On 3-term arithmetic progressions in product sets over finite rings via spectra of graphs

Le Anh Vinh*
University of Education
Vietnam National University, Hanoi
vinhla@vnu.edu.vn

Abstract

Given two sets $\mathcal{A}, \mathcal{B} \subset \mathbb{F}_q$ of elements of the finite field $\mathbb{F}_q$ of q elements, Shparlinski (2008) showed that the product set $\mathcal{AB} = \{ab \mid a \in \mathcal{A}, b \in \mathcal{B}\}$ contains an arithmetic progression of length $k \geq 3$ provided that $k < p$, where $p > 3$ is the characteristic of $\mathbb{F}_q$, and $|\mathcal{A}||\mathcal{B}| \geq 2q^{2-1/(k-1)}$. In this paper, we recover Shparlinski's result for the case of 3-term arithmetic progressions via spectra of product graphs over finite fields. We also illustrate our method in the setting of residue rings. Let m be a large integer and $\mathbb{Z}/m\mathbb{Z}$ be the ring of residues mod m. For any two sets $\mathcal{A}, \mathcal{B} \subset \mathbb{Z}/m\mathbb{Z}$ of cardinality

$$|\mathcal{A}||\mathcal{B}| > m\left(\frac{\tau(m)m}{\gamma(m)^{1/2}} + 1\right),$$

the product set $\mathcal{AB}$ contains a 3-term arithmetic progression where $\gamma(m)$ is the smallest prime divisor of m and $\tau(m)$ is the number of divisors of m. The spectral proofs presented in this paper avoid the use of character and exponential sums, the usual tool to deal with problems of this kind.

1 Introduction

The question of existence of long arithmetic progressions in various sets has been studied extensively in the literature (see [9, Chapters 9–12] for a comprehensive treatment of this topic). One of the most celebrated results of this kind is the theorem of Green and Tao [6] which asserts that there are arbitrary long arithmetic progressions of primes.

Let m be a large integer and $\mathbb{Z}_m = \mathbb{Z}/m\mathbb{Z}$ be the ring of residues mod m. Define the set of units and the set of nonunits in $\mathbb{Z}_m$ by $\mathbb{Z}_m^\times$ and $\mathbb{Z}_m^0$ respectively.

*This research was supported by Vietnam National University - Hanoi project QGTD.13.02.

In the setting of finite fields and residue rings, Green [5] has shown that for some absolute constant $c > 0$ and two subsets $\mathcal{A}, \mathcal{B} \subset \mathbb{Z}_m$ of cardinalities $|\mathcal{A}| \geq \alpha m$ and $|\mathcal{B}| \geq \beta m$, the sum set $\mathcal{A} + \mathcal{B} = \{a + b \mid a \in \mathcal{A}, b \in \mathcal{B}\}$ contains a k-term arithmetic progression with

$$k \geq \exp\left(c\left((\alpha\beta \log m)^{1/2} - \log\log m\right)\right).$$

For the sharpness of this result, Ruzsa [8] showed that for any $\epsilon > 0$ and sufficently large primes p, there is a set $\mathcal{A} \subset \mathbb{Z}_p$ of cardinality $|\mathcal{A}| \geq (1/2 - \epsilon)p$ such that $\mathcal{A} + \mathcal{A}$ does not have an arithmetic progression of length $k \geq \exp((\log p)^{2/3+\epsilon})$. It also follows from a result of Croot, Ruzsa and Schoen [4, Corollary 1] that if $\mathcal{A}, \mathcal{B} \subset \mathbb{Z}_m$ of cardinality $|\mathcal{A}||\mathcal{B}| \geq 6m^{2-2/(k-1)}$ for some integer $k \geq 3$, then sum set $\mathcal{A} + \mathcal{B}$ contains an arithmetic progression $\delta + j\mu, j = 0, \ldots, k-1$, with $\delta \in \mathbb{Z}_m, \mu \in \mathbb{Z}_m^\times$, of length at least k (provided that m is sufficiently large).

