PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 144, Number 7, July 2016, Pages 2837–2846
http://dx.doi.org/10.1090/proc/12949
Article electronically published on January 20, 2016

LINEAR CONGRUENCES WITH RATIOS

IGOR E. SHPARLINSKI

(Communicated by Matthew A. Papanikolas)

Abstract. We use new bounds of double exponential sums with ratios of integers from prescribed intervals to get an asymptotic formula for the number of solutions to congruences

$$\sum_{j=1}^{n} a_j \frac{x_j}{y_j} \equiv a_0 \pmod p,$$

with variables from rather general sets.

1. Introduction

1.1. **Motivation.** We count the number of solutions to a linear congruence with rational variables with restricted numerators and denominators. This includes solutions with rationals of a bounded height or more generally with numerators and denominators from a certain large class of sets with a regular boundary. For example, this class of sets includes all convex sets. In some special cases, the corresponding equation over $\mathbb{Q}$ has recently been considered by Blomer and Brüdern [2] and also by Blomer, Brüdern and Salberger [3]. However, in positive characteristic this natural question has never been studied before.

More precisely, for a prime p we consider the equation

$$\sum_{j=1}^{n} a_j \frac{x_j}{y_j} = a_0, \tag{1}$$

with coefficients $\mathbf{a} = (a_0, a_1, \ldots, a_n) \in \mathbb{F}_p^{n+1}$ and variables

$$\mathbf{x} = (x_1, \ldots, x_n),\ \mathbf{y} = (y_1, \ldots, y_n) \in \mathbb{F}_p^n,$$

where $\mathbb{F}_p$ denotes the finite fields of p elements.

Given a set $\mathcal{S} \subseteq [0, p-1]^{2n}$, we use $N(\mathbf{a}; \mathcal{S})$ to denote the number of solutions to the equation (1) with variables $(x_1, y_1, \ldots, x_n, y_n) \in \mathcal{S}$.

The equation (1) can be considered over the integers. In particular, recently Blomer, Brüdern and Salberger [3] have studied it for $n = 3$, $a_0 = 0$ and $a_1 = a_2 = a_3 = 1$. In particular, by [3, Theorem 1], the number of integer solutions with $(\mathbf{x}, \mathbf{y}) \in [-H, H]^6$ to the analogue of (1) with variables over $\mathbb{Z}$ is given by $H^3 Q(H) + O(H^{3-\delta})$, where $Q \in \mathbb{Q}[X]$ is a polynomial of degree 4 and $\delta > 0$ is some absolute constant. Blomer and Brüdern [2] have also suggested an alternative approach which yields a tight upper bound for the same equation but for a slightly

Received by the editors March 26, 2015 and, in revised form, September 4, 2015.
2010 *Mathematics Subject Classification.* Primary 11D79, 11L07.
Key words and phrases. Linear congruences, exponential sums.
This work was supported in part by ARC Grant DP140100118.

different way of ordering and counting solutions. The methods of [2,3] can probably be extended to arbitrary n (see, for example, the comment in [3, Section 1.3]).

In [15], a different approach has been suggested, which is based on some arguments from [13] and leads to bounds that are weaker by a logarithmic factor than those expected to be produced by the methods of [2, 3]; however it seems to be more robust and is able to work in more general situations.

Here we combine some ideas from [13] with several other arguments and apply them to the case of the equation (1) over a finite field.

Throughout the paper, any implied constants in the symbols O, $\ll$ and $\gg$ may depend on the integer parameter $n \geq 1$. We recall that the notation $U = O(V)$, $U \ll V$ and $V \gg U$ are all equivalent to the statement that the inequality $|U| \leq cV$ holds with some constant $c > 0$.

1.2. **Solutions in boxes.** We fix some intervals

$$\mathcal{I}_j = [A_j + 1, A_j + K_j],\ \mathcal{J}_j = [B_j + 1, B_j + L_j] \subseteq [0, p-1], \tag{2}$$

with integers A_j, B_j, K_j and L_j, $j = 1, \ldots, n$, and obtain the following asymptotic formula.

Theorem 1. *For $n \geq 3$ and arbitrary intervals* (2) *for the box $\mathcal{B} = \mathcal{I}_1 \times \mathcal{J}_1 \times \ldots \times \mathcal{I}_n \times \mathcal{J}_n$ we have*

$$\left| N(\mathbf{a}; \mathcal{B}) - \frac{1}{p} \prod_{j=1}^{n} (K_j L_j) \right| \leq \sqrt{K_1 L_1 K_2 L_2} \prod_{j=3}^{n} (K_j + \sqrt{p L_j}) p^{o(1)}.$$

We now consider the case when $\mathcal{B}$ is a cube with the side length H.

