

# AN EFFECTIVE LOCAL-GLOBAL PRINCIPLE AND ADDITIVE COMBINATORICS IN FINITE FIELDS

By

BRYCE KERR, JORGE MELLO AND IGOR E. SHPARLINSKI

**Abstract.** We use recent results about linking the number of zeros on algebraic varieties over  $\mathbb{C}$ , defined by polynomials with integer coefficients, and on their reductions modulo sufficiently large primes to study congruences with products and reciprocals of linear forms. This allows us to make some progress towards a question of B. Murphy, G. Petridis, O. Roche-Newton, M. Rudnev and I. D. Shkredov (2019) on an extreme case of the Erdős–Szemerédi conjecture in finite fields.

## 1 Introduction

**1.1 Description of our results** In this paper we give a new application of a recent result due to D’Andrea, Ostafe, Shparlinski and Sombra [7, Theorem 2.1], which establishes an effective link between the number of points on zero-dimensional varieties considered over  $\mathbb{C}$  and also considered in the field  $\mathbb{F}_p$ ; see Lemma 3.1 below.

In particular, we give sharp upper bounds on the number of solutions to some multiplicative and additive congruences modulo primes with variables from sets with small doubling; see Section 2.1.

These results complement those of Grosu [10], who has previously applied a similar principle which allows one to study arithmetic in subsets of a finite field by lifting to zero characteristic. The results of Grosu [10] restrict one to consider sets  $\mathcal{A} \subseteq \mathbb{F}_p$  of triple logarithmic size; see (2.5) below. Our results (see Section 2.1) extend the cardinality of the sets considered in some applications (see [10, Section 4]) to the range  $|\mathcal{A}| \leq p^\delta$  for some fixed  $\delta > 0$  which is given explicitly and depends only on the size of  $|\mathcal{A} + \mathcal{A}|$ . We also obtain sharper quantitative bounds for  $\delta$  which hold for almost all primes (in the sense of relative asymptotic density). For example, we prove that if such a set has small doubling, then its product set is of almost largest possible size, see Theorem 2.2 below. This provides some partial

progress towards a question raised by Murphy, Petridis, Roche-Newton, Rudnev and Shkredov [15, Question 2] which has also been considered by Shkredov [16, Corollary 2] in a different context and can be considered a mod  $p$  variant of a few sums, many products estimate due to Elekes and Ruzsa [8]; see Section 2.2 for more details.

We note that some arithmetic applications of [7, Theorem 2.1] have already been given in [4, 7] (to periods of orbits of some dynamical systems) as well as [17] (to torsions of some points on elliptic curves).

**1.2 General notation.** Throughout this work  $\mathbb{N} = \{1, 2, \dots\}$  is the set of positive integers.

For a field  $K$ , we use  $\overline{K}$  to denote the algebraic closure of  $K$ .

For a prime  $p$ , we use  $\mathbb{F}_p$  to denote the finite field of  $p$  elements and  $\mathbb{F}_p^*$  the multiplicative subgroup of  $\mathbb{F}_p$ .

We freely switch between equations in  $\mathbb{F}_p$  and congruences modulo  $p$ .

The letters  $k, \ell, m$  and  $n$  (with or without subscripts) are always used to denote positive integers; the letter  $p$  (with or without subscripts) is always used to denote a prime.

As usual, for given quantities  $U$  and  $V$ , the notations  $U \ll V$ ,  $V \gg U$  and  $U = O(V)$  are all equivalent to the statement that the inequality  $|U| \leq cV$  holds with some constant  $c > 0$ , which may depend on the integer parameter  $d$ .

Furthermore  $V = U^{o(1)}$  means that  $\log |V| / \log U \rightarrow 0$  as  $U \rightarrow \infty$ .

We use  $|\mathcal{S}|$  to denote the cardinality of a finite set  $\mathcal{S}$ .

For a generic point  $\mathbf{x} \in \mathbb{R}^d$ , we write  $x_i$  for the  $i$ -th coordinate of  $\mathbf{x}$ . For example, if  $\alpha, \mathbf{h} \in \mathbb{R}^d$  then

$$\alpha = (\alpha_1, \dots, \alpha_d) \quad \text{and} \quad \mathbf{h} = (h_1, \dots, h_d).$$

Let

$$\langle \alpha, \mathbf{h} \rangle = \alpha_1 h_1 + \dots + \alpha_d h_d$$

denote the Euclidian inner product and  $\|\mathbf{h}\|$  the Euclidean norm of  $\mathbf{h}$ .

For  $\alpha \in \mathbb{R}^d$  and  $\lambda \in \mathbb{C}$  we let  $\lambda\alpha$  denote scalar multiplication

$$\lambda\alpha = (\lambda\alpha_1, \dots, \lambda\alpha_d).$$

Given a set  $\mathcal{D} \subseteq \mathbb{R}^d$  and  $\lambda > 0$  we define

$$\lambda\mathcal{D} = \{\lambda x : x \in \mathcal{D}\}.$$

## 2 Main results

**2.1 Multiplicative equations over sets with small sumsets.** Let  $p$  be prime and for subsets  $\mathcal{A}, \mathcal{B} \subseteq \overline{\mathbb{F}}_p$  and  $\lambda \in \overline{\mathbb{F}}_p$  we define  $I_p(\mathcal{A}, \mathcal{B}, \lambda)$  by

$$(2.1) \quad I_p(\mathcal{A}, \mathcal{B}, \lambda) = |\{(a, b) \in \mathcal{A} \times \mathcal{B} : ab = \lambda\}|,$$

where the equation  $ab = \lambda$  is in  $\overline{\mathbb{F}}_p$ .

A generalised arithmetic progression  $\mathcal{A}$  (defined in any group) is a set of the form

$$\mathcal{A} = \{\alpha_0 + \alpha_1 h_1 + \dots + \alpha_d h_d : 1 \leq h_i \leq A_i\}.$$

We define the rank of  $\mathcal{A}$  to be  $d$  and say  $\mathcal{A}$  is proper if

$$|\mathcal{A}| = A_1 \cdots A_d.$$

It is convenient to define

$$(2.2) \quad \gamma_s = \frac{1}{(11s + 15)2^{3s+5}}.$$

Since our bounds depend only on  $\max\{A_1, \dots, A_d, B_1, \dots, B_e\}$ , without loss of generality we now assume that

$$A_1 = \dots = A_d = B_1 = \dots = B_e = H.$$

We recall that an integer  $k \neq 0$  is called  $y$ -smooth if all prime divisors of  $k$  do not exceed  $y$ .

