

ARITHMETIC AND GEOMETRIC PROGRESSIONS IN PRODUCT SETS OVER FINITE FIELDS

IGOR E. SHPARLINSKI

(Received 28 December 2007)

Abstract

Given two sets $\mathcal{A}, \mathcal{B} \subseteq \mathbb{F}_q$ of elements of the finite field \mathbb{F}_q of q elements, we show that the product set

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

contains an arithmetic progression of length $k \geq 3$ provided that $k < p$, where p is the characteristic of \mathbb{F}_q , and $\#\mathcal{A}\mathcal{B} \geq 3q^{2d-2/k}$. We also consider geometric progressions in a shifted product set $\mathcal{A}\mathcal{B} + h$, for $f \in \mathbb{F}_q$, and obtain a similar result.

2000 Mathematics subject classification: primary 11T30; secondary 11B83, 11T23.

Keywords and phrases: arithmetic progressions, geometric progressions, product sets, character sums.

1. Introduction

There is a very extensive variety of results establishing the existence of long arithmetic progressions that occur in various sets. One of the most celebrated special cases of this problem is the question about arithmetic progressions that occur in sufficiently dense sets of integers; see [9, Chs 10 and 11] for an exhaustive treatment of this problem.

Furthermore, this problem has also been considered for sum sets

$$\mathcal{A} + \mathcal{B} = \{a + b \mid a \in \mathcal{A}, b \in \mathcal{B}\}.$$

One can find a detailed outline of recent achievements in this direction in [9, Ch. 12].

For the set of primes a striking result, due to Green and Tao [5], asserts that there are arbitrary long arithmetic progressions of primes.

Although most commonly these questions have been considered for sets of integers, there are also several very significant results for sets of elements of finite fields and residue rings. For example, Green [4] has shown that for some absolute constant $c > 0$ and two subsets $\mathcal{A}, \mathcal{B} \subseteq \mathbb{Z}/m\mathbb{Z}$ of the residue ring modulo a sufficiently large positive

This work was supported by ARC grant DP0556431.

© 2009 Australian Mathematical Society 0004-9727/09 \$A2.00 + 0.00

integer m , of cardinalities $\#\mathcal{A} \geq \alpha m$ and $\#\mathcal{B} \geq \beta m$, the sum set $\mathcal{A} + \mathcal{B}$ contains a k -term arithmetic progression with

$$k \geq \exp 3(c((\alpha\beta \log m)^{1/2} - \log \log m)).$$

It has also been shown by Ruzsa [8] that for any $\varepsilon > 0$ and sufficiently large prime p there is a set $\mathcal{A} \subseteq \mathbb{Z}/p\mathbb{Z}$ of cardinality $\#\mathcal{A} \geq (0.5 - \varepsilon)p$ such that $\mathcal{A} + \mathcal{A}$ does not have an arithmetic progression of length

$$k \geq \exp((\log p)^{2/3+\varepsilon}).$$

It also follows from a result of Croot *et al.* [3, Corollary 1] that if $\mathcal{A}, \mathcal{B} \subseteq \mathbb{Z}/m\mathbb{Z}$ are such that

$$\#\mathcal{A}\#\mathcal{B} \geq 6m^{2-2/(k-1)} \quad (1)$$

for some integer $k \geq 3$, then set $\mathcal{A} + \mathcal{B}$ contains an arithmetic progression $\lambda + j\mu$, $j = 0, \dots, k - 1$, with $\lambda \in \mathbb{F}_q$, $\mu \in \mathbb{F}_q^*$, of length at least k (provided that N is large enough).

Here we consider product sets

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

where $\mathcal{A}, \mathcal{B} \subseteq \mathbb{F}_q$ are sets of elements of the finite field \mathbb{F}_q of q elements. We show that if

$$\#\mathcal{A}\#\mathcal{B} \geq 2q^{2-1/(k-1)}, \quad (2)$$

then $\mathcal{A}\mathcal{B}$ contains a k -term geometric progression, that is, there are k pairwise distinct elements of the form $\lambda\mu^j$, $j = 0, \dots, k - 1$, for some $\lambda, \mu \in \mathbb{F}_q^*$. Note that the bound (2) is of the same shape as (1) even if they are based on different techniques; in particular, they are nontrivial up to the values of k of order $\log m$ and $\log q$, respectively.

