MODULAR HYPERBOLAS AND THE CONGRUENCE $ax_1x_2\cdots x_k + bx_{k+1}x_{k+2}\cdots x_{2k} \equiv c \pmod{m}$

Anwar Ayyad
Department of Mathematics, Al Azhar University, Gaza Strip, Palestine
anwarayyad@yahoo.com

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: 6/12/17, Accepted: 2/20/18, Published: 4/20/18

Abstract

For any cube-free integer m, and integers a, b, c with $(abc, m) = 1$, we obtain the existence of solutions of the congruence $x_1 \cdots x_k \equiv c \pmod{m}$, in any cube of edge length $B \gg_\epsilon m^{\frac{1}{4}+\frac{1}{\sqrt{2(k+4)}}+\epsilon}$, and of the congruence $ax_1x_2\cdots x_k + bx_{k+1}x_{k+2}\cdots x_{2k} \equiv c \pmod{m}$, in any cube $\mathcal{B}$ of edge length $B \gg_\epsilon m^{\frac{1}{4}+\frac{1}{2(\sqrt{k}+1.95)}+\epsilon}$. Refinements are given for small k, and results are also given for arbitrary $m \in \mathbb{N}$.

1. Introduction

A k-dimensional modular hyperbola is the set of solutions of a congruence

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

where $(c, m) = 1$. Shparlinski [21] has written at length on the properties and applications of modular hyperbolas. Of particular interest is obtaining solutions with coordinates restricted to intervals of short length; see [1], [2], [11], [12] and [20], in addition to [21]. The first two authors [3] studied the related congruence

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

with a prime modulus and obtained a number of results on the distribution its solutions. In this work we extend the results of [1] and [3] to general moduli, addressing modular hyperbolas in the next three sections and the latter congruence in the remaining sections. The proof of our results on the modular hyperbola is a straightforward generalization and refinement of what was done in [1] for the case of prime moduli and in [20] for the case of composite moduli with intervals of the form $[1, B]$. The main novelty of this paper is the method of proof provided for our results on the second congruence. For the case of a prime modulus, the authors in [3] made use of additive combinatorics, in particular a result of Hart and Iosevich [13] on when we have a sum-product relation $A_1B_1 + A_2B_2 \supseteq \mathbb{Z}_p^*$. Here, no appeal is made to additive combinatorics, but rather a more delicate evaluation of character sums is made in order to obtain results of the same strength as the mod p results of [3] for a general modulus, for boxes in general position.

2. The Congruence $x_1 \cdots x_k \equiv c \pmod{m}$

For $k, m \in \mathbb{N}$, and integers c with $(c, m) = 1$, we consider the congruence

$$x_1x_2 \cdots x_k \equiv c \pmod{m}. \tag{1}$$

with variables restricted to a general box $\mathcal{B}$ with sides of length B_i,

$$\mathcal{B} = \{(x_1, \ldots, x_k) \in \mathbb{Z}^k : h_i + 1 \leq x_i \leq h_i + B_i, 1 \leq i \leq k\}; \tag{2}$$

for convenience we take $h_i, B_i \in \mathbb{Z}$, $1 \leq i \leq k$ and assume $1 \leq B_i < m$. If all of the B_i are equal, say $B_i = B$, $1 \leq i \leq k$, then we call $\mathcal{B}$ a cube with edge length B.

Let $\mathbb{Z}_m = \mathbb{Z}/(m)$ and $\mathbb{Z}_m^*$ be the group of units in $\mathbb{Z}_m$. By identifying $\mathbb{Z}_m$ with an appropriate set of integer representatives we may view $\mathcal{B}$ as a box of points in $\mathbb{Z}_m^k$. Let I_i be the interval in $\mathbb{Z}_m^*$ given by

$$I_i = [h_i + 1, h_i + B_i] \cap \mathbb{Z}_m^*, \tag{3}$$

and

$$\mathcal{B}^* = I_1 \times I_2 \times \cdots \times I_k = \mathcal{B} \cap \mathbb{Z}_m^{*k}.$$

If all $B_i = B$ we will continue calling $\mathcal{B}^*$ a cube with edge length B, although it may be the case that the cardinalities $|I_i|$ of the edges are not equal.

Generalizing the work of the first author [1] for prime moduli, and Shparlinski [20, Theorem 9] for composite moduli, we obtain the following result.

Theorem 1. *Suppose that $k \geq 4$, $r \in \mathbb{N}$. Let c be an integer with $(c, m) = 1$. Then the number n_c of solutions of the congruence*

$$x_1 \cdots x_k \equiv c \pmod{m}, \tag{4}$$

with $x_i \in I_i$, $1 \le i \le k$, is given by

$$n_c = \frac{|\mathcal{B}^*|}{\phi(m)} + O_\epsilon\left(|\mathcal{B}^*|^{1-\frac{1}{r}-\frac{2}{k}+\frac{4}{kr}} m^{\frac{r+1}{4r^2}(k-4)+\epsilon} m_1^{\frac{3r-1}{4r^2}(k-4)} \right),$$

where $m_1 = \prod_{\substack{p^e || m \\ e \ge 3}} p^e$. The m_1 term may be removed for $r = 1, 2$ or 3.

Shparlinski proved the special case where each interval is of the form $[1, B_i] \cap \mathbb{Z}_m^*$ and $r = 1, 2$ or 3.

The theorem yields an asymptotic estimate for n_c provided that

$$|\mathcal{B}^*| \gg m^{\frac{k}{4}+\frac{k(k-4+2r^2)}{4r(k-4+2r)}+\epsilon} m_1^{\frac{(3r-1)k(k-4)}{4r(k+2r-4)}}, \tag{5}$$

where the m_1 term may be dropped for $r = 1, 2$, or 3. In particular, using $r = 2$, 3 we see that $n_c > 0$ for any m and any cube $\mathcal{B}^*$ with edge length

$$B \gg_\epsilon \begin{cases} m^{\frac{3}{8}+\frac{1}{2k}+\epsilon}, & \text{for } k = 4, 5, 6; \\ m^{\frac{1}{3}+\frac{1}{k+2}+\epsilon}, & \text{for } k \ge 7. \end{cases}$$

Thus for a general modulus m we can only get down to a threshold of $m^{\frac{1}{3}+\epsilon}$ for k sufficiently large. In particular, this is the best we can do for the case where $m = m_1$. At the other extreme, where $m_1 = 1$, we can reduce the exponent further to $\frac{1}{4} + \epsilon$ for k sufficiently large. To be precise, if $m_1 = 1$ then choosing the optimal value of r (as shown in [1]), we obtain for $k \ge 4$ that $n_c > 0$ for any cube with

$$B \gg_\epsilon m^{\frac{1}{4}+\frac{1}{\sqrt{2(k+4)}}+\epsilon}. \tag{6}$$

For a general box $\mathcal{B}^*$, the same holds for

$$|\mathcal{B}^*| \gg_\epsilon m^{\frac{k}{4}+\frac{k}{\sqrt{2(k+4)}}+\epsilon}.$$