**Theorem 2.1.** *Let  $H, d, e$  be positive integers with  $e \leq d$ . There exists a constant  $b_d$  depending only on  $d$ , and an integer  $Z$ , which is  $O(H^{1/\gamma_{d+e+1}})$ -smooth and satisfies*

$$\log Z \ll H^{(d+e)(d+e+2)^2/4} \log H,$$

such that for each prime number  $p \nmid Z$  the following holds. For any generalised arithmetic progressions  $\mathcal{A}, \mathcal{B} \subseteq \overline{\mathbb{F}}_p$  of the form

$$\mathcal{A} = \{\alpha_0 + \alpha_1 h_1 + \dots + \alpha_d h_d : 1 \leq h_i \leq H, i = 1, \dots, d\},$$

$$\mathcal{B} = \{\beta_0 + \beta_1 j_1 + \dots + \beta_e j_e : 1 \leq j_i \leq H, i = 1, \dots, e\},$$

and  $\lambda \in \overline{\mathbb{F}}_p^*$  we have

$$I_p(\mathcal{A}, \mathcal{B}, \lambda) \leq \exp(b_d \log H / \log \log H).$$

The integer  $Z$  in Theorem 2.1 is constructed explicitly in Lemma 4.1 below and is divisible by all primes  $p \leq H^{d+e+o(1)}$  (note that  $o(1)$  here denotes a negative quantity). This is established at the end of the proof of Lemma 4.1.

From Theorem 2.1 we may deduce an estimate which holds for all primes provided our generalised arithmetic progressions are not too large. We also obtain better results for almost all primes. In particular, using the fact that no primes  $p \geq Z$  divide a  $Z$ -smooth integer, we obtain:

**Corollary 2.1.** *Let notation be as in Theorem 2.1. For any prime  $p$  and integer  $H$  satisfying*

$$H \leq C_0(d)p^{7d+e+1},$$

for some constant  $C_0(d)$  depending only on  $d$ , we have

$$I_p(\mathcal{A}, \mathcal{B}, \lambda) \leq \exp(b_d \log H / \log \log H).$$

As a second application, using the fact that any integer  $Z$  has at most  $O(\log Z / \log \log Z)$  prime divisors, we obtain:

**Corollary 2.2.** *Let notation be as in Theorem 2.1. For all but at most  $O(H^{(d+e)^3+(d+e)})$  primes  $p$ , we have*

$$I_p(\mathcal{A}, \mathcal{B}, \lambda) \leq \exp(b_d \log H / \log \log H).$$

We note an important feature of Theorem 2.2: the set of primes is independent of the generalized arithmetic progressions  $\mathcal{A}, \mathcal{B}$ .

Corollaries 2.1 and 2.2 immediately yield an estimate for equations with Kloosterman fractions and squares. Indeed using that over any field and  $\lambda \neq 0$ , if

$$a^{-1} + b^{-1} = \lambda$$

then

$$(a - \lambda^{-1})(b - \lambda^{-1}) = \lambda^{-2},$$

and over any algebraically closed field, if  $\lambda \neq 0$  and  $a, b$  satisfy

$$a^2 + b^2 = \lambda,$$

then

$$(a + ia)(a - ib) = \lambda,$$

where  $i$  is a square root of  $-1$ , we obtain the following results.

**Corollary 2.3.** *With notation and conditions as in either Corollary 2.1 or Corollary 2.2, the number of solutions to the equations*

$$a^{-1} + b^{-1} = \lambda, \quad a \in \mathcal{A}, b \in \mathcal{B},$$

and

$$a^2 + b^2 = \lambda, \quad a \in \mathcal{A}, b \in \mathcal{B},$$

in  $\overline{\mathbb{F}}_p$  are bounded by  $H^{o(1)}$ .

We remark that our method, with minor changes, can allow us to extend our results to equations

$$(2.3) \quad a_1 \cdots a_\nu = \lambda, \quad a_i \in \mathcal{A}_i, \quad i = 1, \dots, \nu, \quad a_i \in \mathcal{A}_i,$$

with any  $\nu \geq 2$  and generalised arithmetic progressions  $\mathcal{A}_1, \dots, \mathcal{A}_\nu \subseteq \mathbb{F}_p$ . A direct application of such techniques gives a poor dependence on the parameter  $\nu$ . An interesting problem is to determine the largest real numbers  $\gamma_{\nu,d}$  such that the number of solutions to (2.3) is bounded by  $(|\mathcal{A}_1| \cdots |\mathcal{A}_\nu|)^{o(1)}$  provided  $\mathcal{A}_1, \dots, \mathcal{A}_\nu$  are generalized arithmetic progressions of rank at most  $d$  satisfying

$$|\mathcal{A}_i| \ll p^{\gamma_{\nu,d}}.$$

## 2.2 Applications to the Erdős–Szemerédi conjecture in finite fields.

As usual, given a set  $\mathcal{A} \subseteq \mathcal{G}$  with a group operation  $*$ , we write

$$\mathcal{A} * \mathcal{A} = \{a * b : a, b \in \mathcal{A}\}.$$

Clearly for sets in rings we can use  $* \in \{+, \times\}$ .

Here we also denote

$$\mathcal{A}^{-1} = \{a^{-1} : a \in \mathcal{A}\}, \quad \mathcal{A}^2 = \{a^2 : a \in \mathcal{A}\}.$$

Combining the above results with some modern results [6, Theorem 4] of additive combinatorics towards the celebrated theorem of Freiman [9], we, in particular, verify the Erdős–Szemerédi conjecture for sets with small sumset and small cardinality. This can be considered an extension of some ideas of Chang [3] into the setting of prime finite fields.

**Theorem 2.2.** *For any fixed  $K \geq 2$  and*

$$\delta = \frac{1}{(44K + 26)2^{12K+8}},$$

*there exist some constants  $b_0(K)$  and  $c_0(K)$ , depending only on  $K$ , such that for each prime  $p$ , if  $\mathcal{A} \subseteq \mathbb{F}_p$  satisfies*

$$|\mathcal{A} + \mathcal{A}| \leq K|\mathcal{A}| \quad \text{and} \quad |\mathcal{A}| \leq c_0(K)p^\delta$$

*then for any  $\lambda \in \mathbb{F}_p^*$  the number of solutions to each of the equations*

$$a_1 a_2 = \lambda, \quad a_1^{-1} + a_2^{-1} = \lambda, \quad a_1^2 + a_2^2 = \lambda$$

*with variables  $a_1, a_2 \in \mathcal{A}$  is  $\exp(b_0(K) \log |\mathcal{A}| / \log \log |\mathcal{A}|)$ .*

An immediate consequence of Theorem 2.2 is an estimate for the cardinality of sets related to the Erdős–Szemerédi conjecture. Indeed, using Theorem 2.2 one has that

$$|\mathcal{A}|^2 = \sum_{\lambda \in \mathcal{A}\mathcal{A}} I_p(\mathcal{A}, \mathcal{A}, \lambda) \leq 2|\mathcal{A}| + \sum_{\substack{\lambda \in \mathcal{A}\mathcal{A} \\ \lambda \not\equiv 0 \pmod p}} I_p(\mathcal{A}, \mathcal{A}, \lambda) \leq |\mathcal{A}\mathcal{A}||\mathcal{A}|^{o(1)}.$$

A similar argument also works for the sets  $\mathcal{A}^{-1} + \mathcal{A}^{-1}$  and we obtain the following result.