Furthermore, Borenstein and Croot [2] have studied the existence of long geometric progressions in sufficiently ‘massive’ subsets $\mathcal{S} \subseteq \mathcal{A} + \mathcal{B}$ of a sum set. For the easier case when $\mathcal{S} = \mathcal{A} + \mathcal{B}$ stronger results are given by Ahmadi and Shparlinski [1], where several variations of this problem are also considered.

Certainly the existence of long geometric progressions in product sets $\mathcal{A}\mathcal{B}$ for $\mathcal{A}, \mathcal{B} \subseteq \mathbb{F}_q$ is essentially equivalent to the problem of the existence of long geometric progressions in sum sets in the residue ring $\mathbb{Z}/(q - 1)\mathbb{Z}$. However, the question about geometric progressions in shifted product sets

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

where $h \in \mathbb{F}_q$, seems to be more interesting and we address it as well.

2. Arithmetic progressions in product sets

THEOREM 1. For any integer k with $p > k \geq 3$, where p is the characteristic of \mathbb{F}_q , and any two sets $\mathcal{A}, \mathcal{B} \subseteq \mathbb{F}_q$ with

$$\#\mathcal{A}\#\mathcal{B} \geq (k - 1)^{2/(k-1)}q^{2-1/(k-1)},$$

the product set $\mathcal{A}\mathcal{B}$ contains a k -term arithmetic progression.

PROOF. It is enough to show that the system of equations

$$\lambda + (j - 1)\mu = a_j b_j, \quad \lambda \in \mathbb{F}_q, \mu \in \mathbb{F}_q^*, a_j \in \mathcal{A}, b_j \in \mathcal{B}, j = 1, \dots, k, \quad (3)$$

has a solution.

Let \mathcal{X} be the set of all $q - 1$ multiplicative characters of \mathbb{F}_q ; see [7, Ch. 3] for a background. Using the orthogonality property of characters (see [7, Section 3.1]), we write the following for the number of solutions T to Equation (3):

$$\begin{aligned} T &= \frac{1}{(q - 1)^k} \sum_{\lambda \in \mathbb{F}_q} \sum_{\mu \in \mathbb{F}_q^*} \sum_{a_1, \dots, a_k \in \mathcal{A}} \sum_{b_1, \dots, b_k \in \mathcal{B}} \prod_{j=1}^k \sum_{\chi_j \in \mathcal{X}} \chi_j(\lambda + (j - 1)\mu) \overline{\chi_j}(a_j b_j) \\ &= \frac{1}{(q - 1)^k} \sum_{\lambda \in \mathbb{F}_q} \sum_{\mu \in \mathbb{F}_q^*} \sum_{a_1, \dots, a_k \in \mathcal{A}} \sum_{b_1, \dots, b_k \in \mathcal{B}} \sum_{\chi_1, \dots, \chi_k \in \mathcal{X}} \\ &\quad \times \prod_{j=1}^k \chi_j(\lambda + (j - 1)\mu) \overline{\chi_j}(a_j b_j), \end{aligned}$$

where $\overline{\chi}$ is the complex conjugate character. After changing the order of summation and separating the term $q(q - 1)(\#\mathcal{A}\#\mathcal{B})^k / (q - 1)^k$ corresponding to the case when all characters χ_1, \dots, χ_k are principal, we obtain

$$\begin{aligned} T - \frac{q(\#\mathcal{A}\#\mathcal{B})^k}{(q - 1)^{k-1}} &= \frac{1}{(q - 1)^k} \sum_{\chi_1, \dots, \chi_k \in \mathcal{X}}^* \left(\sum_{\lambda \in \mathbb{F}_q} \sum_{\mu \in \mathbb{F}_q^*} \prod_{i=1}^k \chi_i(\lambda + (i - 1)\mu) \right) \\ &\quad \times \prod_{j=1}^k \left(\sum_{a_j \in \mathcal{A}} \overline{\chi_j}(a_j) \sum_{b_j \in \mathcal{B}} \overline{\chi_j}(b_j) \right), \end{aligned}$$

where \sum^* means that the term where all characters χ_1, \dots, χ_k are principal is excluded from the summation.

