\cdots(a_l+Ps_l) \pmod{Q} : 1 \le s_i \le B\} \gg_\varepsilon \min\left\{B^l, \tfrac{Q}{P^{l-1}}\right\}(PQ)^{-l^2\varepsilon}.$$

Proof. With N the quantity in Lemma 1, we have

$$\begin{aligned}\#\{(a_1+Ps_1)\cdots(a_l+Ps_l) \pmod{Q} : 0 \le s_i < B\} &\ge \frac{B^{2l}}{N}\\ &\gg_\varepsilon \frac{B^{2l}}{\left(\frac{P^l B^{2l}}{PQ} + B^l\right)(PB)^{l^2\varepsilon}},\end{aligned}$$

and the result follows. □

Lemma 3. *Let B, P, Q be positive integers with $B < Q$, $(P,Q) = 1$ and $B^l \ge 2^{-l}QP^{1-l}$. Let q^* be the minimal prime divisor of Q and $r = \omega(Q)$. Then, for any $\varepsilon > 0$ and sets $\mathcal{A}_i, \mathcal{B}_i$ of the type occurring in Lemma 2, we have $\mathcal{A}_1\mathcal{B}_1 + \mathcal{A}_2\mathcal{B}_2 \supseteq \mathbb{Z}_Q^*$, provided that*

$$q^* \ge c^*(\varepsilon, l, r)P^{4l-4}(PQ)^{4l^2\varepsilon},$$

for some constant $c^*(\varepsilon, l, r)$ depending on ε, l and r.

Proof. By Lemma 2, since $B^l > 2^{-l}QP^{1-l}$, we have

$$|\mathcal{A}_i|, |\mathcal{B}_i| \gg_{\varepsilon,l} QP^{1-l}(PQ)^{-l^2\varepsilon},$$

$i = 1, 2$. Applying Theorem 2 with $m = Q$, we succeed provided that

$$P^{4-4l}Q^4(PQ)^{-4l^2\varepsilon} \gg_{\varepsilon,l,r} Q^4/q^*,$$

the bound given in the lemma. □

6. Proof of Theorem 1

We present the proof for the case of even k, and then note at the end the modification required for odd k. Let $k = 2l$,

$$m = p_1^{e_1} \cdots p_r^{e_r}, \qquad E = \max_{1\le i\le r} e_i,$$

with $p_1 < p_2 < \cdots < p_r$, Fix i with $1 \le i \le r$, and let

$$P_i := p_1^{e_1} \cdots p_{i-1}^{e_{i-1}}, \qquad Q_i := p_i^{e_i} \cdots p_r^{e_r},$$

so that $P_iQ_i = m$ and $(P_i, Q_i) = 1$. For $i = 1$, we have $P_1 = 1$, $Q_1 = m$. Let I be the maximal i such that $P_i^l < m$. Then, for $i \le I$, we have

$$P_i^{l-1} < Q_i. \tag{15}$$

For fixed $i \le I$, we set $B = \lfloor Q_i^{\frac{1}{l}} P_i^{\frac{1}{l}-1} \rfloor$, a positive integer satisfying $B \ge \frac{1}{2} Q_i^{\frac{1}{l}} P_i^{\frac{1}{l}-1}$, the hypothesis needed for Lemma 3.

Consider the congruence

$$ax_1 \cdots x_k + bx_{k+1} \cdots x_{2k} \equiv c \pmod{m}, \tag{16}$$

with $(abc, m) = 1$. Let $\mathbf{a} = (a_1, \ldots, a_{2k})$ be a solution of the same congruence mod P_i with $0 \le a_i < P_i$, $1 \le i \le 2k$. Such a solution plainly exists. Thus any point of the form $\mathbf{x} = \mathbf{a} + P_i\mathbf{s}$ with $\mathbf{s} = (s_1, \ldots, s_{2k})$ satisfies the congruence mod P_i, and so our task is to find a choice of $\mathbf{s}$ such that $\mathbf{x}$ satisfies the congruence mod Q_i as well. Let

$$\begin{aligned}
\mathcal{A}_1 &= \{a(a_1 + P_i s_1) \cdots (a_l + P_i s_l) \pmod{Q_i} : 1 \le s_i \le B\},\\
\mathcal{B}_1 &= \{(a_{l+1} + P_i s_{l+1}) \cdots (a_k + P_i s_k) \pmod{Q_i} : 1 \le s_i \le B\},\\
\mathcal{A}_2 &= \{b(a_{k+1} + P_i s_{k+1}) \cdots (a_{k+l} + P_i s_{k+l}) \pmod{Q_i} : 1 \le s_i \le B\},\\
\mathcal{B}_2 &= \{(a_{k+l+1} + P_i s_{k+l+1}) \cdots (a_{2k} + P_i s_{2k}) \pmod{Q_i} : 1 \le s_i \le B\},
\end{aligned}$$