**Corollary 2.4.** *With notation and conditions as in Theorem 2.2, for any fixed  $K$  we have*

$$|\mathcal{A}\mathcal{A}| \geq |\mathcal{A}|^{2+o(1)} \quad \text{and} \quad |\mathcal{A}^{-1} + \mathcal{A}^{-1}| \geq |\mathcal{A}|^{2+o(1)}.$$

We note that Corollary 2.4 is a step towards a positive answer to a question raised by Murphy, Petridis, Roche-Newton, Rudnev and Shkredov [15, Question 2] whether for any  $\varepsilon > 0$  there exists some  $\eta(\varepsilon)$  depending only on  $\varepsilon$  with  $\eta(\varepsilon) \rightarrow 0$  as  $\varepsilon \rightarrow 0$ , such that if  $\mathcal{A} \subseteq \mathbb{F}_p$  satisfies  $|\mathcal{A} + \mathcal{A}| \leq |\mathcal{A}|^{1+\varepsilon}$  then

$$|\mathcal{A}\mathcal{A}| \geq |\mathcal{A}|^{2-\eta(\varepsilon)}.$$

Theorem 2.2 confirms this in the extreme case of rapidly decaying (as  $|\mathcal{A}|$  grows) values of  $\varepsilon$ . In other words instead of fixed  $K$  in Corollary 2.4 we can take  $K$  as a very slowly growing function of  $|\mathcal{A}|$ . We also recall that Shkredov [16, Corollary 2] has shown that if

$$(2.4) \quad |\mathcal{A} + \mathcal{A}| \ll |\mathcal{A}|$$

for a set  $\mathcal{A} \subseteq \mathbb{F}_p$  of cardinality  $|\mathcal{A}| \ll p^{13/23}$  then the number of solutions to

$$a_1 a_2 = \lambda, \quad a_1, a_2 \in \mathcal{A},$$

is bounded by  $|\mathcal{A}|^{149/156+o(1)}$ . Clearly, this result and Theorem 2.2 are of similar spirit, however they are incomparable. In particular, the cardinality of the sets considered in [16, Corollary 2] is uniform with respect to the implied constant in (2.4), which is a feature not present in our bound. We refer the reader to [14] for various incidence results related to counting solutions to multiplicative equations with variables belonging to sets with small sumset. Our result does give a direct improvement on Grosu [10, Section 4], who obtains similar estimates to Theorem 2.2 with the condition, which we slightly simplify as

$$(2.5) \quad |\mathcal{A}| \leq \frac{1}{\log 2} \log \log \log p - 1 - \varepsilon,$$

for any  $\varepsilon > 0$  provided that  $p$  is large enough. However, the paper of Grosu [10] contains other interesting results which allow one to lift problems in  $\mathbb{F}_p$  to  $\mathbb{C}$  while preserving more arithmetic information than counting solutions to equations considered in Theorem 2.2.

We now obtain a version of Theorem 2.2 which holds for almost all primes.

**Theorem 2.3.** *Let  $A \geq 3$  be sufficiently large and let  $K \geq 2$  be a fixed integer. For all but at most  $O(A^{8K^3+4K^2} \log A / \log \log A)$  primes  $p$  with*

$$p > c_0(K)A^{2K}$$

*for some sufficiently large constant  $c_0(K)$  depending only on  $K$ , the following holds. If  $\mathcal{A} \subseteq \mathbb{F}_p$  satisfies*

$$|\mathcal{A} + \mathcal{A}| \leq K|\mathcal{A}| \quad \text{and} \quad |\mathcal{A}| \leq A$$

*then for any  $\lambda \in \mathbb{F}_p^*$  the number of solutions to each of the equations*

$$a_1 a_2 = \lambda \quad \text{and} \quad a_1^{-1} + a_2^{-1} = \lambda$$

*with variables  $a_1, a_2 \in \mathcal{A}$  is  $|\mathcal{A}|^{o(1)}$ .*

As before, we obtain a result towards the Erdős–Szemerédi conjecture modulo almost all primes.

**Corollary 2.5.** *With notation and conditions as in Theorem 2.3 we have*

$$|\mathcal{A}\mathcal{A}| \geq |\mathcal{A}|^{2+o(1)} \quad \text{and} \quad |\mathcal{A}^{-1} + \mathcal{A}^{-1}| \geq |\mathcal{A}|^{2+o(1)}.$$

**2.3 Overview of our approach.** We first illustrate the main ideas of our paper in the setting of Corollary 2.1. With  $H$  as in Theorem 2.1, let  $\mathcal{A}, \mathcal{B} \subseteq \mathbb{F}_p$  be generalised arithmetic progressions of rank  $d, e$  respectively and recall we aim to show

$$I_p(\mathcal{A}, \mathcal{B}) = H^{o(1)}.$$

Our main input is the following iterative inequality, see Lemma 4.1, that there exists generalised arithmetic progressions  $\tilde{\mathcal{A}}, \tilde{\mathcal{B}}$  of rank  $\tilde{d}, \tilde{e}$  respectively, satisfying

$$I_p(\mathcal{A}, \mathcal{B}) \ll H^{o(1)} I_p(\tilde{\mathcal{A}}, \tilde{\mathcal{B}}),$$

and

$$\tilde{d} + \tilde{e} < d + e, \quad |\tilde{\mathcal{A}}| |\tilde{\mathcal{B}}| \ll |\mathcal{A}| |\mathcal{B}|.$$

Proceeding by induction on  $d + e$ , the above properties are sufficient to establish the desired result. Suppose  $\mathcal{A}, \mathcal{B} \subseteq \mathbb{F}_p$  are given by

$$\mathcal{A} = \{\alpha_0 + \alpha_1 h_1 + \cdots + \alpha_d h_d : 1 \leq h_i \leq H, i = 1, \dots, d\},$$

$$\mathcal{B} = \{\beta_0 + \beta_1 j_1 + \cdots + \beta_e j_e : 1 \leq j_i \leq H, i = 1, \dots, e\},$$

and for simplicity assume  $\mathcal{A}, \mathcal{B}$  are proper. Hence we aim to count the number of solutions to the equation

$$(2.6) \quad (\alpha_0 + \alpha_1 h_1 + \cdots + \alpha_d h_d)(\alpha_0 + \beta_1 j_1 + \cdots + \beta_e j_e) = \lambda, \\ 1 \leq h_1, \dots, h_d, j_1, \dots, j_e \leq H.$$