1.1 Arithmetic progressions in product sets

For any prime power $q = p^r$ where p is a prime and r is a positive integer, let $\mathbb{F}_q$ be the finite field of q elements. Shparlinski [10] considered a similar problem in product sets

$$\mathcal{AB} = \{ab \mid a \in \mathcal{A}, b \in \mathcal{B}\},$$

where $\mathcal{A}, \mathcal{B} \subset \mathbb{F}_q$. He showed that if $k < p$ and $|\mathcal{A}||\mathcal{B}| \geq 2q^{2-1/(k-1)}$ then $\mathcal{AB}$ contains a k-term arithmetic progression, that is k pairwise distinct elements of the form $\delta + j\mu$, $j = 0, \ldots, k-1$, for some $\delta \in \mathbb{F}_q, \mu \in \mathbb{F}_q^*$. In particular, one needs $p > 3$ and $|\mathcal{A}||\mathcal{B}| \geq 2q^{3/2}$ to ensure that $\mathcal{AB}$ contains a 3-term arithmetic progression. In this paper we reprove this result for the case of 3-term arithmetic progressions via spectra of product graphs over finite fields. Note that in our proof, we will relax the condition $p > 3$ in [10] to $p \geq 3$. More precisely, we have the following theorem.

Theorem 1.1 *Let q be an odd prime power. For any two sets $\mathcal{A}, \mathcal{B} \subset \mathbb{F}_q$ of cardinality*

$$|\mathcal{A}||\mathcal{B}| > q(q^{1/2} + 1),$$

the product set $\mathcal{AB}$ contains a 3-term arithmetic progression.

We also illustrate our method in the setting of residue rings. Let m be a large integer and $\mathbb{Z}_m$ be the ring of residues mod m. Let $\gamma(m)$ be the smallest prime divisor of m, $\omega(m)$ be the number of prime divisors of m, and $\tau(m)$ be the number of divisors of m. Note that our result is only effective when $\gamma(m)$ is large, i.e. $\gamma(m) > m^\epsilon$ for some $\epsilon > 0$. Therefore, we will assume that m is an odd integer. We have the following result on 3-term arithmetic progressions in product sets over finite rings.

Theorem 1.2 *Let m be a large odd integer and $\mathbb{Z}_m$ be the ring of integers modulo m. For any two sets $\mathcal{A}, \mathcal{B} \subset \mathbb{Z}_m$ of cardinality*

$$|\mathcal{A}||\mathcal{B}| > m\left(\frac{\tau(m)m}{\gamma(m)^{1/2}} + 1\right)$$

and $\mathcal{AB} \not\subset \mathbb{Z}_m^0$, the product set $\mathcal{AB}$ contains a 3-term arithmetic progression.

There is no doubt that Shparlinski's method will also work for composite m and will give the same saving of $\gamma(m)^{1/2}$. The spectra proofs presented in this paper avoid the use of character and exponential sums, the usual tool to deal with problems of this kind.

1.2 Product graphs

Our main tools to study the existence of 3-term arithmetic progression in product sets over finite fields and finite rings are product graphs over corresponding spaces. For a graph G (we allow G to have loops but not to have multiple edges between the same two vertices), let $\lambda_1 \geq \lambda_2 \geq \ldots \geq \lambda_n$ be the eigenvalues of its adjacency matrix. The quantity $\lambda(G) = \max\{\lambda_2, -\lambda_n\}$ is called the second eigenvalue of G. A graph $G = (V, E)$ is called an (n, d, λ)-graph if it is d-regular, has n vertices, and the second eigenvalue of G is at most λ.

For any $\delta \in \mathbb{F}_q$, the product graph $\mathcal{P}_{d,q}(\delta)$ is defined as follows. The vertex set of the product graph $\mathcal{P}_{d,q}(\delta)$ is the set $V(\mathcal{P}_{d,q}(\delta)) = \mathbb{F}_q^d \backslash (0, \ldots, 0)$. Two vertices $\boldsymbol{a}$ and $\boldsymbol{b} \in V(\mathcal{P}_{d,q}(\delta))$ are connected by an edge, $(\boldsymbol{a}, \boldsymbol{b}) \in E(\mathcal{P}_{d,q}(\delta))$, if and only if $\boldsymbol{a} \cdot \boldsymbol{b} = \delta$, where $\boldsymbol{a} \cdot \boldsymbol{b} = a_1 b_1 + \ldots + a_d b_d$ is the usual dot product. When $\delta = 0$, the graph is just a blow-up of a variant of the Erdős-Rényi graph. The eigenvalues of this graph are easy to compute (for example, see [1]). We have the following result on the spectra of the product graph when $\delta \in \mathbb{F}_q^*$ (our construction is similar to that of [11]).