Corollary 2. *For $n \geq 3$ and intervals* (2) *with $K_j = L_j = H$, $j = 1, \ldots, n$, for the cubic box $\mathcal{C} = \mathcal{I}_1 \times \mathcal{J}_1 \times \ldots \times \mathcal{I}_n \times \mathcal{J}_n$ we have*

$$\left| N(\mathbf{a}; \mathcal{C}) - \frac{H^{2n}}{p} \right| \leq p^{n/2-1+o(1)} H^{n/2+1}.$$

In particular, the asymptotic formula of Corollary 2 is nontrivial starting from the values of H of order $p^{n/(3n-2)+\delta}$ for any fixed $\delta > 0$ and sufficiently large p. We also record the following result which is convenient for further applications.

For a set $\Omega \subseteq [0,1]^{2n}$ we use $p\Omega$ to denote its blowup by p, that is,

$$p\Omega = \{p\boldsymbol{\omega} \ : \ \boldsymbol{\omega} \in \Omega\}.$$

Rounding up and down the sides of $p\Gamma$ for a cubic box

$$\Gamma = [\alpha_1, \alpha_1 + \xi] \times [\beta_1, \beta_1 + \xi] \times \ldots \times [\alpha_n, \alpha_n + \xi] \times [\beta_n, \beta_n + \xi] \in [0,1]^{2n}, \tag{3}$$

we derive

Corollary 3. *For $n \geq 3$ and a cubic box* (3) *with $\xi > 1/p$ we have*

$$\left| N(\mathbf{a}; p\Gamma) - \xi^{2n} p^{2n-1} \right| \leq \left(\xi^{2n-1} p^{2n-2} + \xi^{n/2+1} p^n \right) p^{o(1)}.$$

1.3. **Solutions in well-shaped sets.** We combine Corollary 2 with some ideas of Schmidt [12] to get an asymptotic formula for $N(\mathbf{a};\Omega)$ for a rather general class of sets, which includes all convex sets.

First we need to introduce some definitions. We define the *distance* between a vector $\boldsymbol{\alpha} \in [0,1]^m$ and a set $\Xi \subseteq [0,1]^m$ by

$$\operatorname{dist}(\boldsymbol{\alpha}, \Xi) = \inf_{\boldsymbol{\beta} \in \Xi} \|\boldsymbol{\alpha} - \boldsymbol{\beta}\|,$$

where $\|\boldsymbol{\gamma}\|$ denotes the *Euclidean norm* of $\boldsymbol{\gamma}$. Given $\varepsilon > 0$ and a set $\Xi \subseteq [0,1]^m$, we define the sets

$$\Xi_\varepsilon^+ = \{\boldsymbol{\alpha} \in [0,1]^m \backslash \Xi \ : \ \operatorname{dist}(\boldsymbol{\alpha}, \Xi) < \varepsilon\}$$

and

$$\Xi_\varepsilon^- = \{\boldsymbol{\alpha} \in \Xi \ : \ \operatorname{dist}(\boldsymbol{\alpha}, [0,1]^m \backslash \Xi) < \varepsilon\}.$$

We note that in the definition of Ξ_ε^+ we discard the part of the outer ε-neighbourhood that does not belong to $[0,1]^m$. These parts can also be included in Ξ_ε^+ but this does not affect our argument as we work only with inner ε-neighbourhoods Ξ_ε^- and $([0,1]^m \backslash \Xi)_\varepsilon^- = \Xi_\varepsilon^+$.

Following [15] (see also [9, 10]), we say that a set Ξ is *well-shaped* if for every $\varepsilon > 0$ the *Lebesgue measures* $\mu(\Xi_\varepsilon^-)$ and $\mu(\Xi_\varepsilon^+)$ exist, for some constant C, and satisfy

$$\mu\left(\Xi_\varepsilon^\pm\right) \le C\varepsilon. \tag{4}$$

As we have mentioned, all convex sets are well-shaped.

Theorem 4. *For $n \ge 3$ and an arbitrary well-shaped set $\Omega \subseteq [0,1]^{2n}$ of Lebesgue measure $\mu(\Omega)$, we have*

$$\left|N(\mathbf{a}; p\Omega) - p^{2n-1}\mu(\Omega)\right| \le p^{2n-(5n-4)/(3n-2)+o(1)}.$$

2. Preliminaries

2.1. **Multiplicative congruences.** We recall the following special case of a result of Ayyad, Cochrane and Zheng [1, Theorem 1].