Fix a pair

$$(h_{1,0}, \dots, h_{d,0}) \in [1, H]^d, \quad (j_{1,0}, \dots, j_{e,0}) \in [1, H]^e,$$

satisfying

$$(\alpha_0 + \alpha_1 h_{1,0} + \cdots + \alpha_d h_{d,0})(\beta_0 + \beta_1 j_{1,0} + \cdots + \beta_e j_{e,0}) = \lambda,$$

and consider the variety  $V_p \subseteq \overline{\mathbb{F}}^{d+e+2}$  defined by the system of equations

$$(X_0 + X_1 h_1 + \cdots + X_d h_d)(Y_0 + Y_1 j_1 + \cdots + Y_e j_e) \\ - (X_0 + X_1 h_{1,0} + \cdots + X_d h_{d,0})(Y_0 + Y_1 j_{1,0} + \cdots + Y_e j_{e,0}) = 0,$$

such that  $h_1, \dots, h_d, j_1, \dots, j_e$  satisfy (2.6) and in variables  $X_0, \dots, Y_e$ . Let  $V$  denote the corresponding variety over  $\mathbb{C}$ . By assumption, we have

$$(\alpha_0, \dots, \alpha_d, \beta_0, \dots, \beta_e) \in V_p.$$



Assuming  $H$  is sufficiently small in terms of  $p$ , a local-global result of D’Andrea, Ostafe, Shparlinski and Sombra [7], see Lemma 3.1 below, implies that there exists

$$(\rho_0, \dots, \rho_d, \gamma_0, \dots, \gamma_e) \in V.$$

Hence any solution  $h_1, \dots, j_e$  to (2.6) also satisfies

$$(\rho_0 + \rho_1 h_1 + \dots + \rho_d h_d)(\gamma_0 + \gamma_1 j_1 + \dots + \gamma_e j_e) = \lambda_0,$$

for some  $\lambda_0 \in \mathbb{C}$ . A result of Chang [3], see Lemma 3.4 below, implies that there exist  $H^{o(1)}$  possible values for either

$$(2.7) \quad \rho_0 + \rho_1 h_1 + \dots + \rho_d h_d = \mu_1,$$

or

$$\gamma_0 + \gamma_1 j_1 + \dots + \gamma_e j_e = \mu_2.$$

Assuming (2.7), our set of solutions to (2.6) is restricted to the union of  $H^{o(1)}$  cosets of a lattice  $\mathcal{L}$  of rank smaller than  $d$ . After performing basis reduction to  $\mathcal{L}$  and back-substitution, the desired iterative inequality follows.

### 3 Preliminaries

**3.1 Tools from Diophantine geometry.** For a polynomial  $G$  with integer coefficients, its **height** is defined as the logarithm of the maximum of the absolute values of the coefficients of  $G$ . The height of an algebraic number  $\alpha$  is defined as the height of its minimal polynomial (we also set it to 1 for  $\alpha = 0$ ).

We now recall the statement of [7, Theorem 2.1] which underlies our approach.

**Lemma 3.1.** *Let  $G_i \in \mathbb{Z}[T_1, \dots, T_n]$ ,  $i = 1, \dots, s$ ,  $n \geq 1$  be polynomials of degree at most  $r \geq 2$  and height at most  $h$ , whose zero set in  $\mathbb{C}^n$  has a finite number  $\kappa$  of distinct points. Then there is an integer  $\mathfrak{A} \geq 1$  with*

$$\log \mathfrak{A} \leq (11n + 4)r^{3n+1}h + (55r + 99) \log((2n + 5)s)r^{3n+2}$$

*such that, if  $p$  is a prime not dividing  $\mathfrak{A}$ , then the zero set in  $\overline{\mathbb{F}}_p^n$  of the polynomials  $G_i$  reduced modulo  $p$ ,  $i = 1, \dots, s$ , consists of exactly  $\kappa$  distinct points.*

Similar results have previously appeared. For example, Chang [3, Lemma 2.14] has shown the following result. Let

$$\mathcal{V} = \bigcap_{j=1, \dots, s} [F_j = 0]$$

be an affine variety in  $\mathbb{C}^n$  defined by polynomials  $F_j \in \mathbb{Z}[X_1, \dots, X_n], j = 1, \dots, s$ , of height at most  $h$  and let  $F \in \mathbb{Z}[X_1, \dots, X_n]$  be a polynomial of height at most  $h$  such that there is  $\alpha \in \mathcal{V}$  with  $F(\alpha) \neq 0$ . Then there is  $\beta \in \mathcal{V}$  with  $F(\beta) \neq 0$  whose coordinates are algebraic numbers of height  $O(h)$ .

There are also modulo  $p$  analogues of [3, Lemma 2.14] which allow one to lift solutions to  $\mathbb{C}$  from a variety modulo  $p$  and we refer the reader to [10] for results of this type. One may also use effective versions of the Bézout identity, and more generally the Hilbert Nullstellensatz, to lift points on a variety modulo  $p$  to  $\mathbb{C}$ , and this idea has previously been used in [1, 2, 5, 13, 17].

**3.2 Tools from geometry of numbers.** Let  $\{\mathbf{b}_1, \dots, \mathbf{b}_m\}$  be a set of  $m \leq d$  linearly independent vectors in  $\mathbb{R}^d$ . The set of vectors

$$\mathcal{L} = \left\{ \sum_{i=1}^m n_i \mathbf{b}_i : n_i \in \mathbb{Z} \right\}$$

is called a  $d$ -dimensional lattice of rank  $m$ . The set  $\{\mathbf{b}_1, \dots, \mathbf{b}_m\}$  is called a **basis** of  $\mathcal{L}$ . Each lattice has multiple sets of basis vectors, and we refer to any other set  $\{\tilde{\mathbf{b}}_1, \dots, \tilde{\mathbf{b}}_m\}$  of linearly independent vectors such that

$$\mathcal{L} = \left\{ \sum_{i=1}^m n_i \tilde{\mathbf{b}}_i : n_i \in \mathbb{Z} \right\}$$

as a basis. We also define the determinant of  $\mathcal{L}$  as

$$\det \mathcal{L} = \sqrt{|\det B \cdot B^T|},$$

where  $B$  is the  $(m \times d)$ -matrix with rows  $\mathbf{b}_1, \dots, \mathbf{b}_m$ , and is independent of the choice of basis. We refer to [11] for a background on lattices.

The following is [12, Lemma 1].