Next, let us examine the cases where $k = 2, 3$ or 4. For $k = 2$ it is well known that $n_c > 0$ for any m and any cube $\mathcal{B}^*$ of edge length B, provided that

$$B \gg_\epsilon m^{\frac{3}{4}+\epsilon};$$

see for example [23], [15] or [21]. The proof makes use of the Kloosterman sum estimate. For $k = 4$, the m_1 term in (5) goes away altogether, and we get $n_c > 0$ for any m and box $\mathcal{B}^*$ with

$$|\mathcal{B}^*| \gg_\epsilon m^{2+\epsilon}. \tag{7}$$

We deduce a result for $k = 3$ from our $k = 4$ result by applying it to a box with $I_4 = \{1\}$. In this case the inequality in (7) yields a solution in any box with

$|I_1||I_2||I_3| \gg_\epsilon m^{2+\epsilon}$. Thus, any cube of side length B contains a solution of (1) provided that

$$B \gg_\epsilon \begin{cases} m^{\frac{2}{3}+\epsilon}, & \text{if } k = 3; \\ m^{\frac{1}{2}+\epsilon}, & \text{if } k = 4. \end{cases}$$

For $k = 3$ the same estimate was given in [1, Theorem 1] for prime moduli. A weaker result for $k = 3$ was given for composite m in [20, Theorem 8].

3. Estimating the Cardinality of an Interval in $\mathbb{Z}_m^*$

Before proceeding with the proof of Theorem 1, let us remind the reader of a well known estimate for the cardinality of an interval

$$I = [h+1, h+B] \cap \mathbb{Z}_m^*, \tag{8}$$

in $\mathbb{Z}_m^*$. We prove a numeric lower bound for our purposes here.

Lemma 1. *For $m > 30$ and any interval I of edge length B in $\mathbb{Z}_m^*$,*

$$|I| > \frac{1}{3}\frac{B}{\log\log m} - m^{.96/\log\log m}.$$

In particular, if $B > m^\epsilon$ and m is sufficiently large, then $|I| > \frac{1}{4}\frac{B}{\log\log m}$. The result follows from the next two lemmas.

Lemma 2. *For any $B, d \in \mathbb{N}$, $h \in \mathbb{Z}$, the number of multiples of d in the interval $[h+1, h+B]$ is $\frac{B}{d} + \frac{r}{d}$, for some $r \in \mathbb{Z}$ with $|r| \le d$.*

Proof. Say $h + 1 = q_1 d + r_1$, $h + B = q_2 d + r_2$, with $q_1, q_2 \in \mathbb{Z}$, $0 \le r_1, r_2 < d$. If $r_1 > 0$, there are $q_2 - q_1$ multiples of d in $[h+1, h+B]$, and we have

$$q_2 - q_1 = \frac{B - r_2 - 1 + r_1}{d} = \frac{B}{d} + \frac{r_1 - r_2 - 1}{d},$$

with $|r_1 - r_2 - 1| \le d$. If $r_1 = 0$, then there are $q_2 - q_1 + 1$ multiples of d in the interval, and we have

$$q_2 - q_1 + 1 = \frac{B - r_2 - 1 + r_1 + d}{d} = \frac{B}{d} + \frac{d - r_2 - 1}{d},$$

with $|d - r_2 - 1| \le d - 1$. $\square$

Lemma 3. *For any $m \in \mathbb{N}$, and interval I in $\mathbb{Z}_m^*$, we have*

$$|I| = \frac{\phi(m)}{m}B + \theta 2^{\omega(m)},$$

for some $|\theta| \le 1$, where $\omega(m)$ is the number of distinct prime divisors of m.

Proof.

$$\sum_{\substack{h+1\le x\le h+B\\(x,m)=1}} 1 = \sum_{h+1\le x\le h+B}\ \sum_{d|(x,m)} \mu(d)$$
$$= \sum_{d|m}\mu(d) \sum_{\substack{h+1\le x\le h+B\\ d|x}} 1.$$

By the preceding lemma, the sum over x is just $\frac{B}{d}+\delta(d)$ for some real number $\delta(d)$ with $|\delta(d)|\le 1$. Thus

$$\sum_{\substack{h+1\le x\le h+B\\(x,m)=1}} 1 = \sum_{d|m}\mu(d)\left(\frac{B}{d}+\delta_d\right)$$
$$= B\sum_{d|m}\frac{\mu(d)}{d} + \sum_{d|m}\mu(d)\delta(d) = B\frac{\phi(m)}{m} + \sum_{d|m}\mu(d)\delta(d).$$

The latter sum is bounded by the number of square-free divisors of m, $2^{\omega(m)}$. □

Proof of Lemma 1. By the work of Robin [18] we have $\omega(m)\le 1.3841\log m/\log\log m$ for $m\ge 3$, whence, $2^{\omega(m)} < m^{.96/\log\log m}$ for $m\ge 3$. Also, by the work of Rosser and Shoenfeld [19] we have $m/\phi(m) < 3\log\log m$ for $m>30$. Thus for $m>30$, it follows from the preceding lemma that for any interval I in $\mathbb{Z}_m^*$,

$$|I| > \frac{1}{3}\frac{B}{\log\log m} - m^{.96/\log\log m},$$

as desired. □

4. Proof of Theorem 1

The theorem is an easy consequence of the following lemma. We let χ_0 denote the principal character $\pmod m$ and write $\sum_{\chi\ne\chi_0}$ to indicate a sum over all multiplicative characters $\pmod m$ with $\chi\ne\chi_0$.

Lemma 4. *For any interval of points in $\mathbb{Z}_m^*$ as in* (8)*, we have*

$$\frac{1}{\phi(m)}\sum_{\chi\ne\chi_0}\left|\sum_{x\in I}\chi(x)\right|^4 \ll_\epsilon |I|^2 m^\epsilon.$$

Proof. Let B denote the length of the interval I. If $B\ge m^{\epsilon/4}$, then by Lemma 1, $B\ll_\epsilon |I|\log\log m$. Using the mean value estimate

$$\frac{1}{\phi(m)}\sum_{\chi\ne\chi_0}\left|\sum_{x=a+1}^{a+B}\chi(x)\right|^4 \ll 8^{\omega(m)}\tau(m)(\log m)^3(\log\log m)^7B^2, \qquad (9)$$

of Cochrane and Shi [8], where $\tau(m)$ is the number of divisors of m and $\omega(m)$ is the number of distinct prime divisors of m, we obtain

$$\frac{1}{\phi(m)}\sum_{\chi\neq\chi_0}\left|\sum_{x\in I}\chi(x)\right|^4 \ll_\epsilon B^2 m^\epsilon \ll_\epsilon |I|^2 m^\epsilon.$$

If $B < m^{\epsilon/4}$, the trivial bound implies

$$\frac{1}{\phi(m)}\sum_{\chi\neq\chi_0}\left|\sum_{x\in I}\chi(x)\right|^4 \ll B^4 \leq m^\epsilon.$$

$\square$

Lemma 5. *We have for any nonprincipal character* $\chi \pmod m$,

$$\left|\sum_{x\in I}\chi(x)\right| \ll_\epsilon |I|^{1-\frac{1}{r}} m^{\frac{r+1}{4r^2}+\epsilon} m_1^{\frac{3r-1}{4r^2}},$$

where $m_1 = \prod_{\substack{p^e\|m\\ e\geq 3}} p^e$.