Furthermore,

$$\begin{aligned} \sum_{\lambda \in \mathbb{F}_q} \sum_{\mu \in \mathbb{F}_q^*} \prod_{i=1}^k \chi_i(\lambda + (i-1)\mu) &= \sum_{\mu \in \mathbb{F}_q^*} \sum_{\lambda \in \mathbb{F}_q} \prod_{i=1}^k \chi_i(\lambda + (i-1)\mu) \\ &= \sum_{\mu \in \mathbb{F}_q^*} \sum_{\lambda \in \mathbb{F}_q} \prod_{i=1}^k \chi_i(\lambda\mu + (i-1)\mu) \\ &= \sum_{\mu \in \mathbb{F}_q^*} \prod_{i=1}^k \chi_i(\mu) \sum_{\lambda \in \mathbb{F}_q} \prod_{i=1}^k \chi_i(\lambda + i - 1). \end{aligned}$$

Again, the orthogonality property of characters, see [7, Section 3.1], implies that the sum over μ vanishes unless χ_1, \dots, χ_k is the trivial character χ_0 , in which case it is equal to $q - 1$.

Since $k < p$ we see that the Weil bound applies to the sum over λ (see [7, Theorem 11.23]) and yields the inequality

$$\left| \sum_{\lambda \in \mathbb{F}_q} \prod_{i=1}^k \chi_i(\lambda + i - 1) \right| \leq (k - 1)q^{1/2}.$$

Therefore,

$$\left| T - \frac{q(\#\mathcal{A}\#\mathcal{B})^k}{(q - 1)^{k-1}} \right| \leq \frac{(k - 1)q^{1/2}}{(q - 1)^{k-1}} \sum_{\substack{\chi_1, \dots, \chi_k \in \mathcal{X} \\ \chi_1 \dots \chi_k = \chi_0}}^* \prod_{j=1}^k \left(\left| \sum_{a_j \in \mathcal{A}} \chi_j(a_j) \right| \left| \sum_{b_j \in \mathcal{B}} \chi_j(b_j) \right| \right).$$

Since χ_k is uniquely defined when $\chi_1 \dots \chi_{k-1}$ are fixed, then, using the trivial estimate

$$\left| \sum_{a_j \in \mathcal{A}} \chi_j(a_j) \right| \left| \sum_{b_j \in \mathcal{B}} \chi_j(b_j) \right| \leq \#\mathcal{A}\#\mathcal{B},$$

we obtain

$$\begin{aligned} &\left| T - \frac{q(\#\mathcal{A}\#\mathcal{B})^k}{(q - 1)^{k-1}} \right| \\ &\leq \frac{(k - 1)q^{1/2}\#\mathcal{A}\#\mathcal{B}}{(q - 1)^{k-1}} \sum_{\chi_1, \dots, \chi_{k-1} \in \mathcal{X}}^* \prod_{j=1}^{k-1} \left(\left| \sum_{a_j \in \mathcal{A}} \chi_j(a_j) \right| \left| \sum_{b_j \in \mathcal{B}} \chi_j(b_j) \right| \right) \\ &\leq \frac{(k - 1)q^{1/2}\#\mathcal{A}\#\mathcal{B}}{(q - 1)^{k-1}} \sum_{\chi_1, \dots, \chi_{k-1} \in \mathcal{X}} \prod_{j=1}^{k-1} \left(\left| \sum_{a_j \in \mathcal{A}} \chi_j(a_j) \right| \left| \sum_{b_j \in \mathcal{B}} \chi_j(b_j) \right| \right). \end{aligned}$$

Since the last sum is the $(k - 1)$ th power of the same sum,

$$\left| T - \frac{q(\#\mathcal{A}\#\mathcal{B})^k}{(q - 1)^{k-1}} \right| \leq \frac{(k - 1)q^{1/2}\#\mathcal{A}\#\mathcal{B}}{(q - 1)^{k-1}} \left(\sum_{\chi \in \mathcal{X}} \left| \sum_{a \in \mathcal{A}} \chi(a) \right| \left| \sum_{b \in \mathcal{B}} \chi(b) \right| \right)^{k-1}. \tag{4}$$