**Lemma 3.2.** *Let  $\mathcal{L} \subseteq \mathbb{Z}^d$  be a lattice of rank  $m$ . Then  $\mathcal{L}$  has a basis  $\mathbf{b}_1, \dots, \mathbf{b}_m$  such that, for each  $\mathbf{x} \in \mathcal{L}$ , we may write*

$$\mathbf{x} = \sum_{j=1}^m \lambda_j \mathbf{b}_j,$$

with

$$\lambda_j \ll \frac{\|\mathbf{x}\|}{\|\mathbf{b}_j\|}.$$

We also have

$$\det \mathcal{L} \ll \prod_{j=1}^m \|\mathbf{b}_j\| \ll \det \mathcal{L}.$$

**Lemma 3.3.** *Let  $\alpha_1, \dots, \alpha_d \in \mathbb{C}$  and let  $\mathcal{L}$  denote the lattice*

$$\mathcal{L} = \{(n_1, \dots, n_d) \in \mathbb{Z}^d : \alpha_1 n_1 + \dots + \alpha_d n_d = 0\}.$$

*For integers  $H_1, \dots, H_d$  we consider the convex body*

$$D = \{(x_1, \dots, x_d) \in \mathbb{R}^d : |x_i| \leq H_i\}.$$

*If  $\mathcal{L} \cap D$  contains  $d - 1$  linearly independent points and there exists some  $1 \leq \ell \leq d$  such that  $\alpha_\ell \neq 0$ , then there exists some  $1 \leq j \leq d$  such that for each  $i = 1, \dots, d$  there exist integers  $a_i$  and  $b_i$  satisfying*

$$\frac{\alpha_i}{\alpha_j} = \frac{a_i}{b_i}, \quad \gcd(a_i, b_i) = 1, \quad a_i, b_i \ll H^d,$$

where

$$H = \max_{1 \leq i \leq d} H_i.$$

**Proof.** Choose  $d - 1$  linearly independent points  $\mathbf{x}^{(1)}, \dots, \mathbf{x}^{(d-1)}$  satisfying

$$\mathbf{x}^{(i)} = (x_{i,1}, \dots, x_{i,d}) \in \mathcal{L} \cap D, \quad 1 \leq i \leq d - 1.$$

Let  $X$  denote the  $(d - 1) \times d$  matrix whose  $i$ -th row is  $\mathbf{x}^{(i)}$  and let  $X^{(j)}$  denote the  $(d - 1) \times (d - 1)$  matrix obtained from  $X$  by removing the  $j$ -th column. By assumption, the rank of  $X$  equals  $d - 1$ . Hence there exists some  $1 \leq j \leq d$  such that

$$(3.1) \quad \det X^{(j)} \neq 0.$$

By symmetry we may suppose  $j = d$ . Since each  $\mathbf{x}^{(i)} \in \mathcal{L} \cap D$ , we have

$$X^{(d)} \begin{pmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_{d-1} \end{pmatrix} = -\alpha_d \begin{pmatrix} x_{1,d} \\ x_{2,d} \\ \vdots \\ x_{d-1,d} \end{pmatrix}.$$

Note that (3.1) and the assumption  $\alpha_\ell \neq 0$  implies  $\alpha_d \neq 0$ . Let  $Y^{(d)}$  denote the adjoint matrix of  $X^{(d)}$ , thus

$$X^{(d)} Y^{(d)} = \det X^{(d)} I_{d-1},$$

where  $I_{d-1}$  is the  $(d - 1) \times (d - 1)$ -identity matrix. Hence, the above implies

$$\det X^{(d)} \begin{pmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_{d-1} \end{pmatrix} = -\alpha_d Y^{(d)} \begin{pmatrix} x_{1,d} \\ x_{2,d} \\ \vdots \\ x_{d-1,d} \end{pmatrix}.$$

By Hadamard's inequality and the definition of  $H$ ,

$$\det X^{(d)} \ll H^d,$$

and

$$Y^{(d)} \begin{pmatrix} x_{1,d} \\ x_{2,d} \\ \vdots \\ x_{d-1,d} \end{pmatrix} = \begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_{d-1} \end{pmatrix},$$

for some integers  $y_1, \dots, y_{d-1} \ll H^d$ , from which the result follows.  $\square$

**3.3 Tools from additive combinatorics.** In our proof of Theorem 2.1 we use Lemma 3.1 to reduce to counting solutions to multiplicative equations over  $\mathbb{C}$  to which the following result of Chang [3, Proposition 2] may be applied; see also [3, Remark 1].

**Lemma 3.4.** *For each integer  $d \geq 1$  there exists a constant  $B_d$ , depending only on  $d$ , such that the following holds. Let  $\gamma_0, \dots, \gamma_d \in \mathbb{C}$  and define the set  $\mathcal{A}$  by*

$$\mathcal{A} = \{ \gamma_0 + \gamma_1 h_1 + \dots + \gamma_d h_d : |h_i| \leq H_i \}.$$

For any  $\lambda \in \mathbb{C}^*$  the number of solutions to

$$a_1 a_2 = \lambda, \quad a_1, a_2 \in \mathcal{A},$$

is bounded by  $\exp(B_d \log |\mathcal{A}| / \log \log |\mathcal{A}|)$ .

## 4 An iterative inequality

**4.1 Formulation of the result.** Our main input for the proof of Theorem 2.1 is the following iterative inequality which combines some ideas of Chang [3] with lattice basis reduction. Note that, as in [3], it is not necessary to assume our generalised arithmetic progression is proper.

Recall that for  $\mathcal{A}, \mathcal{B} \subseteq \mathbb{F}_p$  and  $\lambda \in \mathbb{F}_p$  we define  $I_p(\mathcal{A}, \mathcal{B}, \lambda)$  by (2.1).

We also recall that an integer  $n$  is called  $y$ -smooth if all prime divisors  $p$  of  $n$  satisfy  $p \leq y$ .

**Lemma 4.1.** *Let  $H, d, e$  be positive integers with  $e \leq d$  and let  $H$  be sufficiently large. There exists a constant  $B_d$  depending only on  $d$ , and an integer  $Z_{d,e}$  which*

- (i) is  $O(H^{1/\gamma_{d+e+1}})$ -smooth with  $\gamma_{d+e+1}$  given by (2.2),
- (ii) is divisible by all primes  $p \leq H^{d+e+o(1)}$ ,

(iii) *satisfies*

$$\log Z_{d,e} \ll H^{(d+e)(d+1)(e+1)} \log H,$$

such that for any prime  $p \nmid Z_{d,e}$  the following holds. Let  $\lambda \in \overline{\mathbb{F}}_p^*$  and  $\mathcal{A}, \mathcal{B} \subseteq \overline{\mathbb{F}}_p$  be generalised arithmetic progressions of the form

$$(4.1) \quad \mathcal{A} = \{ \alpha_0 + \alpha_1 h_1 + \cdots + \alpha_d h_d : |h_i| \leq H, i = 1, \dots, d \},$$

and

$$(4.2) \quad \mathcal{B} = \{ \beta_0 + \beta_1 j_1 + \cdots + \beta_e j_e : |j_i| \leq H, i = 1, \dots, e \},$$

with  $d, e \geq 2$  and

$$\alpha_1, \dots, \alpha_d, \beta_1, \dots, \beta_e \in \overline{\mathbb{F}}_p^*.$$

