J Fourier Anal Appl (2016) 22:237–250
DOI 10.1007/s00041-015-9417-y

Erdős Type Problems in Modules over Cyclic Rings

Esen Aksoy Yazici[1]

Received: 14 August 2014 / Revised: 1 June 2015 / Published online: 18 June 2015

Abstract In the present paper, we study various Erdős type geometric problems in the setting of the integers modulo q, where $q = p^l$ is an odd prime power. More precisely, we prove certain results about the distribution of triangles and triangle areas among the points of $E \subset \mathbb{Z}_q^2$.

Keywords Distance sets · Congruence classes of triangles · Erdős problems

Mathematics Subject Classification 42B10 · 51D20 · 97F60

1 Introduction

The classical Erdős distance problem asks for the number of distinct distances determined by n points in $\mathbb{R}^d$. In [6], Erdős conjectured that the minimum number of distinct distances determined by n points in the Euclidean plane is $C\frac{n}{\sqrt{logn}}$. Several results have been given in this direction and recently Guth and Katz [8] settled the conjecture, up to a square root log factor showing that n points determine at least $C\frac{n}{logn}$ distances. We shall note here that in higher dimensions the distance problem is still open with the best known results due to Solymosi and Vu [14].

A natural generalization of the distance problem is the distribution of k-simplices. In this setting, for $k = 2$, two triangles are congruent if there is an orthogonal transformation followed by a translation which takes one to another. If the triangles are non

Communicated by Hans G. Feichtinger.

✉ Esen Aksoy Yazici
eaksoyya@ur.rochester.edu

[1] University of Rochester, Rochester, USA

degenerate, this happens if and only if they have the same side-lengths. We will denote by $T_2(E)$ the set of congruence classes of triangles. In [7], for subsets E of $\mathbb{R}^2$, Greenleaf, Iosevich, Liu and Palsson proved that if $dim_H(E) > \frac{8}{5}$, then $\mathcal{L}^3(T_2(E)) > 0$, where $\mathcal{L}^3(T_2(E))$ denotes the 3-dimensional Lebesgue measure of $T_2(E)$.

A variant of the distance problem is the volume set problem. Given n points in the plane one can easily see that the number of distinct triangle areas determined by the points can be as large as $\binom{n}{3}$ if the points are in general position. In 2008, [13], Pinchasi settled a long standing conjecture of Erdős, Purdy and Straus proving that the number of distinct areas of triangles determined by a non-collinear point set of size n is at least $\lfloor \frac{n-1}{2} \rfloor$.

One can ask similar discrete questions in the context of vector spaces over finite fields $\mathbb{F}_q^d$, or modules over finite cyclic rings $\mathbb{Z}_q^d$. Several problems have been studied by various authors in the context of finite fields, see for example [1–4,9,10,12] and the references therein. Indeed, the techniques and results for the problems in the context of finite fields are an analogous version of those in Euclidean space.

For $G = \mathbb{F}_q$ or $\mathbb{Z}_q$, and $x, y \in G^d$, we can consider the following distance map

$$\lambda : (x, y) \longmapsto \|x - y\| = (x_1 - y_1)^2 + \cdots + (x_d - y_d)^2.$$

This map does not induce a metric on G^d, but is a non-degenerate quadratic form on G^d. The Erdős-Falconer distance problem in G^d asks for a threshold on the size $E \subset G^d$ so that the distance set of E,

$$\Delta(E) := \{\|x - y\| : x, y \in E\},$$

is about the size q.

In [11], Iosevich and Rudnev prove that for $E \subset \mathbb{F}_q^d$ if $|E| > Cq^{\frac{d+1}{2}}$ for a sufficiently large constant C, then $\Delta(E) = \mathbb{F}_q$. Note that this result is in parallel to the Falconer result for the subsets of $\mathbb{R}^d$.

We also define the d- dimensional non-zero volumes of $(d + 1)$-simplices whose vertices are in E by

$$V_d(E) = \{det(x^1 - x^{d+1}, \ldots, x^d - x^{d+1}) : \; x^j \in E\} \setminus \{0\}.$$

The distribution of triangle areas among the points of a subset E of $\mathbb{F}_q^2$ was studied by Iosevich, Rudnev, and Zhai in [12]. The method uses a point-line incidence theory and the result is the following. If $E \subset \mathbb{F}_q^2$ with $|E| > q$, then $|V_2(E)| \geq \frac{q-1}{2}$, and the triangles giving at least $\frac{q-1}{2}$ distinct areas can be chosen such that they share the same base.

In this paper, we turn our attention to the Erdős-Falconer type problems in modules $\mathbb{Z}_q^d$ over the cyclic rings $\mathbb{Z}_q$, where $q = p^l$, p is an odd prime, and prove the following results. Compared to configurations in vector spaces over finite fields, to overcome the difficulties arising from the zero divisors in these cyclic rings, an extra arithmetical machinery is developed.

1.1 Statement of Main Results

$$SO_2(\mathbb{Z}_q) = \{A \in M_2(\mathbb{Z}_q) : AA^T = I,\ det(A) = 1\}$$

In this setting, two triangles (x^1, x^2, x^3), (y^1, y^2, y^3) in $\mathbb{Z}_q^2$ are said to be congruent if $\exists\theta \in SO_2(\mathbb{Z}_q)$ such that

$$x^i - x^j = \theta(y^i - y^j) \quad \text{for all } i, j.$$

Let $T_2(E)$ denote the set of congruence classes of triangles determined by the points of $E \subset \mathbb{Z}_q^2$. We then prove the following.