Theorem 1.3 *For any $d \geq 2$ and $\delta \in \mathbb{F}^*$, the product graph, $\mathcal{P}_{q,d}(\delta)$, is an*

$$(q^d - 1, q^{d-1}, q^{(d-1)/2}) - \textit{graph}.$$

Let m be a large integer and $\mathbb{Z}_m$ be the ring of residues mod m. Recall that $\gamma(m)$ be the smallest prime divisor of m, $\omega(m)$ be the number of prime divisors of m, and $\tau(m)$ be the number of divisors of m. We identify $\mathbb{Z}_m$ with $\{0, 1, \ldots, m-1\}$. For any $\delta \in \mathbb{Z}_m$, the product graph $\mathcal{P}_{m,d}(\delta)$ is defined as follows. The vertex set of the product graph $\mathcal{P}_{m,d}(\delta)$ is the set $V(\mathcal{P}_{m,d}(\delta)) = \mathbb{Z}_m^d \backslash (\mathbb{Z}_m^0)^d$. Two vertices $\boldsymbol{a}$ and $\boldsymbol{b} \in V(\mathcal{P}_{m,d}(\delta))$ are connected by an edge, $(\boldsymbol{a}, \boldsymbol{b}) \in E(\mathcal{P}_{m,d}(\delta))$, if and only if $\boldsymbol{a} \cdot \boldsymbol{b} = \delta$. When $\delta = 0$, the graph is a variant of Erdős-Rényi graph, which has several interesting applications. We will study this case in a separate paper. We have the following result on the spectra of the product graph when $\delta \in \mathbb{Z}_m^\times$ (our construction is similar to that of [12]).

Theorem 1.4 *For any $d \geq 2$ and $\delta \in \mathbb{Z}_m^\times$, the product graph $\mathcal{P}_{m,d}(\delta)$ is an*

$$\left(m^d - (m-\phi(m))^d, m^{d-1}, \frac{\tau(m)m^{d-1}}{\gamma(m)^{(d-1)/2}}\right) - \textit{graph.}$$

2 Arithmetic progressions over finite fields

2.1 Product graphs over finite fields

We first give a proof of Theorem 1.3. It is easy to see that $\mathcal{P}_{q,d}(\delta)$ is a regular graph of order $q^d - 1$ and valency q^{d-1}. We now compute the eigenvalues of this multigraph (i.e. graph with loops). For any $\boldsymbol{a} \neq \boldsymbol{b} \in \mathbb{F}_q^d \backslash (0, \ldots, 0)$, the system

$$\boldsymbol{a} \cdot \boldsymbol{x} = \boldsymbol{b} \cdot \boldsymbol{x} = \delta, \ \boldsymbol{x} \in \mathbb{F}_q^d \backslash (0, \ldots, 0),$$

has q^{d-2} solutions when $\boldsymbol{a} \neq \omega \boldsymbol{b}$ for all $\omega \in \mathbb{F}_q$, and no solution otherwise. Hence, for any two vertices $\boldsymbol{a} \neq \boldsymbol{b}$, $\boldsymbol{a}$ and $\boldsymbol{b}$ have q^{d-2} common neighbors if $\boldsymbol{a}$ and $\boldsymbol{b}$ are linearly independent, and no common neighbor otherwise. Let A be the adjacency matrix of $\mathcal{P}_{q,d}(\delta)$. It follows that