Applying the Cauchy inequality, we derive

$$\begin{aligned} \left(\sum_{\chi \in \mathcal{X}} \left| \sum_{a \in \mathcal{A}} \chi(a) \right| \left| \sum_{b \in \mathcal{B}} \chi(b) \right| \right)^2 &\leq \sum_{\chi \in \mathcal{X}} \left| \sum_{a \in \mathcal{A}} \chi(a) \right|^2 \sum_{\chi \in \mathcal{X}} \left| \sum_{b \in \mathcal{B}} \chi(b) \right|^2 \\ &= \sum_{a_1, a_2 \in \mathcal{A}} \sum_{\chi \in \mathcal{X}} \chi(a_1) \overline{\chi}(a_2) \sum_{b_1, b_2 \in \mathcal{B}} \sum_{\chi \in \mathcal{X}} \chi(b_1) \overline{\chi}(b_2). \end{aligned}$$

Now, using the orthogonality property of characters yet one more time, we see that each of the inner sums is equal to $q - 1$ for $a_1 = a_2$ and $b_1 = b_2$, respectively, and is equal to 0 otherwise. Therefore,

$$\sum_{\chi \in \mathcal{X}} \left| \sum_{a \in \mathcal{A}} \chi(a) \right| \left| \sum_{b \in \mathcal{B}} \chi(b) \right| \leq (q - 1) \sqrt{\#\mathcal{A}\#\mathcal{B}},$$

which, after substitution in (4), yields the inequality

$$\left| T - \frac{q(\#\mathcal{A}\#\mathcal{B})^k}{(q - 1)^{k-1}} \right| \leq (k - 1)q^{1/2}(\#\mathcal{A}\#\mathcal{B})^{(k+1)/2}.$$

We now see that $T > 0$ provided that

$$\frac{q(\#\mathcal{A}\#\mathcal{B})^k}{(q - 1)^{k-1}} > (k - 1)q^{1/2}(\#\mathcal{A}\#\mathcal{B})^{(k+1)/2}$$

or

$$(\#\mathcal{A}\#\mathcal{B})^{(k-1)/2} > (k - 1)(q - 1)^{k-1}q^{-1/2},$$

which concludes the proof. □

Since

$$(k - 1)^{2/(k-1)} \leq 2$$

for $k \geq 3$, we see that (2) implies the condition of Theorem 1.

We notice that Theorem 1 implies that product sets of dense sets contain long arithmetic progressions.

COROLLARY 2. *Let $q = p$ be prime. For any $\alpha, \beta > 0$ there exists $\kappa > 0$ such that, for a sufficiently large prime $q = p$ and any sets $\mathcal{A}, \mathcal{B} \subseteq \mathbb{F}_p$ with*

$$\#\mathcal{A} \geq \alpha p, \quad \#\mathcal{B} \geq \beta p,$$

the product set $\mathcal{A}\mathcal{B}$ contains a k -term arithmetic progression of length $k \geq \kappa \log p$.

3. Geometric progressions in shifted product sets

THEOREM 3. For any integer $k \geq 3$, any two sets $\mathcal{A}, \mathcal{B} \subseteq \mathbb{F}_q$ with

$$\#\mathcal{A}\#\mathcal{B} \geq (4k - 4)^{2/(k-1)} q^{2-1/(k-1)},$$

and any $h \in \mathbb{F}_q^*$, the shifted product set $\mathcal{A}\mathcal{B} + h$ contains a k -term geometric progression.

PROOF. We can assume that

$$k \leq \frac{1}{4}q^{1/2} + 1 \tag{5}$$

since otherwise the result is trivial. Since we also have $k \geq 3$ this implies that

$$q \geq 67. \tag{6}$$

Let \mathcal{M} be the set of $\mu \in \mathbb{F}_q^*$ for which $1, \mu, \dots, \mu^{k-1}$ are pairwise distinct. Clearly

$$q - 1 \geq \#\mathcal{M} = q - 2 - \sum_{j=2}^{k-1} (j - 1) = q - 2 - \frac{(k - 1)(k - 2)}{2}. \tag{7}$$

As in the proof of Theorem 1, we note that it is enough to show that the system of equations

$$\lambda\mu^{j-1} = a_j b_j + h, \quad \lambda \in \mathbb{F}_q^*, \mu \in \mathcal{M}, a_j \in \mathcal{A}, b_j \in \mathcal{B}, j = 1, \dots, k, \tag{8}$$

has a solution.