Proof. The proof is similar to the preceding lemma. If $B \geq m^\epsilon$, the upper bound of Burgess [4], [5] for a general m (see for example [14, equation (12.56)] or [17, Theorem 1.6]),

$$\left|\sum_{x=a+1}^{a+B}\chi(x)\right| \ll_\epsilon B^{1-\frac{1}{r}} m^{\frac{r+1}{4r^2}+\epsilon} m_1^{\frac{3r-1}{4r^2}}, \tag{10}$$

yields the result. If $B < m^\epsilon$, the trivial bound gives the result. $\square$

Lemma 6. *For any positive integers* k, m, r, *with* $k \geq 4$, *and intervals* I_i *as above,*

$$\frac{1}{\phi(m)}\sum_{\chi\neq\chi_0}\prod_{i=1}^{k}\left|\sum_{x_i\in I_i}\chi(x_i)\right| \ll_{\epsilon,k} |\mathcal{B}^*|^{1-\frac{1}{r}-\frac{2}{k}+\frac{4}{kr}} m^{\frac{r+1}{4r^2}(k-4)+\epsilon} m_1^{\frac{3r-1}{4r^2}(k-4)}.$$

Proof. By the preceding two lemmas, we have for any interval I_i,

$$\begin{aligned}\frac{1}{\phi(m)}\sum_{\chi\neq\chi_0}\left|\sum_{x\in I_i}\chi(x)\right|^k &\leq \max_{\chi\neq\chi_0}\left|\sum_{x\in I_i}\chi(x)\right|^{k-4}\frac{1}{\phi(m)}\sum_{\chi\neq\chi_0}\left|\sum_{x\in I_i}\chi(x)\right|^4\\ &\ll_\epsilon |I_i|^2 m^\epsilon \max_{\chi\neq\chi_0}\left|\sum_{x\in I_i}\chi(x)\right|^{k-4}\\ &\ll_{\epsilon,k} |I_i|^{k(1-\frac{1}{r})-2+\frac{4}{r}} m^{\frac{r+1}{4r^2}(k-4)+\epsilon} m_1^{\frac{3r-1}{4r^2}(k-4)}. \end{aligned} \tag{11}$$

By Hölder's inequality,

$$\sum_{\chi\neq\chi_0}\prod_{i=1}^{k}\left|\sum_{x_i\in I_i}\chi(x_i)\right| \le \prod_{i=1}^{k}\left(\sum_{\chi\neq\chi_0}\left|\sum_{x_i\in I_i}\chi(x_i)\right|^k\right)^{1/k}.$$

Inserting the upper bound in (11) completes the proof. □

Proof of Theorem 1. The number of solutions of (4) with $x_i \in I_i$, $1 \le i \le k$, is given by

$$n_c = \frac{1}{\phi(m)}\sum_{x_i\in I_i}\sum_{\chi}\chi(c^{-1}x_1\cdots x_k) \tag{12}$$

$$= \frac{\prod_{i=1}^k |I_i|}{\phi(m)} + \frac{1}{\phi(m)}\sum_{\chi\neq\chi_0}\chi(c^{-1})\prod_{i=1}^{k}\sum_{x_i\in I_i}\chi(x_i). \tag{13}$$

The result follows from the preceding lemma. □

5. The Congruence $ax_1\cdots x_k + by_1\cdots y_k \equiv c \pmod{m}$

We turn now to the congruence

$$ax_1x_2\cdots x_k + by_1y_2\cdots y_k \equiv c \pmod{m}. \tag{14}$$

Let I_i, J_i be intervals in $\mathbb{Z}_m^*$ given by

$$I_i = [h_i+1, h_i+B_i]\cap\mathbb{Z}_m^*, \qquad J_i = [h_{k+i}+1, h_{k+i}+B_{k+i}]\cap\mathbb{Z}_m^*, \tag{15}$$

for some $h_i, B_i \in \mathbb{Z}$, with $1 \le B_i \le m$, $1 \le i \le k$.

Theorem 2. *Suppose that $k, m, r \in \mathbb{N}$ with $k \ge 4$, $r \ge 2$, and that $a, b, c \in \mathbb{Z}$ with $(abc, m) = 1$. The number N^* of solutions of (14) with $x_i \in I_i$, $y_i \in J_i$, $1 \le i \le k$, is given by*

$$N^* = \frac{\prod_{i=1}^k |I_i||J_i|}{\phi(m)}\prod_{p|m}\frac{p-2}{p-1} + O\left(\sqrt{m}\ (\prod_{i=1}^{k}|I_i||J_i|)^{(1-\frac{1}{r})-\frac{2}{k}+\frac{4}{kr}} m^{\frac{r+1}{2r^2}(k-4)+\epsilon} m_1^{\frac{3}{2r}(k-4)}\right)$$
$$+ O\left(\frac{\prod_{i=1}^k |I_i|}{\phi(m)}\prod_{i=1}^{k}|J_i|^{(1-\frac{1}{r})-\frac{2}{k}+\frac{4}{kr}} m^{\frac{r+1}{4r^2}(k-4)+\epsilon} m_1^{\frac{3}{4r}(k-4)}\right)$$
$$+ O\left(\frac{\prod_{i=1}^k |J_i|}{\phi(m)}\prod_{i=1}^{k}|I_i|^{(1-\frac{1}{r})-\frac{2}{k}+\frac{4}{kr}} m^{\frac{r+1}{4r^2}(k-4)+\epsilon} m_1^{\frac{3}{4r}(k-4)}\right).$$

For $r = 2$ or 3, the m_1 term may be dropped from the error terms.