$$A^2 = q^{d-2}J + (q^{d-1} - q^{d-2})I - q^{d-2}E, \tag{2.1}$$

where J is the all-one matrix, I is the identity matrix, and E is the adjacency matrix of the graph $\mathcal{B}_E$, where for any two distinct vertices $\boldsymbol{a}$ and $\boldsymbol{b} \in V(\mathcal{P}_{q,d}(\delta))$, $(\boldsymbol{a}, \boldsymbol{b})$ is an edge of $\mathcal{B}_E$ if and only if $\boldsymbol{a}$ and $\boldsymbol{b}$ are linearly dependent. Since $\mathcal{P}_{q,d}(\delta)$ is a $(q^d - 1)$-regular graph, q^{d-1} is an eigenvalue of A with the all-one eigenvector $\mathbf{1}$. The graph $\mathcal{P}_{q,d}(\delta)$ is connected therefore the eigenvalue q^{d-1} has multiplicity one. For any $\boldsymbol{a}$ with $\boldsymbol{a} \cdot \boldsymbol{a} \neq 0$, we can choose $\boldsymbol{b}$ such that $\boldsymbol{a}, \boldsymbol{b}$ are linearly independent and $\boldsymbol{a} \cdot \boldsymbol{b} = \delta$. This implies that $\boldsymbol{a}$ and $\boldsymbol{b}$ have q^{d-2} common neighbors. Therefore, the graph is not bipartite when $d \geq 2$. Hence, for any other eigenvalue θ, $|\theta| < q^{d-1}$. Let $\boldsymbol{v}_\theta$ denote the corresponding eigenvector of θ. Note that $\boldsymbol{v}_\theta \in \mathbf{1}^\perp$, so $J\boldsymbol{v}_\theta = 0$. It follows from (2.1) that

$$(\theta^2 - q^{d-1} + q^{d-2})\boldsymbol{v}_\theta = -q^{d-2}E\boldsymbol{v}_\theta. \tag{2.2}$$

Hence, $\boldsymbol{v}_\theta$ is also an eigenvector of E. By the definition of E, the graph $\mathcal{B}_E$ is a disjoint union of $(q^d - 1)/(q - 1)$ copies of the complete graph K_{q-1}. This implies that $\mathcal{B}_E$ has eigenvalues $q - 2$ with multiplicity $(q^d - 1)/(q - 1)$, and -1 with multiplicity $(q^d - 1)(q - 2)/(q - 1)$. One corresponding eigenvector of the eigenvalue $q - 2$ is the all-one eigenvector $\mathbf{1}$ and other corresponding eigenvectors can be chosen in the orthogonal space $\mathbf{1}^\perp$. Plug in to Eq. (2.2), A has eigenvalues q^{d-1} with multiplicity 1, and others eigenvalues are $\pm q^{(d-1)/2}$ and $\pm q^{(d-2)/2}$. The theorem follows.

2.2 Proof of Theorem 1.1

Let G be a (n, d, λ)-graph. It is well known (see [2, Chapter 9] for more details) that if λ is much smaller than the degree d, then the G has certain random-like properties. For two (not necessarily) disjoint subsets of vertices $U, W \subset V$, let $e(U, W)$ be the number of ordered pairs (u, w) such that $u \in U$, $w \in W$, and (u, w) is an edge of G. We recall the following well-known fact (see, for example, [2]).

Lemma 2.1 *([2, Corollary 9.2.5]) Let $G = (V, E)$ be an (n, d, λ)-graph. For any two sets $B, C \subset V$, we have*

$$\left| e(B, C) - \frac{d|B||C|}{n} \right| \leq \lambda \sqrt{|B||C|}.$$

We are now ready to give a spectral proof of Theorem 1.1. It is enough to show that the following equation

$$x_0 y_0 + x_2 y_2 = 2x_1 y_1, x_i \in \mathcal{A}, y_i \in \mathcal{B} \tag{2.3}$$

has a solution given that $x_0, y_0, x_2, y_2 \neq x_1 y_1$. Fix some $x_1 \in \mathcal{A}$ and $y_1 \in \mathcal{B}$ such that $2x_1 y_1 \neq 0$ (note that the characteristic of the field is odd as q is an odd prime power). Let G be the product graph $\mathcal{P}_{q,2}(2x_1 y_1)$. It follows from Theorem 1.3 that G is an $(q^2 - 1, q, \sqrt{q})$-graph. Let $U \equiv V \equiv \mathcal{A} \times \mathcal{B}$, Lemma 2.1 implies that the number of solutions (x_0, y_0, x_2, y_2) satisfying Eq. (2.3) is at least

$$\frac{|\mathcal{A}|^2 |\mathcal{B}|^2 q}{q^2 - 1} - \sqrt{q} |\mathcal{A}||\mathcal{B}|.$$

Note that the number of quadruples (x_0, y_0, x_2, y_2) with $x_0 y_0 = x_2 y_2 = x_1 y_1$ is bounded by $|\mathcal{A}||\mathcal{B}|$ (as for each $(x_0, y_2) \in \mathcal{A} \times \mathcal{B}$, we have at most one choice of (y_0, x_2)). Therefore, the product set $\mathcal{AB}$ contains a 3-term artihmetic progression if

$$|\mathcal{A}||\mathcal{B}| > \frac{q^2 - 1}{q}(\sqrt{q} + 1),$$

concluding the proof of Theorem 1.1.