There exists a constant  $\tilde{C}_d$  depending only on  $d$  and  $e$ , integers  $\tilde{d}$  and  $\tilde{e}$  satisfying

$$\tilde{d} \leq d, \quad \tilde{e} \leq e, \quad \tilde{d} + \tilde{e} < d + e,$$

generalised arithmetic progressions  $\tilde{\mathcal{A}}, \tilde{\mathcal{B}}$  of the form

$$\begin{aligned} \tilde{\mathcal{A}} &= \{ \tilde{\alpha}_0 + \tilde{\alpha}_1 h_1 + \cdots + \tilde{\alpha}_{\tilde{d}} h_{\tilde{d}} : |h_i| \leq \tilde{C}_d H, i = 1, \dots, \tilde{d} \}, \\ \tilde{\mathcal{B}} &= \{ \tilde{\beta}_0 + \tilde{\beta}_1 j_1 + \cdots + \tilde{\beta}_{\tilde{e}} j_{\tilde{e}} : |j_i| \leq \tilde{C}_d H, i = 1, \dots, \tilde{e} \}, \end{aligned}$$

with

$$\tilde{\alpha}_1 \cdots, \tilde{\alpha}_{\tilde{d}}, \tilde{\beta}_1 \cdots \tilde{\beta}_{\tilde{e}} \in \overline{\mathbb{F}}_p^*,$$

and some  $\mu \in \overline{\mathbb{F}}_p^*$  such that

$$I_p(\mathcal{A}, \mathcal{B}, \lambda) \leq \exp(B_d \log H / \log \log H) I_p(\tilde{\mathcal{A}}, \tilde{\mathcal{B}}, \mu).$$

We split the proof of Lemma 4.1 in a series of steps.

**4.2 Elimination undesired primes.** We first denote

$$(4.3) \quad Z_0 = \prod_{p \leq C_d H^d} p$$

for an appropriately large constant  $C_d$ , which depends only on  $d$ . We now fix  $p \nmid Z_0$ , thus

$$(4.4) \quad p > C_d H^d.$$

We first construct the integer  $Z_{d,e}$ . For  $\mathbf{h}, \mathbf{h}_0 \in \mathbb{Z}^d$  and  $\mathbf{j}, \mathbf{j}_0 \in \mathbb{Z}^e$  define the polynomial

$$(4.5) \quad \begin{aligned} P_{\mathbf{h}, \mathbf{h}_0, \mathbf{j}, \mathbf{j}_0}(\mathbf{X}, \mathbf{Y}) &= (X_0 + X_1 h_{0,1} + \cdots + X_d h_{0,d})(Y_0 + Y_1 j_{0,1} + \cdots + Y_e j_{0,e}) \\ &\quad - (X_0 + X_1 h_1 + \cdots + X_d h_d)(Y_0 + Y_1 j_1 + \cdots + Y_e j_e). \end{aligned}$$

We may identify the polynomial  $P_{\mathbf{h}, \mathbf{h}_0, \mathbf{j}, \mathbf{j}_0}(\mathbf{X}, \mathbf{Y})$  with a point in the vector space  $\mathbb{C}^\Delta$  where

$$\Delta = (d+1)(e+1) - 1 = de + d + e,$$

which is formed by its coefficients. Suppose  $\mathcal{M} \subseteq \mathbb{Z}^d \times \mathbb{Z}^e$  satisfies  $|\mathcal{M}| \leq \Delta$  and the set

$$\{P_{\mathbf{h}, \mathbf{h}_0, \mathbf{j}, \mathbf{j}_0}(\mathbf{X}, \mathbf{Y}) : (\mathbf{h}, \mathbf{j}) \in \mathcal{M}\}$$

is linearly independent over  $\mathbb{C}$ .

Let  $M(\mathbf{h}_0, \mathbf{j}_0, \mathcal{K})$  denote the  $|\mathcal{M}| \times \Delta$  matrix whose rows correspond to coefficients of the polynomials  $P_{\mathbf{h}, \mathbf{h}_0, \mathbf{j}, \mathbf{j}_0}(\mathbf{X}, \mathbf{Y})$  with  $(\mathbf{h}, \mathbf{j}) \in \mathcal{M}$ . Define

$$(4.6) \quad Z_1(\mathbf{h}_0, \mathbf{j}_0, \mathcal{M}) = \det M_0(\mathbf{h}_0, \mathbf{j}_0, \mathcal{M}),$$

where  $M_0(\mathbf{h}_0, \mathbf{j}_0, \mathcal{M})$  is  $|\mathcal{M}| \times |\mathcal{M}|$  submatrix of  $M(\mathbf{h}_0, \mathbf{j}_0, \mathcal{M})$  with nonzero determinant. If

$$\mathbf{h}_0 \in [-H, H]^d, \quad \mathbf{j}_0 \in [-H, H]^e, \quad \mathcal{M} \subseteq [-H, H]^d \times [-H, H]^e$$

then for each  $(\mathbf{h}, \mathbf{j}) \in \mathcal{M}$  the polynomial  $P_{\mathbf{h}, \mathbf{h}_0, \mathbf{j}, \mathbf{j}_0}$  has height at most  $2 \log H + O(1)$ . Clearly there are

$$(4.7) \quad W = (2H+1)^d \cdot (2H+1)^e \cdot \sum_{r=1}^{\Delta} \binom{(2H+1)^{d+e}}{r} \\ \ll H^{d+e+\Delta(d+e)} = H^{(d+e)(\Delta+1)}$$

choices for the above triple  $(\mathbf{h}_0, \mathbf{j}_0, \mathcal{M})$ .

By Hadamard's inequality

$$(4.8) \quad Z_1(\mathbf{h}_0, \mathbf{j}_0, \mathcal{K}) \ll H^{2|\mathcal{M}|} \ll H^{2\Delta}.$$

Define

$$(4.9) \quad Z_1 = \prod_{\substack{\mathbf{h}_0 \in [-H, H]^d \\ \mathbf{j}_0 \in [-H, H]^e \\ \mathcal{M} \subseteq [-H, H]^d \times [-H, H]^e \\ |\mathcal{M}| \leq \Delta}} Z_1(\mathbf{h}_0, \mathbf{j}_0, \mathcal{M}),$$

so, recalling (4.7) and (4.8), we see that

$$\log Z_1 \ll W \log H \ll H^{(d+e)(\Delta+1)} \log H,$$

and that  $Z_1$  is  $O(H^{2\Delta})$ -smooth.