We note that if $2|m$ the main term of the theorem vanishes. Indeed, in this case it is plain that $N^* = 0$, since for any odd integers x_i, the left-hand side of (14) is even while the right-hand side is odd. Aside from this case, the theorem yields an asymptotic formula for N^* provided that the following three inequalities hold,

$$\prod_{i=1}^{k} |I_i||J_i| \gg_\epsilon m^{\frac{k}{2}+\frac{k(r^2+k-4)}{2r(k-4+2r)}+\epsilon} m_1^{\frac{3k(k-4)}{2(k-4+2r)}}, \tag{16}$$

$$\prod_{i=1}^{k} |I_i| \gg_\epsilon m^{\frac{k(k-4)(r+1)}{4r(k-4+2r)}+\epsilon} m_1^{\frac{3k(k-4)}{4(k-4+2r)}}, \tag{17}$$

and

$$\prod_{i=1}^{k} |J_i| \gg_\epsilon m^{\frac{k(k-4)(r+1)}{4r(k-4+2r)}+\epsilon} m_1^{\frac{3k(k-4)}{4(k-4+2r)}}. \tag{18}$$

The m_1 term may be dropped if $r = 2$ or 3. The result obtained here generalizes the result of [3] for prime moduli. Using $r = 3$ we obtain for $k \geq 4$ and any positive integer m, that $N^* > 0$ provided that

$$\prod_{i=1}^{k} |I_i||J_i| \gg_\epsilon m^{\frac{2k}{3}+\frac{k}{2(k+2)}+\epsilon}, \quad \prod_{i=1}^{k} |I_i| \gg_\epsilon m^{\frac{k}{3}-\frac{2k}{k+2}+\epsilon}, \quad \prod_{i=1}^{k} |J_i| \gg_\epsilon m^{\frac{k}{3}-\frac{2k}{k+2}+\epsilon}. \tag{19}$$

(There is no advantage in using $r = 2$ for any value of k.) For a general modulus this is the best we can do.

For a cube, it is easy to verify that the condition in (16) implies the conditions in (17) and (18). In particular, taking $r = 3$, we see that for $k \geq 4$ and arbitrary m, any cube with edge length

$$B \gg_\epsilon m^{\frac{1}{3}+\frac{1}{4(k+2)}+\epsilon}, \tag{20}$$

contains a solution of (14). Suppose now that $m_1 = 1$, $k \geq 5$. Then the optimal choice of r is an integer satisfying

$$\frac{r^2+k-4}{2r^2+rk-4r} < \frac{2}{\sqrt{k}+1.95},$$

as shown in [3, Lemma 4.2]. For this choice of r we see that any cube with edge length

$$B \gg_\epsilon m^{\frac{1}{4}+\frac{1}{2\sqrt{k}+3.9}+\epsilon},$$

contains a solution of (14).

Although Theorem 2 requires $k \geq 4$, we can deduce a result for $k = 3$ by applying it with $k = 4$ and $I_4 = J_4 = \{1\}$. In this manner we obtain from (19) that $N^* > 0$ for $k = 3$ and any cube with

$$B \gg_\epsilon m^{\frac{1}{2}+\epsilon}.$$

6. Using Multiplicative Characters to Estimate N^*

We may assume that $a = 1$ and write (14),

$$x_1 \cdots x_k \equiv c - by_1 \cdots y_k \pmod{m}.$$

Let I_i, J_i be intervals as in (15). For any $A \in \mathbb{Z}_m^*$, let n_A denote the number of solutions of

$$y_1 \cdots y_k \equiv A \pmod{m},$$

with $y_i \in J_i$, $1 \leq i \leq k$, and n_{c-bA} the number of solutions of

$$x_1 \cdots x_k \equiv c - bA \pmod{m},$$

with $x_i \in I_i$, $1 \leq i \leq k$. Using the formula in (12) for n_A and n_{c-bA}, we have

$$\begin{aligned} N^* &= \sum_{\substack{A \in \mathbb{Z}_m^* \\ (c-bA,m)=1}} n_{c-bA} n_A \\ &= \sum_{\substack{A \in \mathbb{Z}_m^* \\ (c-bA,m)=1}} \frac{1}{\phi(m)} \sum_{x_i \in I_i} \sum_{\chi} \chi((c-bA)^{-1} x_1 \cdots x_k) \frac{1}{\phi(m)} \sum_{y_i \in J_i} \sum_{\psi} \psi(A^{-1} y_1 \cdots y_k) \\ &= \frac{1}{\phi(m)^2} \prod_{i=1}^{k} |I_i||J_i| \sum_{\substack{A \in \mathbb{Z}_m^* \\ (c-bA,m)=1}} 1 + E_1 + E_2 + E_3, \end{aligned} \tag{21}$$

say, where the three error terms are given by

$$E_1 := \frac{1}{\phi(m)^2} \sum_{\chi \neq \chi_0} \left(\sum_{\substack{A \in \mathbb{Z}_m^* \\ (c-bA,m)=1}} \chi((c-bA)^{-1}) \right) \sum_{x_i \in I_i} \chi(x_1 \cdots x_k) \sum_{y_i \in J_i} 1, \tag{22}$$

$$E_2 := \frac{1}{\phi(m)^2} \sum_{\psi \neq \chi_0} \left(\sum_{\substack{A \in \mathbb{Z}_m^* \\ (c-bA,m)=1}} \psi(A^{-1}) \right) \sum_{x_i \in I_i} 1 \sum_{y_i \in J_i} \psi(y_1 \cdots y_k), \tag{23}$$

$$E_3 := \frac{1}{\phi(m)^2} \sum_{\chi \neq \chi_0} \sum_{\psi \neq \chi_0} \left(\sum_{\substack{A \in \mathbb{Z}_m^* \\ (c-bA,m)=1}} \chi((c-bA)^{-1}) \psi(A^{-1}) \right) \tag{24}$$

$$\times \sum_{x_i \in I_i} \chi(x_1 \cdots x_k) \sum_{y_i \in J_i} \psi(y_1 \cdots y_k), \tag{25}$$

say.

6.1. Estimation of the Main Term

To estimate the main term we need,

Lemma 7. *For any integers b, c with $(bc, m) = 1$,*

$$\sum_{\substack{A\in\mathbb{Z}_m^*\\(c-bA,m)=1}} 1 = \phi(m)\prod_{p|m}\frac{p-2}{p-1}. \tag{26}$$

Proof. This is actually a special case of Lemma 10 below applied to the principal character, but let's give a quick proof here. The sum is plainly multiplicative in m, and for a prime power $m = p^e$, the sum just counts the number of $A \in \mathbb{Z}_m$ with $A \not\equiv 0, cb^{-1} \pmod p$, which equals $p^{e-1}(p-2) = \phi(p^e)\frac{p-2}{p-1}$. □

Thus the main term in (21) is just

$$\frac{\prod_{i=1}|I_i||J_i|}{\phi(m)}\prod_{p|m}\frac{p-2}{p-1}. \tag{27}$$

6.2. Estimation of E_1 and E_2

Let us first recall a couple of notions about multiplicative characters. For any multiplicative character $\chi \pmod m$ and divisor d of m, we say that χ is induced by a character $\pmod d$ (or simply χ is a character $\pmod d$) if whenever $x \equiv y \pmod d$, then $\chi(x) = \chi(y)$. Viewed as a character $\pmod d$ there is a slight difference in the definition of χ on values of x with $(x, d) = 1$ but $(x, m) \neq 1$. As a character $\pmod m$, $\chi(x) = 0$, but as a character $\pmod d$, $\chi(x) \neq 0$. This distinction is not a concern in what follows, for we will always restrict our attention to values of x with $(x, m) = 1$. There is a unique minimal divisor d such that χ is a character $\pmod d$, called the conductor of χ, written $\mathrm{cond}(\chi)$. For this d, χ is a primitive character $\pmod d$. For the principal character χ_0 we have $\mathrm{cond}(\chi_0) = 1$.