regarded as subsets of $\mathbb{Z}_Q^*$. Since the constant c in (16) is relatively prime to m, to obtain a solution of (16) mod Q_i, it suffices to show that $\mathcal{A}_1\mathcal{B}_1 + \mathcal{A}_2\mathcal{B}_2 \supseteq \mathbb{Z}_{Q_i}^*$. This will yield a solution of the mod m congruence (16) with

$$1 < x_i < P_i + P_iB \le 2P_iB \le 2Q_i^{1/l} P_i^{1/l} = 2m^{1/l}, \qquad 1 \le i \le 2k,$$

as desired. By Lemma 3, such is the case provided that

$$p_i \ge c^* P_i^{4l-4} m^{4l^2\varepsilon} = c^*(p_1^{e_1} \cdots p_{i-1}^{e_{i-1}})^{4l-4} m^{4l^2\varepsilon},$$

with $c^* = c^*(\varepsilon, l, r)$, the constant in Lemma 3.

Suppose to the contrary that the latter condition fails for $1 \le i \le I$, that is, for $1 \le i \le I$,

$$p_i \le \lambda_i := c^*(p_1^{e_1} \cdots p_{i-1}^{e_{i-1}})^{4l-4} m^{4l^2\varepsilon}.$$

Here, $\lambda_1 = c^* m^{4l^2\varepsilon}$. Observing that for any $2 \le i \le I$,

$$\lambda_i = p_{i-1}^{e_{i-1}(4l-4)} \lambda_{i-1} \le \lambda_{i-1}^{e_{i-1}(4l-4)} \lambda_{i-1} \le \lambda_{i-1}^{e_{i-1}(4l-3)},$$

we obtain

$$\lambda_i \le \lambda_1^{\prod_{j=1}^{i-1} e_j(4l-3)}, \quad 2 \le i \le I,$$

and so for $1 \le i \le I$,

$$p_i \le \lambda_i \le (c^* m^{4l^2\varepsilon})^{E^{i-1}(4l-3)^{i-1}}.$$

For convenience, if $I = r$, set $P_{r+1} = m$. It follows that

$$\begin{aligned} P_{I+1} = \prod_{i=1}^{I} p_i^{e_i} &\le \prod_{i=1}^{I} (c^* m^{4l^2\varepsilon})^{E^i(4l-3)^{i-1}} \le (c^* m^{4l^2\varepsilon})^{E^I \sum_{i=1}^{I}(4l-3)^{i-1}} \\ &< (c^* m^{4l^2\varepsilon})^{E^r(4l-3)^r}. \end{aligned}$$

Now, by definition, $P_{I+1} > m^{\frac{1}{l}}$, and so

$$(c^*)^{E^r(4l-3)^r} m^{4l^2\varepsilon E^r(4l-3)^r} > m^{\frac{1}{l}}.$$

If ε is chosen so that

$$4l^2\varepsilon E^r(4l-3)^r < \frac{1}{2l},$$

then we obtain a contradiction if $m > (c^*)^{2lrE^r(4l-3)^r}$, a constant depending on l, r and E.

For the case of odd k, say $k = 2l+1$, we proceed as above letting $\mathcal{A}_1, \mathcal{A}_2$ be products of $l+1$ variables, and $\mathcal{B}_1, \mathcal{B}_2$ products of l variables. In this case, Lemma 3 requires

$$q^* \ge c^* P^{4l-2}(PQ)^{4(l+1)^2\varepsilon},$$

and thus we reach the same conclusion with a slightly modified choice of ε.

7. The Cases $r = 1, 2$

The proof above can be refined to yield a slightly smaller exponent on m than the value $2/k$ given in Theorem 1. We do so in the next theorem for the cases $r = 1$ and $r = 2$.

Theorem 3. *i) If $m = p^e$, a prime power, then for any a, b, c with $(abc, m) = 1$, there is a solution of (1) with*

$$1 \le x_i \ll_{\varepsilon,k,e} m^{\frac{2}{k}-\frac{1}{2ek}+\varepsilon}, \qquad 1 \le i \le 2k.$$

ii) If $m = p^e q^f$, a product of distinct prime powers, then for any a, b, c with $(abc, m) = 1$, there is a solution of (1) with

$$1 \le x_i \ll_{\varepsilon,k,e,f} m^{\frac{2}{k}-\frac{1}{2ke((k-2)f+1)}+\varepsilon}, \qquad 1 \le i \le 2k.$$

The estimate in part ii) reduces to the part i) estimate when $f = 0$. With $e = 1, f = 0$, both parts recover the prime moduli estimate of [2], $1 \le x_i \ll_\varepsilon p^{\frac{3}{2k}+\varepsilon}$.