Theorem 1.1 *Suppose $E \subset \mathbb{Z}_q^2$ with $q = p^l$ and $p \equiv 3\ mod 4$. If $|E| \geq \sqrt[3]{3}p^{2l-\frac{1}{3}}$, then $|T_2(E)| \gtrsim q^3$.*

In [5], Covert, Iosevich and Pakianathan prove an asymptotically sharp bound for the distance set $\Delta(E)$ of $E \subset \mathbb{Z}_q^d$. More precisely, it is shown that if $E \subset \mathbb{Z}_q^d$, where $q = p^l$, and $|E| \gg l(l+1)q^{\frac{(2l-1)d}{2l}+\frac{1}{2l}}$, then $\Delta(E) \supset \mathbb{Z}_q^*$, where $\mathbb{Z}_q^*$ denotes the set of unit elements of $\mathbb{Z}_q$. In Theorem 1.1 above, we study distribution of triangles for subsets E of $\mathbb{Z}_q^2$.

In Theorem 1.2, we modify a method used in [12] over finite fields, to prove a sufficient condition on the size of $E \subset \mathbb{Z}_q^2$ so that the number of distinct triangle areas determined by E is about the size q.

For $E \subset \mathbb{Z}_q^2$, let

$$V_2(E) = \{det(x^1 - x^3, x^2 - x^3) : x^j \in E\} \setminus \{0\}.$$

Theorem 1.2 *Let $E \subset \mathbb{Z}_q^2$ where $q = p^l$. Suppose that $|E| > p^{2l-\frac{1}{2}}$. Then $|V_2(E)| \geq \frac{q}{4}\frac{1+p}{p} - 1$.*

1.2 Fourier Analysis in $\mathbb{Z}_q^d$

Let $f, g : \mathbb{Z}_q^d \to \mathbb{C}$. The Fourier transform of f is defined as

$$\widehat{f}(m) = q^{-d} \sum_{x\in\mathbb{Z}_q^d} \chi(-x \cdot m) f(x),$$

where $\chi(z) = exp(2\pi iz/q)$.

We use the following properties:

$$q^{-d} \sum_{x\in\mathbb{Z}_q^d} \chi(x \cdot m) = \begin{cases} 1, & \text{if } m = 0 \\ 0, & \text{otherwise} \end{cases} \qquad \text{(Orthogonality)}$$

$$f(x) = \sum_{m \in \mathbb{Z}_q^d} \chi(x \cdot m) \widehat{f}(m) \qquad \text{(Inversion)}$$

$$\sum_{m \in \mathbb{Z}_q^d} |\widehat{f}(m)|^2 = q^{-d} \sum_{x \in \mathbb{Z}_q^d} |f(x)|^2. \qquad \text{(Plancherel)}$$

2 Proof of Theorem 1.1

For the proof of Theorem 1.1 we will need the following lemmas.

Let us first denote by

$$\begin{aligned} SO_2(\mathbb{Z}_q) &= \{A \in M_2(\mathbb{Z}_q) : AA^T = I,\ det(A) = 1\} \\ &= \left\{ \begin{bmatrix} a & -b \\ b & a \end{bmatrix} : a^2 + b^2 \equiv 1 \bmod q \right\} \end{aligned}$$

the special orthogonal group.

Lemma 2.1 *Let $\xi = (\xi_1, \xi_2) \in \mathbb{Z}_q^2$, where $q = p^l$ and p is an odd prime. If $\|\xi\| = \xi_1^2 + \xi_2^2 \neq 0$, then $|Stab(\xi)| \leq p^{l-1}$, where $Stab$ is the stabilizer under the action of the special orthogonal group.*

Proof Let $\xi = (x, y) \in \mathbb{Z}_q^2$. Since $\|\xi\| \neq 0$, we can write $\|\xi\| = x^2 + y^2 = p^i u$, $0 \leq i \leq l-1$, $u \in \mathbb{Z}_q^*$. Now if $A = \begin{bmatrix} a & b \\ -b & a \end{bmatrix} \in SO_2(\mathbb{Z}_q)$ fixes ξ, then from the identity

$$\begin{bmatrix} a & b \\ -b & a \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} x \\ y \end{bmatrix}$$

we get

$$\begin{aligned} (a-1)x + by &= 0 \\ -bx + (a-1)y &= 0. \end{aligned}$$

Multiplying the first equation by x, and the second equation by y, summing together we have $(a-1)(x^2 + y^2) = 0$. Similarly, multiplying the first equation by y, and the second equation by $-x$, summing together we have $b(x^2 + y^2) = 0$. Hence

$$\begin{aligned} (a-1)(x^2 + y^2) &\equiv 0 \mod p^l, \\ b(x^2 + y^2) &\equiv 0 \mod p^l. \end{aligned} \tag{2.1}$$

Putting $x^2 + y^2 = p^i u$ in (2.1), we have

$$a = p^{l-i}k + 1,\ 0 \leq k < p^i,\ \text{and}\ b = p^{l-i}m,\ 0 \leq m < p^i, \tag{2.2}$$

where

$$a^2 + b^2 \equiv 1 \bmod p^l. \tag{2.3}$$

Now to conclude the argument, we claim that for $a_0 \neq a$ if b_0 and b are satisfying $a_0^2 + b_0^2 \equiv 1 \bmod p^l$ and $a^2 + b^2 \equiv 1 \bmod p^l$ and condition (2.2), respectively, then $b_0 \neq b$. This will prove the lemma, for then the number of pairs (a, b) satisfying the conditions (2.2) and (2.3) is at most the number of possibilities of b which is p^i. This is at most p^{l-1} as the valuation of a nonzero element is at most $l - 1$.