Note that the solvability of Eq. (2.3) can be derived directly from the proof of [7, Theorem 1.4]. The above proof avoids the use of character and exponential sums, the usual tool to deal with problems of this kind.

3 Arithmetic progressions over finite rings

3.1 Product graphs over finite rings

In this section, we will give a proof of Theorem 1.4. It follows from the definition of the product graph $\mathcal{P}_{m,d}(\delta)$ that $\mathcal{P}_{m,d}(\delta)$ is a graph of order $m^d - (m - \phi(m))^d$.

The valency of the graph is also easy to compute. Given a vertex $\boldsymbol{x} \in V(\mathcal{P}_{m,d}(\delta))$, there exists an index $x_i \in \mathbb{Z}_m^\times$. We can assume that $x_1 \in \mathbb{Z}_m^\times$. We can choose $y_2, \ldots, y_d \in \mathbb{Z}_m$ arbitrarily, then y_1 is determined uniquely such that $\boldsymbol{x} \cdot \boldsymbol{y} = \delta$. Hence, $B_m(d, \delta)$ is a regular graph of valency m^{d-1}. It remains to estimate the eigenvalues of this multigraph (i.e. graph with loops). For any $\boldsymbol{a} \neq \boldsymbol{b} \in \mathbb{Z}_m^d \backslash (\mathbb{Z}_m^0)^d$, we count the number of solutions of the following system

$$\boldsymbol{a} \cdot \boldsymbol{x} \equiv \boldsymbol{b} \cdot \boldsymbol{x} \equiv \delta \mod m,\ \boldsymbol{x} \in \mathbb{Z}_m^d \backslash (\mathbb{Z}_m^0)^d. \tag{3.1}$$

There exist uniquely $n \mid m$ and $\boldsymbol{b}_1 \in (\mathbb{Z}_{m/n})^d \backslash (\mathbb{Z}_{m/n}^0)^d$ such that $\boldsymbol{b} = \boldsymbol{a} + n\boldsymbol{b}_1$. The system (3.1) above becomes

$$\boldsymbol{a} \cdot \boldsymbol{x} \equiv \delta \mod m,\ n\boldsymbol{b}_1 \cdot \boldsymbol{x} \equiv 0 \mod m,\ \boldsymbol{x} \in (\mathbb{Z}_m)^d \backslash (\mathbb{Z}_m^0)^d. \tag{3.2}$$

Let $\boldsymbol{a}_n \in (\mathbb{Z}_{m/n})^d \backslash (\mathbb{Z}_{m/n}^0)^d \equiv \boldsymbol{a} \mod m/n$, $\boldsymbol{x}_n \in (\mathbb{Z}_{m/n})^d \backslash (\mathbb{Z}_{m/n}^0)^d \equiv \boldsymbol{x} \mod m/n$ and $\delta_n \equiv \delta \mod m/n$. To solve (3.2), we first solve the following system

$$\boldsymbol{a}_n \cdot \boldsymbol{x}_n \equiv \delta_n \mod m/n,\ \boldsymbol{b}_1 \cdot \boldsymbol{x}_n \equiv 0 \mod m/n,\ \boldsymbol{x}_n \in (\mathbb{Z}_{m/n})^d \backslash (\mathbb{Z}_{m/n}^0)^d. \tag{3.3}$$

The system (3.3) has no solution when $\boldsymbol{a}_n \equiv t\boldsymbol{b}_1 \mod p$ for some prime $p \mid (m/n)$ and $t \in \mathbb{Z}_m^\times$; and $(m/n)^{d-2}$ solutions otherwise. For each solution $\boldsymbol{x}_n$ of (3.3), putting back into the system

$$\boldsymbol{a} \cdot \boldsymbol{x} \equiv \delta \mod m,\ \boldsymbol{x} \equiv \boldsymbol{x}_n \mod m/n, \tag{3.4}$$

gives us n^{d-1} solutions of the system (3.2). Hence, the system (3.2) has $m^{d-2}n$ solutions when $\boldsymbol{a}_n \not\equiv t\boldsymbol{b}_1 \mod p$ and no solution otherwise. Let A be the adjacency matrix of $\mathcal{P}_{m,d}(\delta)$, it follows that