Lemma 8. *If $d|m$ and χ is a character $\pmod m$ that is not a character $\pmod d$, then there exists $u \equiv 1 \pmod d$, with $(u, m) = 1$ and $\chi(u) \neq 1$.*

Proof. Say m has prime power factorization $m = p_1^{e_1}p_2^{e_2}\cdots p_\ell^{e_\ell}$, for distinct primes p_i and exponents $e_i \geq 1$, $1 \leq i \leq \ell$. Then χ can be expressed $\chi = \chi_1\chi_2\cdots\chi_\ell$ for some characters $\chi_i \pmod{p^{e_i}}$. Say $d = p_1^{f_1}p_2^{f_2}\cdots p_\ell^{f_\ell}$ with $f_i \leq e_i$, $1 \leq i \leq \ell$. Since χ is not a character $\pmod d$, there exists an $i \leq \ell$ such that χ_i is not a character $\pmod{p_i^{f_i}}$. Let a_i be a primitive root $\pmod{p_i^{e_i}}$, and let j_i be the unique integer with $0 < j_i \leq p_i^{e_i-1}(p_i - 1)$ and

$$\chi_i(a_i) = e^{\frac{2\pi i j_i}{\phi(p_i^{e_i})}}.$$

Since χ_i is not a character $\pmod{p_i^{f_i}}$, then $p_i^{e_i-f_i} \nmid j_i$. Setting $u_0 = a_i^{\phi(p_i^{f_i})}$, we have $u_0 \equiv 1 \pmod{p_i^{f_i}}$ and

$$\chi_i(u_0) = \chi_i(a_i^{\phi(p_i^{f_i})}) = e^{\frac{2\pi i j_i\phi(p_i^{f_i})}{\phi(p_i^{e_i})}} = e^{\frac{2\pi i j_i}{p_i^{e_i-f_i}}} \neq 1,$$

since $p_i^{e_i-f_i} \nmid j_i$. By the Chinese Remainder Theorem, there exists an integer u with

$$u \equiv \begin{cases} u_0 \pmod{p_i^{e_i}}; \\ 1 \pmod{p_j^{e_j}}, \qquad \text{for } j \neq i. \end{cases}$$

Then $(u, m) = 1$, $u \equiv 1 \pmod{d}$ and $\chi(u) \neq 1$. □

Lemma 9. *For any character $\chi \pmod{m}$, integer c with $(c, m) = 1$ and divisor d of m we have*

$$\sum_{t=0}^{\frac{m}{d}-1} \chi(c+td) = \begin{cases} \chi(c)\ \frac{\phi(m)}{\phi(d)}, & \text{if } \chi \text{ is a character} \pmod{d}; \\ 0, & \text{if } \chi \text{ is not a character} \pmod{d}. \end{cases}$$

Proof. If χ is a character $\pmod{d}$ the claim is immediate, since there are $\phi(m)/\phi(d)$ choices for t such that $(c+td, m) = 1$. If χ is not a character $\pmod{d}$, then there exists $u \equiv 1 \pmod{d}$, with $(u, m) = 1$ and $\chi(u) \neq 1$ by the preceding lemma. Then

$$\sum_{t=0}^{\frac{m}{d}-1} \chi(c+td) = \sum_{t=0}^{\frac{m}{d}-1} \chi(u(c+td)) = \chi(u) \sum_{t=0}^{\frac{m}{d}-1} \chi(c+td),$$

and so the sum must be zero. □

Lemma 10. *For any multiplicative character $\chi \pmod{m}$ of conductor e and integer c with $(c, m) = 1$, we have*

$$\sum_{\substack{A \in \mathbb{Z}_m^* \\ (c-A,m)=1}} \chi(A) = \phi(m)\chi(c)\frac{\mu(e)}{\phi(e)} \prod_{\substack{p \mid \frac{m}{e} \\ p \nmid e}} \frac{p-2}{p-1}.$$

Proof. Now,

$$\begin{aligned} \sum_{\substack{A \in \mathbb{Z}_m^* \\ (c-A,m)=1}} \chi(A) &= \sum_{A \in \mathbb{Z}_m^*} \chi(A) \sum_{d \mid (c-A,m)} \mu(d) \\ &= \sum_{d \mid m} \mu(d) \sum_{A \equiv c \pmod{d}} \chi(A) \\ &= \sum_{d \mid m} \mu(d) \sum_{t=0}^{\frac{m}{d}-1} \chi(c+td). \end{aligned}$$

Thus letting e denote the conductor of χ, we get from the preceding lemma,

$$\sum_{\substack{A \in \mathbb{Z}_m^* \\ (c-A,m)=1}} \chi(A) = \phi(m)\chi(c) \sum_{\substack{d \mid m \\ e \mid d}} \frac{\mu(d)}{\phi(d)}$$

$$= \phi(m)\chi(c) \sum_{f \mid \frac{m}{e}} \frac{\mu(ef)}{\phi(ef)}.$$

Now, the only contribution to the sum over f comes from square-free values of ef. Thus if $(e,f)>1$ there is no contribution, and so we may assume $(e,f)=1$, whence $\mu(ef)=\mu(e)\mu(f)$ and $\phi(ef)=\phi(e)\phi(f)$. Thus

$$\sum_{\substack{A\in\mathbb{Z}_m^*\\(c-A,m)=1}}\chi(A)=\phi(m)\chi(c)\frac{\mu(e)}{\phi(e)}\sum_{\substack{f\mid\frac{m}{e}\\(f,e)=1}}\frac{\mu(f)}{\phi(f)}=\phi(m)\chi(c)\frac{\mu(e)}{\phi(e)}\prod_{\substack{p\mid\frac{m}{e}\\p\nmid e}}\frac{p-2}{p-1}.$$

□

Next we have to obtain character sum bounds over intervals with restricted variables. Again let I be an interval of points in $\mathbb{Z}_m^*$, $I=[a+1,a+B]\cap\mathbb{Z}_m^*$. First we obtain the following Burgess-type estimate.

Lemma 11. *For any $e|m$, positive integers B,r and non-principal character χ $\pmod e$, we have*

$$\Big|\sum_{\substack{x=a+1\\(x,m)=1}}^{a+B}\chi(x)\Big|\ll_\epsilon|I|^{1-\frac{1}{r}}m^\epsilon e^{\frac{r+1}{4r^2}}e_1^{\frac{3}{4r}},$$

where e_1 is the product of the prime-power divisors of e of multiplicity at least 3.