It remains to prove the claim and we will prove its contrapositive here. Suppose that $b_0 = b$ and $a_0^2 + b_0^2 \equiv 1 \bmod p^l$, $a^2 + b^2 \equiv 1 \bmod p^l$, so that $a_0^2 \equiv a^2 \bmod p^l$. Writing $a_0 = p^{l-i}k_0 + 1$ and $a = p^{l-i}k + 1$, It follows that

$$(p^{l-i}k_0 + 1)^2 \equiv (p^{l-i}k + 1)^2 \bmod p^l,$$
$$p^{2l-2i}k_0^2 + 2p^{l-i}k_0 \equiv p^{2l-2i}k^2 + 2p^{l-i}k \bmod p^l,$$

therefore,

$$p^{2l-2i}(k_0^2 - k^2) + 2p^{l-i}(k_0 - k) \equiv 0 \bmod p^l,$$
$$p^{l-i}(k_0 - k)(p^{l-i}(k_0 + k) + 2) \equiv 0 \bmod p^l.$$

Thus $p^l \mid p^{l-i}(k_0 - k)(p^{l-i}(k_0 + k) + 2)$, and since $p \nmid p^{l-i}(k_0 + k) + 2$ as p is odd, we must have $p^i \mid k_0 - k < p^i$. Hence we have $k_0 - k = 0$, i.e., $k_0 = k$ and therefore $a_0 = a$. □

Lemma 2.2 *Let $\xi \in \mathbb{Z}_q^2 \setminus (0, 0)$, where $q = p^l$ and $p \equiv 3$ mod 4. If $\|\xi\| = 0$, then $|Stab(\xi)| \leq p^{l-1}$.*

For the proof of Lemma 2.2 we will use Hensel's Lemma.

Lemma 2.3 (Hensel's Lemma) *Let $f(x) \in \mathbb{Z}[x]$, $f(r) \equiv 0$ mod p and $f'(r) \not\equiv 0$ mod p so that r is a simple root of f modulo p. Then for any $k \geq 2$, there exists a unique $\hat{r}$ in $\mathbb{Z}_{p^k}$ such that $f(\hat{r}) \equiv 0$ mod p^k with $\hat{r} \equiv r$ mod p.*

Proof of Lemma 2.2 We first note that as $p \equiv 3 \bmod 4$, for $\xi = (\xi_1, \xi_2) \in \mathbb{Z}_q^2 \setminus (0, 0)$, $\|\xi\| = \xi_1^2 + \xi_2^2 = 0$ forces the p-adic norms $\|\xi_1\|_p = \|\xi_2\|_p$. Therefore, $\xi = (\xi_1, \xi_2) = (p^m u, p^m v)$ for some $m \geq \frac{l}{2}$ and $u, v \in \mathbb{Z}_q^*$. Now if $A \in SO_2(\mathbb{Z}_q)$ fixes $\xi = (p^m u, p^m v)$, it can be readily shown that it also fixes $\eta = (-p^m v, p^m u)$. Hence A also fixes $Span\{\xi, \eta\} = p^m(\mathbb{Z}_{p^l} \times \mathbb{Z}_{p^l}) \cong \mathbb{Z}_{p^{l-m}} \times \mathbb{Z}_{p^{l-m}}$.

Since $\xi \neq (0, 0)$, we have $m \leq l - 1$. We shall note that $\mathbb{Z}_{p^{l-m}} \times \mathbb{Z}_{p^{l-m}}$ is smallest, and hence the number of matrices A that fixes $\mathbb{Z}_{p^{l-m}} \times \mathbb{Z}_{p^{l-m}}$ is largest, when $m = l - 1$. Therefore it is sufficient to consider the case $m = l - 1$. In this case A fixes $p^{l-1}(\mathbb{Z}_{p^l} \times \mathbb{Z}_{p^l}) \cong \mathbb{Z}_p \times \mathbb{Z}_p$.

We now write

$$A = I_2 + B,$$

where I_2 denotes the 2×2 identity matrix and $B \in M_2(\mathbb{Z}_q)$. Then for any $y \in \mathbb{Z}_q^2$ we have

$$Ap^{l-1}y = p^{l-1}y + Bp^{l-1}y,$$

so that $Bp^{l-1}y = 0$ as A fixes $p^{l-1}y$. This implies that $B = pB'$ for some $B' \in M_2(\mathbb{Z}_q)$, and

$$A = I_2 + pB' \in \Gamma_1 \cap SO_2(\mathbb{Z}_q).$$

where Γ_1 denotes the matrices in $M_2(\mathbb{Z}_q)$ congruent to I_2 mod p.

It follows that

$$Stab(\xi) = \left\{ \begin{bmatrix} a & -b \\ b & a \end{bmatrix} : a, b \in \mathbb{Z}_q,\ a^2 + b^2 \equiv 1 \bmod q,\ a \equiv 1 \bmod p,\ b \equiv 0 \bmod p \right\}. \tag{2.4}$$

Now we count the number of matrices in (2.4). We first fix b. Since $b \equiv 0 \bmod p$, we have p^{l-1} choices for b. Then we consider the polynomial $f(x) = x^2 - (1 - b^2) \in \mathbb{Z}[x]$. Note that $f(x) = x^2 - 1$ in $\mathbb{Z}_p$ as $b \equiv 0 \bmod p$. Hence 1 is a root of $f(x)$ and $f'(1) = 2 \neq 0$ in $\mathbb{Z}_p$ as p is odd. Hence by Hensel's Lemma there exists a unique a in $\mathbb{Z}_q$ such that $f(a) = a^2 - (1 - b^2) = 0$ in $\mathbb{Z}_q$ with $a \equiv 1 \mathrm{mod} p$. Therefore the number matrices of the form in (2.4) is p^{l-1}. This completes the proof. □

We make use of the following lemma from [1].