Lemma 5. *Let $\mathcal{I}_j, \mathcal{J}_j$, $j = 1,2$, be four intervals of the form* (2). *Then*

$$x_1 y_2 \equiv x_2 y_1 \pmod p, \quad x_i \in \mathcal{I}_i,\ y_i \in \mathcal{J}_i,\ i = 1,2,$$

has $K_1K_2L_1L_2/p + O\left(\sqrt{K_1K_2L_1L_2}\,p^{o(1)}\right)$ solutions.

We also need a version of the result of Cilleruelo and Garaev [5, Theorem 1].

Lemma 6. *For any integers B, L and M with $0 \le L, M < p$, the congruence*

$$(B+y)z \equiv 1 \pmod p, \qquad 1 \le y \le L,\ 1 \le z \le M,$$

has at most $p^{-1/2+o(1)}L^{1/2}M + p^{o(1)}$ solutions.

Proof. As in the proof of [5, Theorem 1] we note that by the Dirichlet principle, for any positive integers $U < p$ and V with $UV \ge p$ one can choose integers u and v with

$$1 \le u \le U, \qquad |v| = O(V), \qquad uB \equiv v \pmod p$$

(see also [6, Lemma 3.2] for a more general statement). With this choice of u and v the above congruence can be written as

$$vz + uyz \equiv u \pmod p.$$

We now take $U = \lceil (p/L)^{1/2} \rceil$ and $V = \lceil (pL)^{1/2} \rceil$ (thus $UV \ge p$).

Since the left hand side is at most $O(MV + LMU) = O((pL)^{1/2}M)$, we see that for every solution (y, z) we have

$$vz + uyz = u + kp \tag{5}$$

with some integer $k = O\left((pL)^{1/2}M/p\right) = O\left(p^{-1/2}L^{1/2}M\right)$.

We now recall the well-known bound

$$\tau(m) \le m^{o(1)}$$

on the number of integer positive divisors $\tau(m)$ of an integer $m \ne 0$; see, for example, [7, Theorem 317]. Since by (5) we have the divisibility $z \mid |u + kp|$ and also $0 < |u + kp| = O(p^2)$, we conclude that for each of the $O\left(p^{-1/2}L^{1/2}M + 1\right)$ possible values of k, there are at most $p^{o(1)}$ possible values for z, and thus for y. The result now follows. □

2.2. **Exponential sums with ratios.** For a prime p, we denote $\mathbf{e}_p(z) = \exp(2\pi i z/p)$. Clearly for $p \nmid u$ the expression $\mathbf{e}_p(av/u)$ is correctly defined (as $\mathbf{e}_p(aw)$ for $w \equiv v/u \pmod p$).

Let

$$\mathcal{I} = [A + 1, A + K], \ \mathcal{J} = [B + 1, B + L] \subseteq [0, p - 1] \tag{6}$$

be two intervals with integers A, B, K and L.

The following result is a variation of [13, Lemma 3]. We present it in the slightly more general form that we need for our applications.

Lemma 7. *Let $\mathcal{I}$ and $\mathcal{J}$ be two intervals of the form* (6) *and let $\mathcal{W} \subseteq \mathcal{I} \times \mathcal{J}$ be an arbitrary convex set. Then uniformly over the integers a with* $\gcd(a, p) = 1$, *we have*

$$\sum_{(x,y)\in\mathcal{W}} \mathbf{e}_p(ax/y) \ll (K + p^{1/2}L^{1/2})p^{o(1)},$$

where the summation is over all integral points $(x, y) \in \mathcal{W}$.

Proof. Since $\mathcal{W}$ is convex, for each y there are integers $K \ge K_y > H_y \ge 1$ such that

$$\sum_{(x,y)\in\mathcal{W}} \mathbf{e}_p(ax/y) = \sum_{y\in\mathcal{J}} \sum_{x=A+H_y}^{A+K_y} \mathbf{e}_p(ax/y).$$

Following the proof of [13, Lemma 3], we define

$$I = \lfloor \log(2p/K) \rfloor \qquad \text{and} \qquad J = \lfloor \log(2p) \rfloor .$$