$$A^2 = m^{d-2}J + (m^{d-1} - m^{d-2})I - m^{d-2} \sum_{\substack{n \mid m \\ 1 \leq n < m}} E_n + \sum_{\substack{n \mid m \\ 1 < n < m}} (m^{d-2}n - m^{d-2})F_n, \tag{3.5}$$

where J is the all-one matrix, I is the identity matrix, E_n is the adjacency matrix of the graph $B_{E,n}$, where for any two vertices $\boldsymbol{a}, \boldsymbol{b} \in V(\mathcal{P}_{m,d}(\delta))$, $(\boldsymbol{a}, \boldsymbol{b})$ is an edge of $B_{E,n}$ if and only if $\boldsymbol{b} = \boldsymbol{a} + n\boldsymbol{b}_1$, $\boldsymbol{b}_1 \in (\mathbb{Z}_{m/n})^d \backslash (\mathbb{Z}_{m/n}^0)^d$ and $\boldsymbol{a}_n \equiv t\boldsymbol{b}_1 \mod p$ for some prime $p \mid (m/n)$, and F_n is the adjacency matrix of the graph $B_{F,n}$, where for any two vertices $\boldsymbol{a}, \boldsymbol{b} \in V(\mathcal{P}_{m,d}(\delta))$, $(\boldsymbol{a}, \boldsymbol{b})$ is an edge of $B_{F,n}$ if and only if $\boldsymbol{b} = \boldsymbol{a} + n\boldsymbol{b}_1$, $\boldsymbol{b}_1 \in (\mathbb{Z}_{m/n})^d \backslash (\mathbb{Z}_{m/n}^0)^d$ and $\boldsymbol{a}_n \not\equiv t\boldsymbol{b}_1 \mod p$ for any prime $p \mid (m/n)$.

Therefore, $B_{E,n}$ is a regular graph of valency at most

$$\sum_{p \mid (m/n),\ p \in \mathcal{P}} (p-1) \left(\frac{m}{np}\right)^d < \omega(m)(m/n)^d \gamma(m)^{1-d}.$$

Hence absolute values of eigenvalues of E_n are bounded by $\omega(m)(m/n)^d\gamma(m)^{1-d}$. Besides, it is clear that absolute values of eigenvalues of F_n are at most $(m/n)^d$. Since $\mathcal{P}_{m,d}(\delta)$ is a m^{d-1}-regular graph, m^{d-1} is an eigenvalue of A with the all-one eigenvector $\mathbf{1}$. The graph $\mathcal{P}_{m,d}(\delta)$ is connected therefore the eigenvalue m^{d-1} has multiplicity one. Since the graph $\mathcal{P}_{m,d}(\delta)$ contains (many) triangles, it is not bipartite. Hence, for any other eigenvalue θ, $|\theta| < m^{d-1}$. Let v_θ denote the corresponding eigenvector of θ. Note that $v_\theta \in \mathbf{1}^\perp$, so $Jv_\theta = 0$. It follows from (3.5) that

$$(\theta^2 - m^{d-1} + m^{d-2})v_\theta = \left(m^{d-2} \sum_{\substack{n|m \\ 1\le n<m}} E_n - \sum_{\substack{n|m \\ 1<n<m}} (m^{d-2}n - m^{d-2})F_n \right) v_\theta.$$

Hence, v_θ is also an eigenvalue of

$$m^{d-2} \sum_{\substack{n|m \\ 1\le n<m}} E_n - \sum_{\substack{n|m \\ 1<n<m}} (m^{d-2}n - m^{d-2})F_n$$

Since eigenvalues of sum of matrices are bounded by sum of largest eigenvalues of summands. We have

$$\begin{aligned}
\theta^2 &\le m^{d-1} - m^{d-2} + m^{d-2} \sum_{\substack{n|m \\ 1\le n<m}} \omega(m)(m/n)^d\gamma(m)^{1-d} \\
&\quad + \sum_{\substack{n|m \\ 1<n<m}} (m^{d-2}n - m^{d-2})(m/n)^d \\
&< m^{d-1} + \omega(m)(\tau(m)-1)m^{2d-2}\gamma(m)^{1-d} + \sum_{\substack{n|m \\ 1<n<m}} m^{2d-2}n^{1-d} \\
&< (\omega(m)+1)(\tau(m)-1)m^{2d-2}\gamma(m)^{1-d} \\
&\le \tau(m)^2 m^{2d-2}\gamma(m)^{1-d}.
\end{aligned}$$

The theorem follows.