Lemma 2.4 *For any finite space F, any function $f : F \to \mathbb{R}_{\geq 0}$, and any $n \geq 2$ we have*

$$\sum_{z \in F} f^n(z) \leq |F| \left(\frac{\|f\|_1}{|F|} \right)^n + \frac{n(n-1)}{2} \|f\|_\infty^{n-2} \sum_{z \in F} \left(f(z) - \frac{\|f\|_1}{|F|} \right)^2,$$

where $\|f\|_1 = \sum_{z \in F} |f(z)|$, and $\|f\|_\infty = max_{z \in F} f(z)$.

Lastly, we state the following lemma from [5] and use Remark 2.6 for the proof of Theorem 1.1.

Lemma 2.5 *Let $d \geq 2$ and $j \in \mathbb{Z}_q^*$, where q is odd. Set $||x|| = x_1^2 + \cdots + x_d^2$. Denote by $S_j = \{x \in \mathbb{Z}_q^d : ||x|| = j\}$ the sphere of radius j. Then,*

$$|S_j| = q^{d-1}(1 + o(1)).$$

Remark 2.6 Note that

$$SO_2(\mathbb{Z}_q) = \left\{ \begin{bmatrix} a & -b \\ b & a \end{bmatrix} : a^2 + b^2 \equiv 1 \bmod q \right\} \tag{2.5}$$

and hence if we denote by S_1 the sphere of radius 1 in $\mathbb{Z}_q^2$, then $|SO_2(\mathbb{Z}_q)| = |S_1| \sim q$, by Lemma 2.5.

Proof of Theorem 1.1 We first recall that $SO_2(\mathbb{Z}_q) = \{A \in M_2(\mathbb{Z}_q) : AA^T = I,\ det(A) = 1\}$ and define an equivalence relation on $(\mathbb{Z}_q^2)^3$ as

$$(a, b, c) \sim (a', b', c')$$

if $\exists \theta \in SO_2(\mathbb{Z}_q)$ with $a' = \theta a,\ b' = \theta b,\ c' = \theta c.$

For $E \subset \mathbb{Z}_q^2$ and $a, b, c \in \mathbb{Z}_q^2$, let

$$\begin{aligned}\mu(a, b, c) = |\{(x, y, z) \in E^3 : \exists \theta \in SO_2(\mathbb{Z}_q) \text{ such that } x - y = \theta a, y - z \\ = \theta b, x - z = \theta c.\}|.\end{aligned}$$

Note that $\mu(\theta a, \theta b, \theta c) = \mu(a, b, c)$ for all $\theta \in SO_2(\mathbb{Z}_q)$, so μ can be viewed as a function $\mu : (\mathbb{Z}_q^2)^3/\sim \to \mathbb{Z}_{\geq 0}$.

Then by the Cauchy–Schwarz inequality,

$$|E|^6 = \left(\sum_{(a,b,c)\in(\mathbb{Z}_q^2)^3/\sim} \mu(a, b, c) \right)^2 \leq |T_2(E)| \left(\sum_{(a,b,c)\in(\mathbb{Z}_q^2)^3/\sim} \mu^2(a, b, c) \right),$$

where

$$|T_2(E)| = |\{(a, b, c) \in (\mathbb{Z}_q^2)^3/\sim: \mu(a, b, c) \neq 0\}|,$$

which is equal to

$$\begin{aligned}|\{(a, b, c) \in (\mathbb{Z}_q^2)^3/\sim: \exists (x, y, z) \in E^3 \text{ and } \theta \in SO_2(\mathbb{Z}_q) \text{ such that } x - y \\ = \theta a, y - z = \theta b, x - z = \theta c\}|.\end{aligned}$$

We have,

$$\begin{aligned}\mu^2(a, b, c) = |\{&(x, y, z, x', y', z') \in E^6 : \exists \theta_1, \theta_2 \in SO_2(\mathbb{Z}_q) \text{ such that} \\ &x - y = \theta_1 a,\ x' - y' = \theta_2 a \\ &y - z = \theta_1 b,\ y' - z' = \theta_2 b \\ &x - z = \theta_1 c,\ x' - z' = \theta_2 c\}| \\ = |\{&(x, y, z, x', y', z') \in E^6 : \exists \theta_1, \theta_2 \in SO_2(\mathbb{Z}_q) \text{ such that} \\ &\theta_1^{-1}(x - y) = \theta_2^{-1}(x' - y') = a \\ &\theta_1^{-1}(y - z) = \theta_2^{-1}(y' - z') = b \\ &\theta_1^{-1}(x - z) = \theta_2^{-1}(x' - z') = c\}|\end{aligned}$$

so that

$$\begin{aligned}\sum_{(a,b,c)\in(\mathbb{Z}_q^2)^3/\sim}\mu^2(a,b,c) &= |\{(x,y,z,x',y',z')\in E^6 : \exists\theta_1,\theta_2\in SO_2(\mathbb{Z}_q) \text{ such that}\\ &\qquad \theta_1^{-1}(x-y)=\theta_2^{-1}(x'-y')\\ &\qquad \theta_1^{-1}(y-z)=\theta_2^{-1}(y'-z')\\ &\qquad \theta_1^{-1}(x-z)=\theta_2^{-1}(x'-z')\}|\\ &= |\{(x,y,z,x',y',z')\in E^6 : \exists\theta\in SO_2(\mathbb{Z}_q) \text{ such that}\\ &\qquad \theta(x-y)=x'-y',\ \theta(y-z)=y'-z',\ \theta(x-z)=x'-z'\}|\\ &= |\{(x,y,z,x',y',z')\in E^6 : \exists\theta\in SO_2(\mathbb{Z}_q) \text{ such that}\\ &\qquad x'-\theta x=y'-\theta y=z'-\theta z\}|.\end{aligned}$$