Furthermore, for a rational number $\alpha = u/v$ with $\gcd(v, p) = 1$, we denote by $\rho(\alpha)$ the unique integer w with $w \equiv u/v \pmod p$ and $|w| < p/2$ (we can assume that $p \ge 3$). Using the bound

$$\sum_{x=A+H_y}^{A+K_y} \mathbf{e}_p(\alpha x) \ll \min\left\{K, \frac{p}{|\rho(\alpha)|}\right\},$$

which holds for any rational α with the denominator that is not a multiple of p (see [8, Bound (8.6)]), we obtain a version of [13, Equation (1)],

$$\sum_{(x,y)\in\mathcal{W}} \mathbf{e}_p(ax/y) \ll KR + p \sum_{j=I+1}^{J} T_j e^{-j}, \tag{7}$$

where

$$R = \#\left\{y \ : \ B+1 \le y \le B+L, \ |\rho(a/y)| < e^I\right\},$$
$$T_j = \#\left\{y \ : \ B+1 \le y \le B+L, \ e^j \le |\rho(a/y)| < e^{j+1}\right\}.$$

We now see that Lemma 6 implies the bounds

$$R \le p^{-1/2+o(1)} L^{1/2} e^I + p^{o(1)} \le p^{1/2+o(1)} L^{1/2} K^{-1} + p^{o(1)}$$

and

$$T_j \le p^{-1/2+o(1)} L^{1/2} e^j + p^{o(1)}.$$

Substituting these bounds in (7), we obtain

$$\begin{aligned}
&\left|\sum_{(x,y)\in\mathcal{W}} \mathbf{e}_p(ax/y)\right| \\
&\qquad \ll p^{1/2+o(1)} L^{1/2} + K p^{o(1)} + p \sum_{j=I+1}^{J} \left(p^{-1/2+o(1)} L^{1/2} e^j + p^{o(1)}\right) e^{-j} \\
&\qquad = p^{1/2+o(1)} L^{1/2} + K p^{o(1)} + J p^{1/2+o(1)} L^{1/2} + p^{1+o(1)} e^{-I} \\
&\qquad = p^{1/2+o(1)} L^{1/2} + K p^{o(1)},
\end{aligned}$$

which concludes the proof. □

We also need a version of Lemma 7 on average over a.

Lemma 8. *Let $\mathcal{I}$ and $\mathcal{J}$ be two intervals of the form* (6)*. Then we have*

$$\sum_{a=1}^{p-1} \left|\sum_{x\in\mathcal{I}} \sum_{y\in\mathcal{J}} \mathbf{e}_p(ax/y)\right|^2 \le KLp^{1+o(1)}.$$

Proof. First we write

$$\sum_{a=1}^{p-1} \left|\sum_{x\in\mathcal{I}} \sum_{y\in\mathcal{J}} \mathbf{e}_p(ax/y)\right|^2 = \sum_{a=0}^{p-1} \left|\sum_{x\in\mathcal{I}} \sum_{y\in\mathcal{J}} \mathbf{e}_p(ax/y)\right|^2 - K^2L^2. \tag{8}$$

Expanding the square of the inner sum on the right hand side of (8), changing the order of summations and using the orthogonality of characters, we obtain

$$\sum_{a=0}^{p-1} \left|\sum_{x\in\mathcal{I}} \sum_{y\in\mathcal{J}} \mathbf{e}_p(ax/y)\right|^2 = \sum_{x_1,x_2\in\mathcal{I}} \sum_{y_1,y_2\in\mathcal{J}} \sum_{a=0}^{p-1} \mathbf{e}_p(a(x_1/y_1 - x_2/y_2)) = pT,$$

where T is the number of solutions to the congruence

$$x_1/y_1 \equiv x_2/y_2 \pmod{p}, \qquad x_1, x_2 \in \mathcal{I}, y_1, y_2 \in \mathcal{J}. \tag{9}$$

Extending the admissible region of solutions to $\mathcal{I} \times \mathcal{J}$ and evoking Lemma 5, we conclude that

$$T = \frac{K^2L^2}{p} + O\left(KLp^{o(1)}\right),$$

which together with (8) completes the proof. □

3. Proofs of the main results

3.1. **Proof of Theorem 1.** Using the orthogonality of the exponential function, we write

$$N(\mathbf{a};\mathcal{B}) = \sum_{(x_1,y_1,\ldots,x_n,y_n)\in\mathcal{B}} \cdots \sum \frac{1}{p}\sum_{\lambda=0}^{p-1} \mathbf{e}_p\left(\lambda\left(\sum_{j=1}^{n} a_j\frac{x_j}{y_j} - a_0\right)\right).$$