For each  $\mathbf{h}_0, \mathbf{j}_0, \mathcal{M}$  as above, let  $V(\mathbf{h}_0, \mathbf{j}_0, \mathcal{M})$  denote the variety

$$V(\mathbf{h}_0, \mathbf{j}_0, \mathcal{M}) = \bigcap_{(\mathbf{h}, \mathbf{j}) \in \mathcal{M}} \{(\mathbf{x}, \mathbf{y}) \in \mathbb{C}^{d+1} \times \mathbb{C}^{e+1} : P_{\mathbf{h}, \mathbf{h}_0, \mathbf{j}, \mathbf{j}_0}(\mathbf{x}, \mathbf{y}) = 0\} \\ \cap \{(\mathbf{x}, \mathbf{y}) \in \mathbb{C}^{d+1} \times \mathbb{C}^{e+1} : x_1 = 1, y_1 = 1\},$$

and let  $V_p(\mathbf{h}_0, \mathbf{j}_0, \mathcal{M})$  be the reduction of  $V(\mathbf{h}_0, \mathbf{j}_0, \mathcal{M})$  modulo  $p$

$$V_p(\mathbf{h}_0, \mathbf{j}_0, \mathcal{M}) = \bigcap_{(\mathbf{h}, \mathbf{j}) \in \mathcal{M}} \{(\mathbf{x}, \mathbf{y}) \in \overline{\mathbb{F}}_p^{d+1} \times \overline{\mathbb{F}}_p^{e+1} : P_{\mathbf{h}, \mathbf{h}_0, \mathbf{j}, \mathbf{j}_0}(\mathbf{x}, \mathbf{y}) = 0\} \\ \cap \{(\mathbf{x}, \mathbf{y}) \in \overline{\mathbb{F}}_p^{d+1} \times \overline{\mathbb{F}}_p^{e+1} : x_1 = 1, y_1 = 1\}.$$

If  $|V(\mathbf{h}_0, \mathbf{j}_0, \mathcal{M})| = \infty$  then define

$$Z_2(\mathbf{h}_0, \mathbf{j}_0, \mathcal{M}) = 1.$$

Otherwise, that is, if  $|V(\mathbf{h}_0, \mathbf{j}_0, \mathcal{M})| < \infty$ , by Lemma 3.1 there exists a positive integer  $Z_2(\mathbf{h}_0, \mathbf{j}_0, \mathcal{M})$  satisfying

$$Z_2(\mathbf{h}_0, \mathbf{j}_0, \mathcal{M}) \ll H^{1/\gamma_{d+e+1}},$$

such that for each prime  $p$  not dividing  $Z_2(\mathbf{h}_0, \mathbf{j}_0, \mathcal{M})$ , we have

$$|V(\mathbf{h}_0, \mathbf{j}_0, \mathcal{M})| = |V_p(\mathbf{h}_0, \mathbf{j}_0, \mathcal{M})|.$$

Denote

$$(4.10) \quad Z_2 = \prod_{\substack{\mathbf{h}_0, \in [-H, H]^d \\ \mathbf{j}_0 \in [-H, H]^e \\ \mathcal{M} \subseteq [-H, H]^d \times [-H, H]^e \\ |\mathcal{M}| \leq \Delta}} Z_2(\mathbf{h}_0, \mathbf{j}_0, \mathcal{M}).$$

With  $Z_1$  and  $Z_2$  as in (4.9) and (4.10) we define

$$Z_{d,e} = Z_0 Z_1 Z_2.$$

Since  $\gamma_{d+e+1} \leq \Delta^{-1}$  we see that  $Z_{d,e}$  is  $O(H^{1/\gamma_{d+e+1}})$ -smooth and satisfies

$$\log Z_{d,e} \ll H^{(d+e)(\Delta+1)} \log H.$$

From now on we only consider primes  $p \nmid Z_{d,e}$ .

**4.3 Local to global lifting of rational points on some varieties.** Fix some prime  $p$  not dividing  $Z_{d,e}$ . With  $\mathcal{A}, \mathcal{B}$  as in (4.1) and (4.2), choose

$$\begin{aligned}\mathcal{H} &\subseteq [-H, H]^d \cap \mathbb{Z}^d, \\ \mathcal{J} &\subseteq [-H, H]^e \cap \mathbb{Z}^e,\end{aligned}$$

such that the points

$$\begin{aligned}\alpha_0 + h_1\alpha_1 + \cdots + h_d\alpha_d, & \quad (h_1, \dots, h_d) \in \mathcal{H}, \\ \beta_0 + j_1\beta_1 + \cdots + j_e\beta_e, & \quad (j_1, \dots, j_e) \in \mathcal{J},\end{aligned}$$

are distinct modulo  $p$  and for each  $a \in \mathcal{A}$  there exists some integer vector  $(h_1, \dots, h_d) \in \mathcal{H}$  such that

$$a = \alpha_0 + h_1\alpha_1 + \cdots + h_d\alpha_d$$

and for each  $b \in \mathcal{B}$  there exists some  $(j_1, \dots, j_e) \in \mathcal{J}$  such that

$$b = \beta_0 + j_1\beta_1 + \cdots + j_e\beta_e.$$

Write

$$\mathbf{h} = (h_1, \dots, h_d) \quad \text{and} \quad \mathbf{j} = (j_1, \dots, j_e),$$

so that  $I_p(\mathcal{A}, \mathcal{B}, \lambda)$  is bounded by the number of solutions to

$$(4.11) \quad (\alpha_0 + \alpha_1 h_1 + \cdots + \alpha_d h_d)(\beta_0 + \beta_1 j_1 + \cdots + \beta_e j_e) \equiv \lambda \pmod{p},$$

with  $\mathbf{h} \in \mathcal{H}$  and  $\mathbf{j} \in \mathcal{J}$ . Dividing both sides of (4.11) by  $\alpha_1 \beta_1$  and modifying  $\alpha_0, \dots, \alpha_d, \beta_0, \dots, \beta_e, \lambda$  if necessary, we may assume

$$(4.12) \quad \alpha_1 = \beta_1 = 1.$$

This reduction allows for a convenient application of Lemma 3.1. In what follows, we will construct a variety over  $\overline{\mathbb{F}}_p$  which contains the point  $(\alpha_0, \dots, \alpha_d, \beta_0, \dots, \beta_e)$  and the assumption that  $\alpha_1 = \beta_1 = 1$  allows us to obtain a nonzero point in the corresponding variety over  $\mathbb{C}$  after applying Lemma 3.1.