For a fixed $\theta\in SO_2(\mathbb{Z}_q)$, let

$$\nu_\theta(t)=|\{(u,v)\in E\times E:\ u-\theta(v)=t\}|. \tag{2.6}$$

Then we have

$$\nu_\theta^3(t)=|\{(x,y,z,x',y',z')\in E^6 : x'-\theta x=y'-\theta y=z'-\theta z=t\}|,$$

and therefore

$$\sum_{(a,b,c)\in(\mathbb{Z}_q^2)^3/\sim}\mu^2(a,b,c)\le\sum_{\substack{\theta\in SO_2(\mathbb{Z}_q)\\ t\in\mathbb{Z}_q^2}}\nu_\theta^3(t). \tag{2.7}$$

By Lemma 2.4,

$$\sum_{t\in\mathbb{Z}_q^2}\nu_\theta^3(t)\le q^2\left(\frac{\|\nu_\theta\|_1}{q^2}\right)^3+3\|\nu_\theta\|_\infty\sum_{t\in\mathbb{Z}_q^2}\left(\nu_\theta(t)-\frac{\|\nu_\theta\|_1}{q^2}\right)^2$$

where $\|\nu_\theta\|_1=\sum_{t\in\mathbb{Z}_q^2}\nu_\theta(t)=|E|^2$ and $\|\nu_\theta\|_\infty=sup_t|\nu_\theta(t)|\le|E|$ as when we first fix v in (2.6), u is uniquely determined.

It follows that

$$\begin{aligned}\sum_{t\in\mathbb{Z}_q^2}\nu_\theta^3(t)&\le q^{-4}|E|^6+3|E|\sum_{t\in\mathbb{Z}_q^2}\left(\nu_\theta(t)-\frac{\|\nu_\theta\|_1}{q^2}\right)^2\\ &\le q^{-4}|E|^6+3q^2|E|\sum_{\xi\in\mathbb{Z}_q^2\setminus(0,0)}|\widehat{\nu}_\theta(\xi)|^2 \text{ (by Plancherel Theorem)}\end{aligned}$$

and thus

$$\sum_{\substack{\theta\in SO_2(\mathbb{Z}_q)\\ t\in\mathbb{Z}_q^2}} \nu_\theta^3(t) \leq |SO_2(\mathbb{Z}_q)|q^{-4}|E|^6 + 3q^2|E| \sum_{\substack{\theta\in SO_2(\mathbb{Z}_q)\\ \xi\in\mathbb{Z}_q^2\setminus(0,0)}} |\widehat{\nu_\theta}(\xi)|^2$$

By Remark 2.6, $|SO_2(\mathbb{Z}_q)| \sim q$ and hence

$$\sum_{\substack{\theta\in SO_2(\mathbb{Z}_q)\\ t\in\mathbb{Z}_q^2}} \nu_\theta^3(t) \lesssim q^{-3}|E|^6 + 3q^2|E| \sum_{\substack{\theta\in SO_2(\mathbb{Z}_q)\\ \xi\in\mathbb{Z}_q^2\setminus(0,0)}} |\widehat{\nu_\theta}(\xi)|^2 \tag{2.8}$$

Noting that

$$\begin{aligned}
\nu_\theta(t) &= \sum_{v\in\mathbb{Z}_q^2} E(v)E(t+\theta v)\\
&= \sum_{v,\alpha\in\mathbb{Z}_q^2} E(v)\chi(\alpha\cdot(t+\theta v))\widehat{E}(\alpha)\\
&= \sum_{v,\alpha\in\mathbb{Z}_q^2} \widehat{E}(\alpha)\chi(t\cdot\alpha)E(v)\chi(\alpha\cdot\theta v)\\
&= \sum_{\alpha\in\mathbb{Z}_q^2} \widehat{E}(\alpha)\chi(t\cdot\alpha) \sum_{v\in\mathbb{Z}_q^2} \chi(\alpha\cdot\theta v)E(v)\\
&= \sum_{\alpha\in\mathbb{Z}_q^2} \widehat{E}(\alpha)\chi(t\cdot\alpha) \sum_{v\in\mathbb{Z}_q^2} \chi(\theta^T(\alpha)\cdot v)E(v)\\
&= q^2 \sum_{\alpha\in\mathbb{Z}_q^2} \widehat{E}(\alpha)\chi(t\cdot\alpha)\widehat{E}(-\theta^T(\alpha)),
\end{aligned}$$

and

$$\begin{aligned}
\widehat{\nu_\theta}(\xi) &= q^{-2}\sum_{t\in\mathbb{Z}_q^2} \chi(-t\cdot\xi)\nu_\theta(t)\\
&= q^{-2}\sum_{t\in\mathbb{Z}_q^2} \chi(-t\cdot\xi)q^2 \sum_{\alpha\in\mathbb{Z}_q^2} \widehat{E}(\alpha)\chi(t\cdot\alpha)\widehat{E}(-\theta^T(\alpha))\\
&= \sum_{\alpha\in\mathbb{Z}_q^2} \widehat{E}(\alpha)\widehat{E}(-\theta^T(\alpha)) \sum_{t\in\mathbb{Z}_q^2} \chi(t\cdot(\alpha-\xi))\\
&= q^2\widehat{E}(\xi)\widehat{E}(-\theta^T(\xi)),
\end{aligned}$$