Proof. We have

$$\begin{aligned}\sum_{\substack{x=a+1\\(x,m)=1}}^{a+B}\chi(x)&=\sum_{x=a+1}^{a+B}\chi(x)\sum_{\lambda|(x,m)}\mu(\lambda)\\&=\sum_{\lambda|m}\mu(\lambda)\sum_{\substack{x=a+1\\\lambda|x}}^{a+B}\chi(x)\\&=\sum_{\lambda|m}\mu(\lambda)\chi(\lambda)\sum_{(a+1)/\lambda\le t\le(a+B)/\lambda}\chi(t).\end{aligned}\tag{28}$$

Then by the Burgess bound in (10),

$$\begin{aligned}\Big|\sum_{\substack{x=a+1\\(x,m)=1}}^{a+B}\chi(x)\Big|&\le\sum_{\lambda|m}\Big|\sum_{(a+1)/\lambda\le t\le(a+B)/\lambda}\chi(t)\Big|\\&\ll\sum_{\lambda|m}(B/\lambda+1)^{1-\frac{1}{r}}e^{\frac{r+1}{4r^2}+\epsilon}e_1^{\frac{3}{4r}}\\&\ll\tau(m)B^{1-\frac{1}{r}}e^{\frac{r+1}{4r^2}+\epsilon}e_1^{\frac{3}{4r}}.\end{aligned}$$

Replacing B with $|I|$ in the statement of the lemma now follows as in the proof of Lemma 4. □

Generalizing the result of Cochrane and Shi [8], we have

Lemma 12. *For any $e|m$, integer a and positive integer B we have*

$$\frac{1}{\phi(e)} \sum_{\substack{\chi (mod\ e) \\ \chi \neq \chi_0}} \Big| \sum_{\substack{x=a+1 \\ (x,m)=1}}^{a+B} \chi(x) \Big|^4 \ll_\epsilon |I|^2 m^\epsilon.$$

Proof. By (28), Hölder's inequality and then employing the upper bound in (4), we get

$$\begin{aligned}
\frac{1}{\phi(e)} \sum_{\substack{\chi (\mathrm{mod}\ e) \\ \chi \neq \chi_0}} \Big| \sum_{\substack{x=a+1 \\ (x,m)=1}}^{a+B} \chi(x) \Big|^4 &\leq \frac{1}{\phi(e)} \sum_{\substack{\chi (\mathrm{mod}\ e) \\ \chi \neq \chi_0}} \Big(\sum_{\lambda|m} \Big| \sum_{(a+1)/\lambda \leq t \leq (a+B)/\lambda} \chi(t) \Big| \Big)^4 \\
&\leq \tau(m)^3 \sum_{\lambda|m} \Big(\frac{1}{\phi(e)} \sum_{\substack{\chi (\mathrm{mod}\ e) \\ \chi \neq \chi_0}} \Big| \sum_{(a+1)/\lambda \leq t \leq (a+B)/\lambda} \chi(t) \Big|^4 \Big) \\
&\leq \tau(m)^3 \sum_{\lambda|m} 8^{\omega(e)} \tau(e) (\log e)^3 (\log\log e)^7 (B/\lambda + 1)^2 \\
&\ll \tau(m)^4 8^{\omega(m)} \tau(m) (\log m)^3 (\log\log m)^7 B^2 \ll_\epsilon B^2 m^\epsilon.
\end{aligned}$$

□

Lemma 13. *Suppose that $k \geq 4$. For any $e|m$, integer a and positive integers r, B we have*

$$\frac{1}{\phi(e)} \sum_{\substack{\chi (mod\ e) \\ \chi \neq \chi_0}} \Big| \sum_{\substack{x=a+1 \\ (x,m)=1}}^{a+B} \chi(x) \Big|^k \ll_\epsilon |I|^{k(1-\frac{1}{r})-2+\frac{4}{r}} e^{\frac{r+1}{4r^2}(k-4)} e_1^{\frac{3}{4r}(k-4)} m^\epsilon. \tag{29}$$

Proof. From the preceding two lemmas we have

$$\begin{aligned}
\frac{1}{\phi(e)} \sum_{\substack{\chi (\mathrm{mod}\ e) \\ \chi \neq \chi_0}} \Big| \sum_{\substack{x=a+1 \\ (x,m)=1}}^{a+B} \chi(x) \Big|^k &\leq \max_{\chi \neq \chi_0} \Big| \sum_{\substack{x=a+1 \\ (x,m)=1}}^{a+B} \chi(x) \Big|^{k-4} \frac{1}{\phi(e)} \sum_{\chi \neq \chi_0} \Big| \sum_{\substack{x=a+1 \\ (x,m)=1}}^{a+B} \chi(x) \Big|^4 \\
&\ll_\epsilon |I|^{k(1-\frac{1}{r})-2+\frac{4}{r}} e^{\frac{r+1}{4r^2}(k-4)} e_1^{\frac{3}{4r}(k-4)} m^\epsilon.
\end{aligned}$$

Again, replacing B with $|I|$ in the statement of the lemma follows as before. □

Turning to E_1 we have by Lemma 10, letting e_χ denote the conductor of χ, cond(χ),

$$
\begin{aligned}
E_1 := & \frac{1}{\phi(m)^2} \sum_{\chi \neq \chi_0} \left(\sum_{\substack{A \in \mathbb{Z}_m^* \\ (c-bA,m)=1}} \chi((c-bA)^{-1}) \right) \sum_{x_i \in I_i} \chi(x_1 \cdots x_k) \sum_{y_i \in J_i} 1 \\
= & \frac{1}{\phi(m)^2} \sum_{\chi \neq \chi_0} \phi(m)\chi(c^{-1}) \frac{\mu(e_\chi)}{\phi(e_\chi)} \prod_{\substack{p \mid \frac{m}{e_\chi} \\ p \nmid e_\chi}} \frac{p-2}{p-1} \sum_{x_i \in I_i} \chi(x_1 \cdots x_k) \sum_{y_i \in J_i} 1 \\
= & \frac{\prod_{i=1}^k |J_i|}{\phi(m)} \sum_{\substack{e \mid m \\ e>1}} \frac{\mu(e)}{\phi(e)} \prod_{\substack{p \mid m/e \\ p \nmid e}} \tfrac{p-2}{p-1} \sum_{\substack{\chi \pmod e \\ \mathrm{cond}(\chi)=e}} \chi(c^{-1}) \sum_{x_i \in I_i} \chi(x_1 \cdots x_k).
\end{aligned}
$$