Changing the order of summation, and recalling that $\mathcal{B}$ is a direct product of the intervals $\mathcal{I}_j$ and $\mathcal{J}_j$, $j=1,\ldots,n$, we obtain

$$N(\mathbf{a};\mathcal{B}) = \frac{1}{p}\sum_{\lambda=0}^{p-1} \mathbf{e}_p\left(-\lambda a_0\right)\prod_{j=1}^{n}\sum_{x_j\in\mathcal{I}_j}\sum_{y_j\in\mathcal{J}_j} \mathbf{e}_p\left(\lambda a_j x_j/y_j\right).$$

Now, the contribution from $\lambda=0$ gives the main term

$$\frac{1}{p}\prod_{j=1}^{n}\sum_{x_j\in\mathcal{I}_j}\sum_{y_j\in\mathcal{J}_j} 1 = \frac{1}{p}\prod_{j=1}^{n}(K_jL_j).$$

To estimate the error term, we apply Lemma 7 to $n-2$ sums with $j=3,\ldots,n$, getting

$$N(\mathbf{a};\mathcal{B}) - \frac{1}{p}\prod_{j=1}^{n}(K_jL_j) \le p^{-1+o(1)}\prod_{j=3}^{n}(K_j + p^{1/2}L_j^{1/2})W, \tag{10}$$

where

$$W = \sum_{\lambda=1}^{p-1}\left|\sum_{x_1\in\mathcal{I}_1}\sum_{y_1\in\mathcal{J}_1} \mathbf{e}_p\left(\lambda a_1x_1/y_1\right)\right|\left|\sum_{x_2\in\mathcal{I}_2}\sum_{y_2\in\mathcal{J}_2} \mathbf{e}_p\left(\lambda a_2x_2/y_2\right)\right|.$$

Hence, by the Cauchy inequality,

$$W \le \sqrt{W_1W_2}, \tag{11}$$

where, for $\nu=1,2$,

$$W_\nu = \sum_{\lambda=1}^{p-1}\left|\sum_{x_\nu\in\mathcal{I}_\nu}\sum_{y_\nu\in\mathcal{J}_\nu} \mathbf{e}_p\left(\lambda a_\nu x_\nu/y_\nu\right)\right|^2 = \sum_{a=1}^{p-1}\left|\sum_{x_\nu\in\mathcal{I}_\nu}\sum_{y_\nu\in\mathcal{J}_\nu} \mathbf{e}_p\left(a x_\nu/y_\nu\right)\right|^2.$$

We now apply Lemma 8 to estimate W_1 and W_2 and see from (11) that

$$W \le \sqrt{K_1L_1K_2L_2}\,p^{1+o(1)},$$

which together with (10) concludes the proof.

3.2. **Proof of Corollaries 2 and 3.** For Corollary 2, we see that the first term appearing in the bound of Theorem 1 is H^2 while each term in the product becomes $O(p^{1/2}H^{1/2})$. The result now follows.

For Corollary 3, we approximate the set $p\Gamma$ by two cubes with side lengths $\lfloor \xi p\rfloor$ and $\lceil \xi p\rceil$. Since $\xi > 1/p$, we have $(\xi p + O(1))^{2n} = (\xi p)^{2n} + O\left((\xi p)^{2n-1}\right)$. The result now follows from Corollary 2.

3.3. **Proof of Theorem 4.** The proof follows the arguments of the proofs of [10, Theorem 1] or [14, Theorem 3.1] (however the concrete details are different).

First we observe that since the complementary set $[0,1]^{2n}\setminus\Omega$ is also well-shaped, it is enough to establish only the lower bound

$$N(\mathbf{a};p\Omega) \ge \frac{N(p\Omega)}{p} + O\left(p^{2n-4/3+o(1)}\right). \tag{12}$$

We now recall some constructions and arguments from the proof of [12, Theorem 2]. Pick a point $\boldsymbol{\alpha} = (\alpha_1,\ldots,\alpha_{2n}) \in [0,1]^{2n}$ such that all its coordinates are irrational. For a positive integer k, let $\mathfrak{C}(k)$ be the set of cubes of the form

$$\left[\alpha_1 + \frac{u_1}{k}, \alpha_1 + \frac{u_1+1}{k}\right] \times \ldots \times \left[\alpha_{2n} + \frac{u_{2n}}{k}, \alpha_{2n} + \frac{u_{2n}+1}{k}\right],$$

with $u_1,\ldots,u_{2n} \in \mathbb{Z}$.