we have

$$\begin{aligned}\sum_{\substack{\theta\in SO_2(\mathbb{Z}_q)\\ \xi\in\mathbb{Z}_q^2\setminus(0,0)}}|\widehat{\nu_\theta}(\xi)|^2 &= q^4\sum_{\substack{\theta\in SO_2(\mathbb{Z}_q)\\ \xi\in\mathbb{Z}_q^2\setminus(0,0)}}|\widehat{E}(\xi)|^2|\widehat{E}(-\theta^T(\xi))|^2\\ &= q^4\sum_{\substack{\theta\in SO_2(\mathbb{Z}_q)\\ \xi\in\mathbb{Z}_q^2\setminus(0,0)}}|\widehat{E}(\xi)|^2|\widehat{E}(\theta^T(\xi))|^2\\ &\le q^4\left(\max_{\xi\in\mathbb{Z}_q^2\setminus(0,0)}|Stab(\xi)|\right)\sum_{\xi\neq(0,0)}|\widehat{E}(\xi)|^2\sum_{\substack{\eta\neq(0,0)\\ \|\eta\|=\|\xi\|}}|\widehat{E}(\eta)|^2\end{aligned}$$

Plugging this value in (2.8) and using (2.7) we get

$$\begin{aligned}\sum_{(a,b,c)\in(\mathbb{Z}_q^2)^3/\sim}\mu^2(a,b,c) &\le \sum_{\substack{\theta\in SO_2(\mathbb{Z}_q)\\ t\in\mathbb{Z}_q^2}}\nu_\theta^3(t)\\ &\lesssim q^{-3}|E|^6+3q^6|E|\left(\max_{\xi\in\mathbb{Z}_q^2\setminus(0,0)}|Stab(\xi)|\right)\\ &\quad\times\sum_{\xi\neq(0,0)}|\widehat{E}(\xi)|^2\sum_{\substack{\eta\neq(0,0)\\ \|\eta\|=\|\xi\|}}|\widehat{E}(\eta)|^2\\ &= q^{-3}|E|^6+3q^6|E|\mathrm{I}\end{aligned}\tag{2.9}$$

where

$$\mathrm{I}=\left(\max_{\xi\in\mathbb{Z}_q^2\setminus(0,0)}|Stab(\xi)|\right)\sum_{\xi\neq(0,0)}|\widehat{E}(\xi)|^2\sum_{\substack{\eta\neq(0,0)\\ \|\eta\|=\|\xi\|}}|\widehat{E}(\eta)|^2$$

We first note that $|Stab(\xi)|\le p^{l-1}$ for $\xi\neq(0,0)$ by Lemma 2.1 and 2.2. Extending the summation in η over all η and using Plancherel twice in I, we get

$$\mathrm{I}\le p^{l-1}q^{-4}|E|^2.$$

Plugging this value in (2.9) gives

$$\sum_{(a,b,c)\in(\mathbb{Z}_q^2)^3/\sim}\mu^2(a,b,c)\lesssim q^{-3}|E|^6+3q^2|E|^3p^{l-1},\tag{2.10}$$

so that

$$
\begin{aligned}
|T_2(E)| &\geq \frac{|E|^6}{q^{-3}|E|^6 + 3q^2|E|^3 p^{l-1}} \\
&\geq \frac{|E|^6}{2q^{-3}|E|^6} = \frac{q^3}{2}
\end{aligned}
$$

whenever $|E| \geq \sqrt[3]{3}p^{2l-\frac{1}{3}}$, which completes the proof. □

3 Proof of Theorem 1.2

Now before giving the proof, let us introduce the necessary background.

Let $q = p^l$ and $(a, b) \in \mathbb{Z}_q^2$. Let $\langle (a, b)\rangle = \{t(a, b) \colon t \in \mathbb{Z}_q\}$ be the submodule of $\mathbb{Z}_q^2$ generated by (a, b), which gives the line through origin and the point (a, b) in $\mathbb{Z}_q^2$. Now, consider the set

$$\Lambda_n = \{(a, b) \in \mathbb{Z}_q^2 : p^n | a, b \text{ but } (a, b) \neq (0, 0) \text{ mod } p^{n+1}\},$$

and denote $|\Lambda_n| = \lambda_n$ for $n = 0, 1, \ldots, l - 1$.

Lemma 3.1 $\lambda_n = p^{2(l-n)} - p^{2(l-n-1)}$.

Proof Since $p^n|a, b$ in $\mathbb{Z}_q$ we have p^{l-n} choices for a and b each and hence $p^{2(l-n)}$ choices for (a, b). Now we need to subtract $p^{2(l-n-1)}$ cases where p^{n+1} divides both a and b to get the desired result. □

Lemma 3.2 *Let $\mathcal{L}_n = \{\langle (a, b)\rangle : (a, b) \in \Lambda_n\}$ denote the set of lines generated by the points of Λ_n. Then $|\mathcal{L}_n| = p^{l-n} + p^{l-n-1}$.*

Proof For $(a, b) \in \Lambda_n$, note that $\langle (a, b)\rangle$ is cyclic and $|\, \langle (a, b)\rangle \,| = p^{l-n}$. Hence there exist $\phi(p^{l-n}) = p^{l-n} - p^{l-n-1}$ generators of the group which lies in Λ_n. So that for each n, we have

$$\frac{p^{2(l-n)} - p^{2(l-n-1)}}{p^{l-n} - p^{l-n-1}} = p^{l-n} + p^{l-n-1}$$

many lines in $\mathcal{L}_n$ each containing p^{l-n} points. □

We now conclude that the average number of points in a line in $\mathbb{Z}_q^2$ is

$$
\begin{aligned}
&= \frac{\sum_{n=0}^{l-1}(p^{l-n} + p^{l-n-1})p^{l-n}}{\sum_{n=0}^{l-1} p^{l-n} + p^{l-n-1}} \\
&= \frac{p^{2l} + p^{2l-1} + p^{2l-2} + \cdots + p^2 + p}{p^l + 2p^{l-1} + 2p^{l-2} + \cdots + 2p + 1} \\
&\sim p^l
\end{aligned}
$$

In what follows we will only consider $\mathcal{L}_0$, i.e. the set of all lines of full length q in $\mathbb{Z}_q^2$.