Thus, by Holder's inequality and the preceding lemma,

$$
\begin{aligned}
|E_1| \ll & \frac{\prod_{i=1}^k |J_i|}{\phi(m)} \sum_{\substack{e \mid m \\ e>1}} \prod_{i=1}^k |I_i|^{1-\frac{1}{r}-\frac{2}{k}+\frac{4}{kr}} e^{\frac{r+1}{4r^2}(k-4)} e_1^{\frac{3}{4r}(k-4)} m^{\epsilon} \\
\ll & \frac{\prod_{i=1}^k |J_i|}{\phi(m)} \prod_{i=1}^k |I_i|^{1-\frac{1}{r}-\frac{2}{k}+\frac{4}{kr}} m^{\frac{r+1}{4r^2}(k-4)+\epsilon} m_1^{\frac{3}{4r}(k-4)}.
\end{aligned}
$$

In a similar manner we obtain the following upper bound for $|E_2|$,

$$
|E_2| \ll \frac{\prod_{i=1}^k |I_i|}{\phi(m)} \prod_{i=1}^k |J_i|^{1-\frac{1}{r}-\frac{2}{k}+\frac{4}{kr}} m^{\frac{r+1}{4r^2}(k-4)+\epsilon} m_1^{\frac{3}{4r}(k-4)}. \tag{30}
$$

6.3. Estimation of E_3

Lemma 14. *For any multiplicative characters $\chi, \psi \pmod m$ and integers c, A with $(c, m) = 1$ we have,*

$$
\left| \sum_{\substack{A \in \mathbb{Z}_m^* \\ (c-A,m)=1}} \chi(A)\psi((c-A)^{-1}) \right| \leq \frac{m}{\sqrt{[cond(\chi), cond(\psi)]}},
$$

where $[cond(\chi), cond(\psi)]$ denotes the least common multiple of the conductors of χ and ψ.

Proof. We first consider the case of a prime power $m = p^e$. Let a be a primitive root $\pmod{p^e}$ and α be the generator of the character group defined by

$$
\alpha(a^j) = e^{\frac{2\pi i j}{\phi(p^e)}}.
$$

For any rational function $q = q(x) = f(x)/g(x)$ with integer coefficients, we define the character sum

$$S_{p^e}(q) = \sum_{\substack{x=1 \\ (f(x)g(x),p)=1}}^{p^e} \alpha(q(x)),$$

where it is understood that $1/g(x)$ means the multiplicative inverse of $g(x) \pmod{p^e}$. Following the method of critical points developed in [9], [10] and [6], we define t to be the maximum power of p dividing all of the coefficients of $g(x)f'(x) - g'(x)f(x)$, and the critical point congruence to be the congruence

$$p^{-t}(g(x)f'(x) - g'(x)f(x)) \equiv 0 \pmod{p}. \tag{31}$$

The *critical points* are the solutions x of the congruence (31) with $p \nmid f(x)g(x)$. By [6, Theorem 1.1], if $e \geq t+2$ and (31) has a unique critical point of multiplicity 1 then $|S_{p^e}(q)| = p^{\frac{e+t}{2}}$. If $e \geq t+2$ and there is no critical point, then $S_{p^e}(q) = 0$. We claim that one of these two options always occurs for the case at hand.

Let χ, ψ be characters $\pmod{p^e}$ and say $\chi = \alpha^u, \psi = \alpha^v$, for some positive integers $u, v \leq \phi(p^e)$. Then

$$\chi(x)\psi((c-x)^{-1}) = \alpha\left(\frac{x^u}{(c-x)^v}\right).$$

With $q(x) = \frac{x^u}{(c-x)^v}$ we have

$$\begin{aligned} g(x)f'(x) - g'(x)f(x) &= ux^{u-1}(c-x)^v + vx^u(c-x)^{v-1} \\ &= x^{u-1}(c-x)^{v-1}(uc + (v-u)x), \end{aligned}$$

and so $p^t \| (u,v)$, and so there is either no critical point or a single critical point of multiplicity one. Thus, if $t \leq e-2$ then

$$\left|\sum_{\substack{x=1 \\ p \nmid x(c-x)}}^{p^e} \chi(x)\psi((c-x)^{-1})\right| = |S_{p^e}(q)| \leq p^{\frac{e+t}{2}}.$$

Otherwise, $t = e-1$. In this case, both χ and ψ are characters $\pmod{p}$ and we have by the Weil bound [22] for character sums over finite fields (see eg. [7]) that

$$\left|\sum_{\substack{x=1 \\ p \nmid x(c-x)}}^{p^e} \chi(x)\psi((c-x)^{-1})\right| = p^{e-1}\left|\sum_{\substack{x=1 \\ p \nmid x(c-x)}}^{p} \alpha\left(\frac{x^u}{(c-x)^v}\right)\right| \leq p^{e-1}\sqrt{p} = p^{\frac{e+t}{2}}.$$

Suppose that $p^{t_1} \| u$, $p^{t_2} \| v$. Then $\mathrm{cond}(\chi) = p^{e-t_1}$ while $\mathrm{cond}(\psi) = p^{e-t_2}$, and we see that

$$[\mathrm{cond}(\chi), \mathrm{cond}(\psi)] = p^{e-\min(t_1,t_2)} = p^{e-t},$$

and
$$p^{\frac{e+t}{2}} = \frac{p^e}{\sqrt{p^{e-t}}} = \frac{p^e}{\sqrt{[\mathrm{cond}(\chi), \mathrm{cond}(\psi)]}}.$$

For general m we write $m = p_1^{e_1} p_2^{e_2} \cdots p_\ell^{e_\ell}$ with the p_i distinct primes,
$$\chi = \chi_1 \chi_2 \cdots \chi_\ell,\ \ \psi = \psi_1 \psi_2 \cdots \psi_\ell,$$
with χ_i, ψ_i characters $\pmod{p_i^{e_i}}$, and
$$S_m(q) = \prod_{i=1}^{\ell} S_{p_i^{e_i}}(A_i q),$$
for appropriate integers A_i with $(A_i, p_i) = 1$. Then
$$|S_m(q)| \leq \prod_{i=1}^{\ell} \frac{p_i^{e_i}}{\sqrt{[cond(\chi_i), cond(\psi_i)]}} = \frac{m}{\sqrt{[cond(\chi), cond(\psi)]}}.$$

□

From the preceding lemma we have,
$$E_3 := \frac{1}{\phi(m)^2} \sum_{\chi \neq \chi_0} \sum_{\psi \neq \chi_0} \left(\sum_{\substack{A \in \mathbb{Z}_m^* \\ (c-bA,m)=1}} \chi((c-bA)^{-1}) \psi(A^{-1}) \right) \times \sum_{x_i \in I_i} \chi(x_1 \cdots x_k) \sum_{y_i \in J_i} \psi(y_1 \cdots y_k).$$