We consider the set of points

$$\left(\frac{x_1}{p}, \frac{y_1}{p}, \ldots, \frac{x_n}{p}, \frac{y_n}{p}\right) \in [0,1]^{2n} \tag{13}$$

taken over all solutions $(\mathbf{x},\mathbf{y}) \in \mathbb{F}_p^{2n}$ to the equation (1).

Note that the above irrationality condition on $\boldsymbol{\alpha}$ guarantees that the points (13) all belong to the interior of the cubes from $\mathfrak{C}(k)$.

Furthermore, let $\mathfrak{C}_0(k)$ be the set of cubes from $\mathfrak{C}(k)$ that are contained inside of Ω. By [12, Equation (9)], for any well-shaped set $\Omega \in [0,1]^{2n}$, we have

$$\#\mathfrak{C}_0(k) = k^{2n}\mu(\Omega) + O(k^{2n-1}). \tag{14}$$

Let $\mathfrak{B}_1 = \mathfrak{C}_0(2)$ and for $i = 2,3,\ldots$, let $\mathfrak{B}_i$ be the set of cubes $\Gamma \in \mathfrak{C}_0(2^i)$ that are not contained in any cube from $\mathfrak{C}_0(2^{i-1})$. Clearly

$$2^{-2in}\#\mathfrak{B}_i + 2^{-2(i-1)n}\#\mathfrak{C}_0(2^{i-1}) \le \mu(\Omega), \qquad i = 2,3,\ldots. \tag{15}$$

We now infer from (14) that

$$\begin{aligned}
&\mu(\Omega) - 2^{-2(i-1)n}\#\mathfrak{C}_0(2^{i-1}) \\
&\quad = \mu(\Omega) - 2^{-2(i-1)n}\left(2^{2(i-1)n}\mu(\Omega) + O(2^{(i-1)(2n-1)})\right) \\
&\quad \ll 2^{(i-1)(2n-1)-2(i-1)n} = 2^{-i+1}.
\end{aligned}$$

Therefore, the inequality (15) implies the bound

$$\#\mathfrak{B}_i \ll 2^{i(2n-1)}. \tag{16}$$

We also see that for any integer $M \ge 1$,

$$\Omega \setminus \Omega_\varepsilon^- \subseteq \bigcup_{i=1}^{M} \bigcup_{\Gamma\in\mathfrak{B}_i} \Gamma \subseteq \Omega, \tag{17}$$

with $\varepsilon = (2n)^{1/2}2^{-M}$. Indeed, for any point $\boldsymbol{\gamma} \in \Omega\setminus\Omega_\varepsilon^-$ there is a cube $\Gamma_{\boldsymbol{\gamma}} \in \mathfrak{C}(2^M)$ with $\boldsymbol{\gamma} \in \Gamma$ (since for any integer $k \ge 1$, the cubes from $\mathfrak{C}(k)$ tile the whole space $\mathbb{R}^{2n}$). Because the diameter (that is, the largest distance between the points) of $\Gamma_{\boldsymbol{\gamma}}$

is $(2n)^{1/2}2^{-M}$, we see from the definition of Ω_ε^- that $\Gamma_{\boldsymbol{\gamma}} \cap [0,1]^{2n} \backslash \Omega = \emptyset$. Thus $\Gamma_{\boldsymbol{\gamma}} \subseteq \Omega$. This implies

$$\Gamma_{\boldsymbol{\gamma}} \subseteq \bigcup_{i=1}^{2n} \bigcup_{\Gamma \in \mathfrak{B}_i} \Gamma$$

and (17) follows.

Since Ω is well-shaped, from (4) we deduce that

$$\mu\left(\bigcup_{i=1}^{2n} \bigcup_{\Gamma \in \mathfrak{B}_i} \Gamma\right) = \mu\left(\Omega\right) + O(2^{-M}). \tag{18}$$

We now assume that

$$2^M < p, \tag{19}$$

so Corollary 3 applies to all cubes $\Gamma \in \mathfrak{C}_0(2^i)$, $i = 1, \ldots, M$. Together with (17), this implies the inequality:

$$N(\mathbf{a}; p\Omega) \geq \sum_{i=1}^{M} \sum_{\Gamma \in \mathfrak{B}_i} N(\mathbf{a}; p\Gamma) = p^{2n-1} \sum_{i=1}^{M} \sum_{\Gamma \in \mathfrak{B}_i} \mu(\Gamma) + O(R), \tag{20}$$

where

$$R = \sum_{i=1}^{M} \#\mathfrak{B}_i \left(2^{-i(2n-1)} p^{2n-2} + 2^{-i(n/2+1)} p^n\right) p^{o(1)}.$$