Arguing as in the proof of Theorem 1, we obtain the following result for the number of solutions Q to Equation (3):

$$\begin{aligned} Q - \frac{(\#\mathcal{A}\#\mathcal{B})^k \#\mathcal{M}}{(q - 1)^{k-1}} &= \frac{1}{(q - 1)^k} \sum_{\chi_1, \dots, \chi_k \in \mathcal{X}}^* \left(\sum_{\lambda, \mu \in \mathbb{F}_q^*} \prod_{i=1}^k \chi_i(\lambda\mu^{i-1} - h) \right) \\ &\times \prod_{j=1}^k \left(\sum_{a_j \in \mathcal{A}} \overline{\chi_j}(a_j) \sum_{b_j \in \mathcal{B}} \overline{\chi_j}(b_j) \right). \end{aligned} \tag{9}$$

We note that

$$\sum_{\lambda \in \mathbb{F}_q^*} \sum_{\mu \in \mathcal{M}} \prod_{i=1}^k \chi_i(\lambda\mu^{i-1} - h) = \sum_{\lambda \in \mathbb{F}_q^*} \chi_1(\lambda - h) \prod_{i=2}^k \overline{\chi_i}(\lambda) \sum_{\mu \in \mathcal{M}} \prod_{i=2}^k \chi_i(\mu^{i-1} - h/\lambda).$$

Using (7), we derive

$$\begin{aligned} & \left| \sum_{\lambda \in \mathbb{F}_q^*} \sum_{\mu \in \mathcal{M}} \prod_{i=1}^k \chi_i(\lambda \mu^{i-1} - h) \right| \\ & \leq \sum_{\lambda \in \mathbb{F}_q^*} \left(\left| \sum_{\mu \in \mathbb{F}_q^*} \prod_{i=2}^k \chi_i(\mu^{i-1} - h/\lambda) \right| + \frac{(k-1)(k-2)}{2} \right) \\ & \leq \sum_{\lambda \in \mathbb{F}_q^*} \left| \sum_{\mu \in \mathbb{F}_q^*} \prod_{i=2}^k \chi_i(\mu^{i-1} - h/\lambda) \right| + \frac{(k-1)(k-2)}{2}(q-1). \end{aligned}$$

We see that the polynomial $X - h/\lambda$ has a common root with the polynomial $X^{i-1} - h/\lambda$, $i = 3, \dots, k$, if and only if $(h/\lambda)^{i-2} = 1$, which happens for at most $i - 2$ values of $\lambda \in \mathbb{F}_q^*$. Therefore, for all but

$$\sum_{i=3}^k (i-2) = \frac{(k-1)(k-2)}{2}$$

values of $\lambda \in \mathbb{F}_q^*$, the Weil bound applies to the sums over μ (which we estimate trivially as $q - 1$ for the other values of λ). Therefore,

$$\begin{aligned} & \left| \sum_{\lambda \in \mathbb{F}_q^*} \sum_{\mu \in \mathcal{M}} \prod_{i=1}^k \chi_i(\lambda \mu^{i-1} - h) \right| \\ & \leq (k-1)(q-1)q^{1/2} + (k-1)(k-2)(q-1) < 2(k-1)(q-1)q^{1/2} \end{aligned}$$

under the conditions (5) and (6).