Thus,
$$\begin{aligned} |E_3| &\leq \frac{1}{\phi(m)^2} \sum_{\substack{d|m \\ d>1}} \sum_{\substack{e|m \\ e>1}} \frac{m}{\sqrt{[e,d]}} \sum_{\substack{\chi \\ \mathrm{cond}(\chi)=d}} \sum_{\substack{\psi \\ \mathrm{cond}(\psi)=e}} \left| \sum_{x_i \in I_i} \chi(x_1 \cdots x_k) \sum_{y_i \in J_i} \psi(y_1 \cdots y_k) \right| \\ &\leq \frac{m}{\phi(m)^2} \sum_{\substack{d|m \\ d>1}} \sum_{\substack{e|m \\ e>1}} \frac{\phi(d)\phi(e)}{\sqrt{[e,d]}} \\ &\qquad \times \frac{1}{\phi(d)} \sum_{\substack{\chi \\ \mathrm{cond}(\chi)=d}} \left| \sum_{x_i \in I_i} \chi(x_1 \cdots x_k) \right| \frac{1}{\phi(e)} \sum_{\substack{\psi \\ \mathrm{cond}(\psi)=e}} \left| \sum_{y_i \in J_i} \psi(y_1 \cdots y_k) \right| \\ &\leq \frac{m}{\phi(m)^2} \sum_{\substack{d|m \\ d>1}} \sum_{\substack{e|m \\ e>1}} \frac{\phi(d)\phi(e)}{\sqrt{[e,d]}} \\ &\qquad \times \frac{1}{\phi(d)} \sum_{\substack{\chi (\mathrm{mod}\ \mathrm{d}) \\ \chi \neq \chi_0}} \left| \sum_{x_i \in I_i} \chi(x_1 \cdots x_k) \right| \frac{1}{\phi(e)} \sum_{\substack{\psi (\mathrm{mod}\ \mathrm{e}) \\ \psi \neq \chi_0}} \left| \sum_{y_i \in J_i} \psi(y_1 \cdots y_k) \right| \end{aligned}$$

Letting $L = [d, e]$ and applying Lemma 13 we obtain

$$|E_3| \ll \frac{m}{\phi(m)^2} (\prod_{i=1} |I_i||J_i|)^{(1-\frac{1}{r})-\frac{2}{k}+\frac{4}{kr}} \sum_{L|m} \frac{1}{\sqrt{L}} \left(\sum_{d|L} \phi(d) d^{\frac{r+1}{4r^2}(k-4)} d_1^{\frac{3}{4r}(k-4)} \right)^2 m^{\epsilon}$$

$$\ll \sqrt{m}\ (\prod_{i=1} |I_i||J_i|)^{(1-\frac{1}{r})-\frac{2}{k}+\frac{4}{kr}} m^{\frac{r+1}{2r^2}(k-4)+\epsilon} m_1^{\frac{3}{2r}(k-4)}.$$

6.4. Proof of Theorem 2

From equation (21), the value for the main term in (27) and the estimates for the error terms E_1, E_2 and E_3 in the preceding sections we see that

$$N^* = \frac{\prod_{i=1} |I_i||J_i|}{\phi(m)} \prod_{p|m} \frac{p-2}{p-1} + O\left(\sqrt{m}\ (\prod_{i=1} |I_i||J_i|)^{(1-\frac{1}{r})-\frac{2}{k}+\frac{4}{kr}} m^{\frac{r+1}{2r^2}(k-4)+\epsilon} m_1^{\frac{3}{2r}(k-4)} \right)$$
$$+ O\left(\frac{\prod_{i=1}^k |I_i|}{\phi(m)} \prod_{i=1}^k |J_i|^{(1-\frac{1}{r})-\frac{2}{k}+\frac{4}{kr}} m^{\frac{r+1}{4r^2}(k-4)+\epsilon} m_1^{\frac{3}{4r}(k-4)} \right)$$
$$+ O\left(\frac{\prod_{i=1}^k |J_i|}{\phi(m)} \prod_{i=1}^k |I_i|^{(1-\frac{1}{r})-\frac{2}{k}+\frac{4}{kr}} m^{\frac{r+1}{4r^2}(k-4)+\epsilon} m_1^{\frac{3}{4r}(k-4)} \right).$$

References

[1] A. Ayyad, The distribution of solutions of the congruence $x_1x_2\cdots x_n \equiv c \pmod p$, *Proc. Amer. Math. Soc.* **127** (1999), no. 4, 943-950.

[2] 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.

[3] 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.

[4] D. A. Burgess, On character sums and L-series I, *Proc. London Math. Soc.* **12** (1962), no. 2, 193-206.

[5] D. A. Burgess, On character sums and L-series II, *Proc. London Math. Soc.* **13** (1963), no. 3, 524-536.

[6] T. Cochrane, Exponential sums modulo prime powers, *Acta Arith.* **101** (2002), no. 2, 131-149.

[7] T. Cochrane and C. Pinner, Using Stepanov's method for exponential sums involving rational functions, *J. Number Theory* **116** (2006), no. 2, 270-292.

[8] 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** no. 3 (2010), 767-785.

[9] T. Cochrane and Z. Zheng, Pure and mixed exponential sums, *Acta Arith.* **91** (1999), no. 3, 249-278.

[10] T. Cochrane and Z. Zheng, Exponential sums with rational function entries, *Acta Arith.* **95** (2000), no. 1, 67-95.

[11] M. Z. Garaev, On multiplicative congruences, *Math. Zeit.* **272** (2012), 473-482.

[12] G. Harman and I. E. Shparlinski, Products of small integers in residue classes and additive properties of Fermat quotients, *Int. Math. Res. Not. IMRN* 2016, no. 5, 1424-1446.

[13] 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.

[14] H. Iwaniec and E. Kowalski, *Analytic number theory*, American Mathematical Society Colloquium Publications, 53. American Mathematical Society, Providence, RI, 2004.

[15] M. R. Khan and I. E. Shparlinski, On the maximal difference between an element and its inverse modulo n, *Period. Math. Hungar.* **47** (2003), no. 1-2, 111-117.

[16] K. K. Norton, Upper Bounds for Sums of Powers of Divisor Functions, *J. Number Theory* **40** (1992), 65-85.

[17] K. K. Norton, A character-sum estimate and applications, *Acta Arith.* **85** (1998), no. 1, 51-78.

[18] G. Robin, Estimate of the Chebyshev function θ 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.

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

[20] I. E. Shparlinski, On the distribution of points on multidimensional modular hyperbolas, *Proc. Japan Acad.* **83** (2007), Ser. A, 5-9.

[21] I. E. Shparlinski, Modular Hyperbolas, *Japanese J. Math.* **7** (2012) no. 2, 235-294.

[22] A. Weil, On some exponential sums, *Proc. Nat. Acad. Sci.* **34** (1948), 204-207.

[23] W. Zhang, On the distribution of inverses modulo n, *J. Number Theory* **61** (1996), no. 2, 301-310.