3.2 Proof of Theorem 1.2

We are now ready to give a proof of Theorem 1.2. It is enough to show that the following equation

$$x_0y_0 + x_2y_2 = 2x_1y_1, x_i \in \mathcal{A}, y_i \in \mathcal{B} \tag{3.6}$$

has a solution given that $x_0, y_0, x_2, y_2 \neq x_1y_1$. Fix some $x_1 \in \mathcal{A}$ and $y_1 \in \mathcal{B}$ such that $2x_1y_1 \in \mathbb{Z}_m^\times$. Let G be the product graph $\mathcal{P}_{m,2}(2x_1y_1)$. It follows

from Theorem 1.4 that G is an $\left(m^2-(m-\phi(m))^2, m, \frac{\tau(m)m}{\gamma(m)^{1/2}}\right)$-graph. Let $U \equiv V \equiv \mathcal{A}\times\mathcal{B}$, Lemma 2.1 implies that the number of solutions (x_0, y_0, x_2, y_2) satisfying Eq. (2.3) is at least

$$\frac{|\mathcal{A}|^2|\mathcal{B}|^2 m}{m^2-(m-\phi(m))^2} - \frac{\tau(m)m}{\gamma(m)^{1/2}}|\mathcal{A}||\mathcal{B}|.$$

Note that the number of quadtuples (x_0, y_0, x_2, y_2) with $x_0y_0 = x_2y_2 = x_1y_1$ is bounded by $|\mathcal{A}||\mathcal{B}|$ (as for each $(x_0, y_2) \in \mathcal{A}\times\mathcal{B}$, we have at most one choice of (y_0, x_2)). Therefore, the product set $\mathcal{AB}$ contains a 3-term artihmetic progression if

$$|\mathcal{A}||\mathcal{B}| > \frac{m^2-(m-\phi(m))^2}{m}\left(\frac{\tau(m)m}{\gamma(m)^{1/2}}+1\right),$$

concluding the proof of Theorem 1.2.

Note that the solvability of Eq. (3.6) can be derived directly from the proof of [3, Theorem 1.3.2]. The above proof avoids the use of exponential sums, the usual tool to deal with problems of this kind.

References

[1] N. Alon and M. Krivelevich, Constructive bounds for a Ramsey-type problem, *Graphs and Combinatorics* **13** (1997), 217-225.

[2] N. Alon and J. H. Spencer, *The probabilistic method*, 2nd ed., Willey-Interscience, 2000.

[3] D. Covert, A. Iosevich and J. Pakianathan, Geometric configurations in the ring of integers modulo p^l, *Indiana University Mathematics Journal*, to appear.

[4] E. Croot, I. Z. Ruzsa and T. Schoen, Arithmetic progressions in sparse sumsets, Combinatorial Number Theory, Walter de Gruyter, 2007, 157-164.

[5] B. J. Green, Arithmetic progressions in sumsets, *Geom. and Func. Anal.*, **3** (2002), 584-597.

[6] B. Green and T. Tao, The primes contain arbitrarily long arithmetic progressions, *Annals of Math.*, **167**(2) (2008), 481–547.

[7] D. Hart and A. Iosevich, Sums and products in finite fields: an integral geometric viewpoint, *Contemporary Mathematics: Radon transforms, geometry, and wavelets*, **464** (2008).

[8] I. Z. Ruzsa, Arithmetic progressions in sumsets, *Acta Arith.*, **60** (1991), 191202.

[9] T. Tao and V. Vu, *Additive combinatorics*, Cambridge Univ. Press, Cambridge, 2006.

[10] I. Shparlinski, Arithmetic and geometric progressions in product sets over finite fields, *Bulletin of the Australian Mathematical Society*, **78** (2008), 357–364.

[11] L. A. Vinh, The solvability of norm, bilinear and quadratic equations over finite fields via spectra of graphs, *Forum Mathematicum*, DOI: 10.1515/form.2011.155.

[12] L. A. Vinh, Product graphs, sum-product graphs and sum-product estimates over finite rings, *Forum Mathematicum*, DOI: 10.1515/forum-2012-0177.