Lemma 3.3 *For any $(a, b) \in \mathbb{Z}_q^2$ if $(a, b) \in \Lambda_n$, then (a, b) appears in p^n distinct lines in $\mathcal{L}_0$.*

Proof Say $(a, b) \in \Lambda_n$ and $p^{n+1} \nmid a$. Then (a, b) belongs to the lines generated by $\left(\frac{a}{p^n}, ip^{l-n} + \frac{b}{p^n}\right)$ for $i = 0, \dots, p^n - 1$. Note that $i_0 p^{l-n} + \frac{b}{p^n} = i_1 p^{l-n} + \frac{b}{p^n} \mod p^l$ would imply

$$\begin{aligned} i_0 p^{l-n} &= i_1 p^{l-n} \mod p^l \\ i_0 &= i_1 \mod p^n \end{aligned}$$

which is not the case. Hence the given points are all distinct. Since $\frac{a}{p^n}$ is a unit in $\mathbb{Z}_q$ it follows that the lines determined by the given generators are all distinct. □

Lemma 3.4 *Let $R_i = \{(x, y) \in \mathbb{Z}_q^2 \times \mathbb{Z}_q^2 : x - y \in \Lambda_i\}$ and $r_i = |R_i|$, for $i = 1, \dots, l-1$. Then $r := r_1 p + r_2 p^2 + \cdots + r_{l-1} p^{l-1} \leq 2p^{4l-1}$.*

Proof Let $x = (x_1, x_2)$, $y = (y_1, y_2)$ in Z_q^2. Now if $x - y = (x_1 - y_1, x_2 - y_2) \in \Lambda_i$ then $p^i | x_1 - y_1$ and $x_2 - y_2$ but $p^{i+1} \nmid x_1 - y_1$ or $x_2 - y_2$. $p^i | x_1 - y_1$ gives p^{l-i} choices for $x_1 - y_1$ in $\mathbb{Z}_q$, we have q choices for y_1 and y_1 determines x_1 uniquely. Hence we have qp^{l-i} choices for x_1 and y_1. Same argument applies for x_2 and y_2. Altogether the condition $p^i | x_1 - y_1$ and $x_2 - y_2$ gives $qp^{l-i} qp^{l-i}$ choices for $x = (x_1, x_2)$, $y = (y_1, y_2)$.

To exclude the cases where p^{i+1} divides both $x_1 - y_1$ and $x_2 - y_2$ we need to subtract $qp^{l-(i+1)} qp^{l-(i+1)}$ cases of x and y. Hence,

$$r_i = qp^{l-i} qp^{l-i} - qp^{l-i-1} qp^{l-i-1}.$$

Now summing $r_i p^i$'s over all $i = 1, \dots, l-1$ we get

$$\begin{aligned} r &= (qp^{l-1} qp^{l-1} - qp^{l-2} qp^{l-2}) p + (qp^{l-2} qp^{l-2} - qp^{l-3} qp^{l-3}) \\ &\quad \times p^2 + \cdots + (qpqp - q^2) p^{l-1} \\ &= q^2 (p^{2l-1} + p^{2l-2} - p^l - p^{l-1}) \\ &\leq 2q^2 p^{2l-1} = 2p^{4l-1}. \end{aligned}$$

□

Proof of Theorem 1.2 Let L be a line in $\mathcal{L}_0$ and consider the sum set

$$E + L = \{e + l : e \in E,\ l \in L\}$$

Since $|L||E| > q^2$

$$e_1 + l_1 = e_2 + l_2 \text{ for some } l_1 \neq l_2$$

so that

$$l_2 - l_1 = e_1 - e_2. \tag{3.1}$$

Here we aim to average the solutions of the Eq. (3.1) over $p^l + p^{l-1}$ lines in $\mathcal{L}_0$. To start with, we count the number of solutions of (3.1) over all lines in $\mathcal{L}_0$ in two cases:

In the case $e_1 = e_2$, there are $|E|$ and q^2 choices for $e_1 = e_2$ and $l_1 = l_2$, respectively.

In the case $e_1 \neq e_2$, we can choose e_1 and e_2 in $|E|(|E| - 1)$ different ways, and once we fix them, we look at the difference $e_1 - e_2$. At that point let $S_i = \{(e_1, e_2) \in E \times E : e_1 - e_2 \in \Lambda_i\}$ and $s_i = |S_i|$ for $i = 0, \dots, l - 1$. We know from Lemma 3.3 that if $(e_1, e_2) \in S_i$, then $e_1 - e_2$ lies on p^i lines in $\mathcal{L}_0$ and when we fix the line, $l_2 - l_1$ can be written q different ways on that line. In other words, for all s_i pairs $(e_1, e_2) \in S_i, l_1, l_2$ is chosen $p^i q$ different ways over the lines in $\mathcal{L}_0$.

So altogether we have

$$\begin{aligned}
&|\{(e_1, e_2, l_1, l_2) \in E \times E \times L \times L : \text{ (3.1) holds for some } L \in \mathcal{L}_0\}| \\
&= |E|q^2 + s_0 q + s_1 pq + s_2 p^2 q + \cdots + s_{l-1} p^{l-1} q \\
&\leq |E|^2 q + (s_0 + s_1 p + s_2 p^2 + \cdots + s_{l-1} p^{l-1})q \\
&\leq |E|^2 q + (|E|^2 + s)q
\end{aligned}$$

where $s = s_1 p + s_2 p^2 + \cdots + s_{l-1} p^{l-1}$. Note that $s \leq r \leq 2p^{4l-1} \leq 2|E|^2$ by Lemma 3.4 and the assumption on the size of E.