Inserting this bound into (9), we obtain

$$\left| Q - \frac{(\#\mathcal{A}\#\mathcal{B})^k \#\mathcal{M}}{(q-1)^{k-1}} \right| = \frac{2(k-1)q^{1/2}}{(q-1)^{k-1}} \sum_{\chi_1, \dots, \chi_k \in \mathcal{X}}^* \prod_{j=1}^k \left(\sum_{a_j \in \mathcal{A}} \overline{\chi_j}(a_j) \sum_{b_j \in \mathcal{B}} \overline{\chi_j}(b_j) \right).$$

Now, as in the proof of Theorem 1, we obtain

$$\left| Q - \frac{(\#\mathcal{A}\#\mathcal{B})^k \#\mathcal{M}}{(q-1)^{k-1}} \right| < 2(k-1)q^{1/2}(\#\mathcal{A}\#\mathcal{B})^{(k+1)/2}.$$

Using (5) and (6), we derive from (7) that $\#\mathcal{M} \geq (q-1)/2$, so

$$Q > \frac{(\#\mathcal{A}\#\mathcal{B})^k}{2(q-1)^{k-2}} - 2(k-1)q^{1/2}(\#\mathcal{A}\#\mathcal{B})^{(k+1)/2},$$

which concludes the proof. □

We remark that

$$(4k-4)^{2/(k-1)} \leq 8$$

for $k \geq 3$.

Similarly to Corollary 2, we also derive that shifted product sets of dense sets contain long geometric progressions.

COROLLARY 4. *For any $\alpha, \beta > 0$ there exists $\kappa > 0$ such that for any sets $\mathcal{A}, \mathcal{B} \subseteq \mathbb{F}_q$ with*

$$\#\mathcal{A} \geq \alpha q, \quad \#\mathcal{B} \geq \beta q,$$

and any $h \in \mathbb{F}_q^$, the shifted product set $\mathcal{A}\mathcal{B} + h$ contains a k -term geometric progression of length $k \geq \kappa \log q$.*

4. Comments

It is certainly interesting to understand how tight the results of Corollaries 2 and 4 are. For example, using the Burgess bound (see [7, Theorem 12.6]) one sees that if $q = p$ is prime and $\mathcal{A} = \mathcal{B}$ are the sets of quadratic residues modulo p , then the longest arithmetic progression contained in $\mathcal{A}\mathcal{B}$ is of length at most $p^{1/4+o(1)}$.

The above method can easily be adopted to study arithmetic and geometric progressions where one of the parameters λ or μ is fixed. It can also be used to study more general polynomial structures in product sets.

The same technique also applies to sets in residue rings $\mathbb{Z}/m\mathbb{Z}$; however, unless m is square-free, or almost square-free, instead of the Weil bound we only have a much weaker bound of Ismoilov [6] at our disposal. Thus the final results will be weaker than those of Theorems 1 and 3.

It would be interesting to relax the condition $k < p$ in Theorem 1 and thus extend Corollary 2 to arbitrary finite fields.

References

- [1] O. Ahmadi and I. E. Shparlinski, ‘Geometric progressions in sum sets over finite fields’, *Monatsh. Math.* **152** (2007), 177–185.
- [2] E. Croot and E. Borestein, ‘Geometric progressions in thin sets’, Preprint, 2006.
- [3] E. Croot, I. Z. Ruzsa and T. Schoen, ‘Arithmetic progressions in sparse sumsets’, in: *Combinatorial Number Theory* (Walter de Gruyter, Berlin, 2007), pp. 157–164.
- [4] B. J. Green, ‘Arithmetic progressions in sumsets’, *Geom. Funct. Anal.* **3** (2002), 584–597.
- [5] B. Green and T. Tao, ‘The primes contain arbitrarily long arithmetic progressions’, *Ann. of Math.* **167** (2008), 481–547.
- [6] D. Ismoilov, ‘Estimates of complete character sums of polynomials’, *Proc. Steklov Math. Inst., Moscow* **200** (1992), 171–184 (in Russian).
- [7] H. Iwaniec and E. Kowalski, *Analytic Number Theory* (American Mathematical Society, Providence, RI, 2004).
- [8] I. Z. Ruzsa, ‘Arithmetic progressions in sumsets’, *Acta Arith.* **60** (1991), 191–202.
- [9] T. Tao and V. Vu, *Additive Combinatorics* (Cambridge University Press, Cambridge, 2006).

IGOR E. SHPARLINSKI, Department of Computing, Macquarie University, Sydney, NSW 2109, Australia
e-mail: igor@ics.mq.edu.au