We see from (18) that

$$\begin{aligned} p^{2n-1} \sum_{i=1}^{M} \sum_{\Gamma \in \mathfrak{B}_i} \mu(\Gamma) &= p^{2n-1} \mu\left(\bigcup_{i=1}^{M} \bigcup_{\Gamma \in \mathfrak{B}_i} \Gamma\right) \\ &= p^{2n-1} \mu\left(\Omega\right) + O\left(p^{2n-1} 2^{-M}\right). \end{aligned} \tag{21}$$

Furthermore, using (16), we derive

$$\begin{aligned} R &\leq \sum_{i=1}^{M} \left(p^{2n-2} + 2^{i(3n/2-2)} p^n\right) p^{o(1)} \\ &= \left(M p^{2n-2} + 2^{M(3n/2-2)} p^n\right) p^{o(1)}. \end{aligned} \tag{22}$$

Substituting (21) and (22) in (20) with the above choice of M, noticing that (19) implies $M = O(\log p)$, we obtain

$$N(\mathbf{a}; p\Omega) \geq p^{2n-1} \mu\left(\Omega\right) - Q p^{o(1)}, \tag{23}$$

where

$$Q \leq p^{2n-1} 2^{-M} + p^{2n-2} + 2^{M(3n/2-2)} p^n. \tag{24}$$

We now choose M to satisfy

$$2^M \leq p^{2(n-1)/(3n-2)} < 2^{M+1},$$

which asymptotically optimises the right hand side of the bound (24), verifies (19) and produces the bound $Q \ll p^{2n-(5n-4)/(3n-2)} + p^{2n-2} \ll p^{2n-5n/(3n-2)}$. We now see from (23) that (12) holds, which concludes the proof.

4. Comments

We note that for $B_1 = \ldots = B_n = 0$, using [13, Lemma 3] instead of Lemma 7 in this special case, one can improve Theorem 1 as follows:

$$\left| N(\mathbf{a};\mathcal{B}) - \frac{1}{p}\prod_{j=1}^{n}(K_jL_j) \right| \le \left(\frac{K_1L_1}{p^{1/2}} + \sqrt{K_1L_1}\right)\left(\frac{K_2L_2}{p^{1/2}} + \sqrt{K_2L_2}\right)\prod_{j=3}^{n}(K_j+L_j)p^{o(1)}.$$

Furthermore, it is easy to see that one can get a version of Lemma 8 for the more general sums of Lemma 7, which now becomes

$$\sum_{a=1}^{p-1}\left|\sum_{(x,y)\in\mathcal{W}} \mathbf{e}_p(ax/y)\right|^2 \le K^2L^2 + KLp^{1+o(1)},$$

that is, there is no cancellation of the main term for the number of solutions to the congruence (9) anymore. Thus the same arguments lead to the following result. For $n \ge 3$ and arbitrary intervals (2) and arbitrary convex sets $\mathcal{W}_j \subseteq \mathcal{I}_j \times \mathcal{J}_j$, $j = 1, \ldots, n$, for the set $\mathcal{S} = \mathcal{W}_1 \times \ldots \times \mathcal{W}_n$ we have

$$\left| N(\mathbf{a};\mathcal{S}) - \frac{N(\mathcal{S})}{p} \right| \le \left(\frac{K_1L_1}{p^{1/2}} + \sqrt{K_1L_1}\right)\left(\frac{K_2L_2}{p^{1/2}} + \sqrt{K_2L_2}\right)\prod_{j=3}^{n}(K_j+\sqrt{pL_j})p^{o(1)},$$

where $N(\mathcal{S}) = \#\left(\mathcal{S}\cap\mathbb{Z}^{2n}\right)$. For example, this can be used for counting solutions to the equation (1) with variables in disks

$$(x_j - b_j)^2 + (y_j - c_j)^2 \le r_j^2, \qquad j = 1, \ldots, n.$$

One can also ask about solutions to (1) with the additional co-primality condition $\gcd(x_j, y_j) = 1$, $j = 1, \ldots, n$, that is, essentially in *Farey fractions*. Using simple inclusion-exclusion arguments, one can easily derive relevant asymptotic formulas from our results.