Proof. i) Let $m = p^e$ and assume $k = 2l$. The proof follows the same argument as the proof of Theorem 1 and so we will be brief. By Theorem 2 and Lemma 2 with $P = 1$, $Q = m$, we succeed provided that

$$\min\{B^l, m\}^4 \gg_\varepsilon \frac{m^{4+l^2\varepsilon}}{p},$$

that is, $p \gg_\varepsilon m^{l^2\varepsilon}$ and $B^{4l} \gg_\varepsilon m^{4+l^2\varepsilon}/p$. The first condition holds for $\varepsilon < \frac{1}{el^2}$ and p greater than a constant depending on e and l. Since $p = m^{1/e}$, the second condition can be rewritten $B^{4l} \gg_\varepsilon m^{4-\frac{1}{e}+l^2\varepsilon}$, and thus the theorem follows.

ii) Let $m = PQ$ with $P = p^e$, $Q = q^f$ with $p < q$ primes. If we apply Theorem 2 to the congruence (1) mod m as above, then we succeed provided that

$$\min\{B^l, PQ\}^4 \gg_\varepsilon \tfrac{m^{4+l^2\varepsilon}}{p}, \tag{17}$$

whereas if we apply it the congruence (1) mod Q, restricting the x_i to an arithmetic progression $x_i = a_i + Ps_i$ with the a_i a solution to the mod P congruence with $a_{k+1} = \cdots = a_{2k} = 0$, then we succeed provided that

$$\min\{B^l, Q\}^2 \min\left\{B^l, \frac{Q}{P^{l-1}}\right\}^2 \gg_\varepsilon \frac{Q^4}{q} m^{l^2\varepsilon}. \tag{18}$$

We consider B^l in the different ranges, $Q < B^l < PQ$, $\frac{Q}{P^{l-1}} < B^l < Q$ and $B^l < \frac{Q}{P^{l-1}}$. By Theorem 1, we may assume $B^l < PQ$.

I. If $Q < B^l < PQ$, then by (17) and (18), we succeed if either

$$B^{4l} \gg_\varepsilon \frac{m^{4+l^2\varepsilon}}{p}, \quad \text{or} \quad q \gg_\varepsilon p^{e(2l-2)} m^{l^2\varepsilon}. \tag{19}$$

If the second inequality fails, that is, $q \ll_\varepsilon p^{e(2l-2)} m^{l^2\varepsilon}$ with the same implied constant, then

$$m = p^e q^f \le p^e \cdot p^{ef(2l-2)} m^{l^2 f\varepsilon} \ll_{e,f,l,\varepsilon} p^{e(2fl-2f+1)} m^\varepsilon,$$

whence $p \gg_{e,f,l,\varepsilon} m^{\frac{1}{e(2lf-2f+1)}-\varepsilon}$. Thus, the first inequality in (19) holds if

$$B^{4l} \gg_{e,f,l,\varepsilon} m^{4-\frac{1}{e(2lf-2f+1)}+\varepsilon},$$

yielding the result of the theorem.

II. If $\frac{Q}{P^{l-1}} < B^l \leq Q$, then by (17) and (18) we need

$$B^{4l} \gg_{\varepsilon} \frac{m^{4+l^2\varepsilon}}{p}, \tag{20}$$

or $\quad B^{2l}\frac{q^{2f}}{p^{2e(l-1)}} \gg_{\varepsilon} \frac{q^{4f}}{q}m^{l^2\varepsilon}$, that is,

$$B^{2l} \gg_{\varepsilon} q^{2f-1}p^{2e(l-1)}m^{l^2\varepsilon}. \tag{21}$$

If $q^2 < p^{4e(l-2)+1}$, then $m = p^eq^f < p^{e+\frac{f}{2}(4e(l-2)+1)}$, and so

$$p > m^{\frac{2}{4ef(l-2)+f+2e}}.$$

Thus by (20) it suffices to have

$$B^{4l} > m^{4-\frac{2}{4ef(l-2)+f+2e}+l^2\varepsilon}, \tag{22}$$

which is weaker than the inequality in case I.

If $q^2 \geq p^{4e(l-2)+1}$, equivalently

$$q^{2f-1}p^{2e(l-1)} \leq m^{2-\frac{1}{4ef(l-2)+f+2e}},$$

then by (21) it again suffices to have (22).

III. If $B^l < Q/P^{l-1}$, then by (18) it suffices to have $B^{4l} \gg_{\varepsilon} q^{4f-1}m^{l^2\varepsilon}$. Since $m \geq q^f$, it suffices to have $B^{4l} \gg_{\varepsilon} m^{4-\frac{1}{f}+l^2\varepsilon}$, which again is weaker than the lower bound in case I. □

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, and 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), no. A37, 1-18.

[4] M. Z. Garaev, On congruences involving products of variables from short intervals, *Quarterly J. Math.* **69** (2018), no. 3, 769-778.

[5] 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.

[6] D. Hart and A. Iosevich, Sums and products in finite fields: an integral geometric viewpoint, Radon transforms, geometry, and wavelets, 129-135, *Contemp. Math.*, **464**, Amer. Math. Soc., Providence, RI, 2008.