Hence we get,

$$|\{(e_1, e_2, l_1, l_2) \in E \times E \times L \times L : \text{ (3.1) holds for some } L \in \mathcal{L}_0\}| \leq 4|E|^2 q$$

It follows that there exists a $L \in \mathcal{L}_0$ such that

$$\begin{aligned}
|\{(e_1, e_2, l_1, l_2) \in E \times E \times L \times L : \text{ (3.1) holds}\}| &\leq 4|E|^2 \frac{p^l}{p^l + p^{l-1}} \\
&= 4|E|^2 \frac{p}{1 + p}.
\end{aligned}$$

If we let $\nu_{E+L}(n)$ denote the number of representations of n as $e + l$ for some $e \in E, l \in L$, then by the Cauchy–Schwarz inequality, for this particular L,

$$\begin{aligned}
|E|^2 |L|^2 &= \left(\sum_{n \in E+L} \nu(n) \right)^2 \\
&\leq |E + L| \sum_{n \in E+L} \nu^2(n) \\
&= |E + L| |\{(e_1, e_2, l_1, l_2) \in E \times E \times L \times L : \text{ (3.1) holds}\}|.
\end{aligned}$$

Hence,

$$|E+L| \geq \frac{|E|^2|L|^2}{|\{(e_1,e_2,l_1,l_2)\in E\times E\times L\times L:\ (3.1)\text{ holds}\}|}$$
$$\geq \frac{|E|^2p^{2l}}{4|E|^2\frac{p}{1+p}} = \frac{q^2}{4}\frac{1+p}{p}.$$

We conclude that there exist points of E in at least $\frac{q}{4}\frac{1+p}{p}$ parallel lines. Here we shall note that there are totally q parallel lines to L, including itself, and one of them must contain two points of E with a unit distance in between. For otherwise, on each of these parallel lines there would be at most p^{l-1} points of E yielding $|E| \leq qp^{l-1} = p^{2l-1}$ which is not the case. Now if we take those two points of E with a unit distance in between on one of the parallel lines to L as a base, then each point of E on the remaining $\frac{q}{4}\frac{1+p}{p} - 1$ parallel lines to L gives a different height, yielding at least $\frac{q}{4}\frac{1+p}{p} - 1$ many distinct triangle areas. □

Acknowledgments The author is grateful to Alex Iosevich and Jonathan Pakianathan for their guidance and support. She would like to thank the referee for the careful reading of the paper and for comments improving the exposition.

References

1. Bennett, M., Hart, D., Iosevich, A., Pakianathan J., Rudnev, M.: Group actions and geometric combinatorics in $\mathbb{F}_q^d$. http://arxiv.org/pdf/1311.4788.pdf
2. Bennett, M., Iosevich, A., Pakianathan, J.: Three-point configurations determined by subsets of $\mathbb{F}_q^2$ via the Elekes-Sharir paradigm. Combinatorica **34**(6), 689–706 (2014)
3. Chapman, J., Erdogan, M.B., Hart, D., Iosevich, A., Koh, D.: Pinned distance sets, k- simplices, Wolff's exponent in finite fields and sum-product estimates. Math. Z. **271**(1–2), 63–93 (2012)
4. Covert, D., Hart, D., Iosevich, A., Senger, S., Uriarte-Tuero, I.: A Furstenberg-Katznelson-Weiss type theorem on $(d+1)$-point configurations in sets of positive density in finite field geometries. Discret. Math. **311**(6), 423–430 (2011)
5. Covert, D., Iosevich, A., Pakianathan, J.: Geometric configurations in the ring of integers modulo p^l. Indiana Univ. Math. J. **61**(5), 1949–1969 (2012)
6. Erdős, P.: On sets of distances of n points. Am. Math. Mon. **53**, 248–250 (1946)
7. Greenleaf, A., Iosevich, A., Liu, B., Palsson, E.: A group-theoretic viewpoint on Erdos-Falconer problems and the Mattila integral. http://arxiv.org/pdf/1306.3598v3.pdf
8. Guth, L., Katz, N.: On the Erdős distinct distance problem in the plane. Ann. Math. (2) **181**(1), 155–190 (2015)
9. Hart, D., Iosevich, A.: Sums and products in finite fields: an integral geometric viewpoint. Radon transforms, geometry, and wavelets, Contemp. Math., 464. American Mathematical Society, Providence (2008)
10. Hart, D., Iosevich, A., Koh, D., Rudnev, M.: Averages over hyperplanes, sum-product theory in finite fields, and the Erdős-Falconer distance conjecture. Trans. AMS **363**, 3255–3275 (2011)
11. Iosevich, A., Rudnev, M.: Erdős distance problem in vector spaces over finite fields. Trans. Am. Math. Soc. **359**(12), 6127–6142 (2007)
12. Iosevich, A., Rudnev, M., Zhai, Y.: Areas of triangles and Beck's theorem in planes over finite fields. http://arxiv.org/pdf/1205.0107.pdf
13. Pinchasi, R.: The minimum number of distinct areas of triangles determined by a set of n points in the plane. SIAM J. Discret. Math. **22**(2), 828–831 (2008)
14. Solymosi, J., Vu, V.: Distinct distances in high dimensional homogeneous sets, towards a theory of geometric graphs. Contemp. Math. 342. American Mathematical Society, Providence (2004)