Finally, we remark that Lemma 7 can be viewed as a statement about cancellations among short Kloosterman sums of the form

$$\mathcal{K}(\lambda;\mathcal{J}) = \sum_{u\in\mathcal{J}} \mathbf{e}_p(\lambda/u)$$

over an interval $\mathcal{J} = [B+1, B+L]$ when λ runs over an interval $\mathcal{I} = [A+1, A+K]$. Say, for $K = L$ we have a nontrivial cancellation starting with $L \ge p^{1/3+\delta}$ for any fixed $\delta > 0$, which is beyond the range of modern bounds of individual short Kloosterman sums over intervals that are not at the origin; we refer to the recent work of Bourgain and Garaev [4] for an outline of the state of art and several results.

References

[1] Anwar Ayyad, Todd Cochrane, and Zhiyong 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. Number Theory **59** (1996), no. 2, 398–413, DOI 10.1006/jnth.1996.0105. MR1402616 (97i:11091)

[2] Valentin Blomer and Jörg Brüdern, *The density of rational points on a certain threefold*, Contributions in analytic and algebraic number theory, Springer Proc. Math., vol. 9, Springer, New York, 2012, pp. 1–15, DOI 10.1007/978-1-4614-1219-9_1. MR3060454

[3] Valentin Blomer, Jörg Brüdern, and Per Salberger, *On a certain senary cubic form*, Proc. Lond. Math. Soc. (3) **108** (2014), no. 4, 911–964, DOI 10.1112/plms/pdt043. MR3198752

[4] J. Bourgain and M. Z. Garaev, *Sumsets of reciprocals in prime fields and multilinear Kloosterman sums* (Russian, with Russian summary), Izv. Ross. Akad. Nauk Ser. Mat. **78** (2014), no. 4, 19–72; English transl., Izv. Math. **78** (2014), no. 4, 656–707. MR3288401

[5] Javier Cilleruelo and Moubariz Z. Garaev, *Concentration of points on two and three dimensional modular hyperbolas and applications*, Geom. Funct. Anal. **21** (2011), no. 4, 892–904, DOI 10.1007/s00039-011-0127-6. MR2827013 (2012i:11093)

[6] Javier Cilleruelo, Igor E. Shparlinski, and Ana Zumalacárregui, *Isomorphism classes of elliptic curves over a finite field in some thin families*, Math. Res. Lett. **19** (2012), no. 2, 335–343, DOI 10.4310/MRL.2012.v19.n2.a6. MR2955765

[7] G. H. Hardy and E. M. Wright, *An introduction to the theory of numbers*, 5th ed., The Clarendon Press, Oxford University Press, New York, 1979. MR568909 (81i:10002)

[8] Henryk Iwaniec and Emmanuel Kowalski, *Analytic number theory*, American Mathematical Society Colloquium Publications, vol. 53, American Mathematical Society, Providence, RI, 2004. MR2061214 (2005h:11005)

[9] Bryce Kerr, *Solutions to polynomial congruences in well-shaped sets*, Bull. Aust. Math. Soc. **88** (2013), no. 3, 435–447, DOI 10.1017/S0004972713000324. MR3189293

[10] Bryce Kerr and Igor E. Shparlinski, *On the distribution of values and zeros of polynomial systems over arbitrary sets*, J. Number Theory **133** (2013), no. 9, 2863–2873, DOI 10.1016/j.jnt.2013.02.012. MR3057051

[11] Oscar Marmon, *The density of integral points on hypersurfaces of degree at least four*, Acta Arith. **141** (2010), no. 3, 211–240, DOI 10.4064/aa141-3-1. MR2587286 (2011a:11068)

[12] Wolfgang M. Schmidt, *Irregularities of distribution. IX*, Acta Arith. **27** (1975), 385–396. Collection of articles in memory of Juriĭ Vladimirovič Linnik. MR0376593 (51 #12768)

[13] Igor E. Shparlinski, *Exponential sums with Farey fractions*, Bull. Pol. Acad. Sci. Math. **57** (2009), no. 2, 101–107, DOI 10.4064/ba57-2-2. MR2545841 (2010h:11128)

[14] Igor E. Shparlinski, *On the distribution of solutions to polynomial congruences*, Arch. Math. (Basel) **99** (2012), no. 4, 345–351, DOI 10.1007/s00013-012-0436-5. MR2990153

[15] Igor E. Shparlinski, *Linear equations with rational fractions of bounded height and stochastic matrices*, Quart. J. Math. (to appear).

Department of Pure Mathematics, University of New South Wales, Sydney, New South Wales 2052, Australia

E-mail address: igor.shparlinski@unsw.edu.au