Let  $\mathcal{K} \subseteq \mathcal{H} \times \mathcal{J}$  denote the set

$$\mathcal{K} = \{(\mathbf{h}, \mathbf{j}) \in \mathcal{H} \times \mathcal{J} : \mathbf{h}, \mathbf{j} \text{ satisfy (4.11)}\},$$

so that

$$(4.13) \quad I_p(\mathcal{A}, \mathcal{B}, \lambda) = |\mathcal{K}|.$$



Since we may assume  $\mathcal{K} \neq \emptyset$ , fix some  $(\mathbf{h}_0, \mathbf{j}_0) \in \mathcal{K}$  and for each  $(\mathbf{h}, \mathbf{j}) \in \mathcal{K}$  consider the polynomial  $P_{\mathbf{h}, \mathbf{h}_0, \mathbf{j}, \mathbf{j}_0}(\mathbf{X}, \mathbf{Y})$ , given by (4.5). Clearly for  $(\mathbf{h}_0, \mathbf{j}_0) \neq (\mathbf{h}, \mathbf{j})$  the polynomial  $P_{\mathbf{h}, \mathbf{h}_0, \mathbf{j}, \mathbf{j}_0}(\mathbf{X}, \mathbf{Y})$  is not identical to zero over  $\mathbb{C}$ . Indeed, it is enough to consider the specialisations  $P_{\mathbf{h}, \mathbf{h}_0, \mathbf{j}, \mathbf{j}_0}((1, 0, \dots, 0), \mathbf{Y})$  and  $P_{\mathbf{h}, \mathbf{h}_0, \mathbf{j}, \mathbf{j}_0}(\mathbf{X}, (1, 0, \dots, 0))$  to see this. Furthermore, if  $p > 2H$  (which is guaranteed by our assumption), then  $(\mathbf{h}_0, \mathbf{j}_0) \neq (\mathbf{h}, \mathbf{j})$  implies  $(\mathbf{h}_0, \mathbf{j}_0) \not\equiv (\mathbf{h}, \mathbf{j}) \pmod p$  and we see that  $P_{\mathbf{h}, \mathbf{h}_0, \mathbf{j}, \mathbf{j}_0}(\mathbf{X}, \mathbf{Y})$  is also not identical to zero over  $\overline{\mathbb{F}}_p$ .

Let  $V_p \subseteq \overline{\mathbb{F}}_p^{d+e+2}$  denote the variety

$$V_p = \bigcap_{(\mathbf{h}, \mathbf{j}) \in \mathcal{K}} \{(\mathbf{x}, \mathbf{y}) \in \overline{\mathbb{F}}_p^{d+1} \times \overline{\mathbb{F}}_p^{e+1} : P_{\mathbf{h}, \mathbf{h}_0, \mathbf{j}, \mathbf{j}_0}(\mathbf{x}, \mathbf{y}) = 0\} \\ \cap \{(\mathbf{x}, \mathbf{y}) \in \overline{\mathbb{F}}_p^{d+1} \times \overline{\mathbb{F}}_p^{e+1} : x_1 = 1, y_1 = 1\}.$$

Let  $\mathcal{M} \subseteq \mathcal{K}$  be a maximal set of  $(\mathbf{h}, \mathbf{j}) \in \mathcal{K}$ , such that the polynomials  $P_{\mathbf{h}, \mathbf{h}_0, \mathbf{j}, \mathbf{j}_0}(\mathbf{X}, \mathbf{Y})$  are linearly independent over  $\mathbb{C}$ . With  $Z_1(\mathbf{h}_0, \mathbf{j}_0, \mathcal{M})$  defined as in (4.6), with respect to such  $\mathcal{K}$ , since

$$p \nmid Z_1(\mathbf{h}_0, \mathbf{j}_0, \mathcal{M})$$

we conclude that  $\mathcal{M} \subseteq \mathcal{K}$  is also a maximal set such that the polynomials  $P_{\mathbf{h}, \mathbf{h}_0, \mathbf{j}, \mathbf{j}_0}(\mathbf{X}, \mathbf{Y})$  are linearly independent over  $\overline{\mathbb{F}}_p$ . Hence

$$V_p = \bigcap_{(\mathbf{h}, \mathbf{j}) \in \mathcal{M}} \{(\mathbf{x}, \mathbf{y}) \in \overline{\mathbb{F}}_p^{d+1} \times \overline{\mathbb{F}}_p^{e+1} : P_{\mathbf{h}, \mathbf{h}_0, \mathbf{j}, \mathbf{j}_0}(\mathbf{x}, \mathbf{y}) = 0\} \\ \cap \{(\mathbf{x}, \mathbf{y}) \in \overline{\mathbb{F}}_p^{d+1} \times \overline{\mathbb{F}}_p^{e+1} : x_1 = 1, y_1 = 1\}$$

and  $1 \leq |\mathcal{M}| \leq \Delta$ . By definition of  $\mathcal{K}$  and (4.12), we have

$$(4.14) \quad (\alpha_0, \dots, \alpha_d, \beta_0, \dots, \beta_e) \in V_p.$$

Let  $V \subseteq \mathbb{C}^{d+e+2}$  denote the variety

$$(4.15) \quad V = \bigcap_{(\mathbf{h}, \mathbf{j}) \in \mathcal{M}} \{(\mathbf{x}, \mathbf{y}) \in \mathbb{C}^{d+1} \times \mathbb{C}^{e+1} : P_{\mathbf{h}, \mathbf{h}_0, \mathbf{j}, \mathbf{j}_0}(\mathbf{x}, \mathbf{y}) = 0\} \\ \cap \{(\mathbf{x}, \mathbf{y}) \in \mathbb{C}^{d+1} \times \mathbb{C}^{e+1} : x_1 = 1, y_1 = 1\}.$$

We next show there exists some

$$(\rho, \tau) = (\rho_0, \rho_1, \dots, \rho_d, \tau_0, \tau_1, \dots, \tau_e) \in \mathbb{C}^{d+1} \times \mathbb{C}^{e+1}$$

satisfying

$$(4.16) \quad (\rho, \tau) \in V, \quad (\rho_1, \dots, \rho_d) \neq \mathbf{0}, \quad (\tau_1, \dots, \tau_e) \neq \mathbf{0}.$$

Certainly it is enough to show that

$$(4.17) \quad |V| \geq 1,$$

as the non-vanishing conditions in (4.16) are obvious because any point  $(\rho, \tau) \in V$  satisfies  $\rho_1 = \tau_1 = 1$ .

We may assume

$$(4.18) \quad |V| < \infty,$$

since otherwise (4.16) is trivial. We next apply Lemma 3.1. The assumption (4.18) and that

$$p \nmid Z_2(\mathbf{h}_0, \mathbf{j}_0, \mathcal{M})$$

implies

$$(4.19) \quad |V| = |V_p|.$$

We see from (4.14) that

$$|V_p| \geq 1.$$

Combining the above with (4.19), we obtain (4.17).

Hence there exists some  $(\rho, \tau) \in \mathbb{C}^{d+1} \times \mathbb{C}^{e+1}$  satisfying (4.16). Note that from (4.15) we have

$$(4.20) \quad \rho_1 = \tau_1 = 1.$$

**4.4 Reduction to counting solutions to a multiplicative congruence on a complex line.** We see that any solution to (4.11) satisfies

$$(4.21) \quad (\rho_0 + \rho_1 h_1 + \cdots + \rho_d h_d)(\tau_0 + \tau_1 j_1 + \cdots + \tau_e j_e) = \vartheta,$$

where

$$\vartheta = (\rho_0 + \rho_1 h_{0,1} + \cdots + \rho_d h_{0,d})(\tau_0 + \tau_1 j_{0,1} + \cdots + \tau_e j_{0,e}).$$

Consider the following two cases

- If  $\vartheta = 0$ , then either

$$\rho_0 + \rho_1 h_1 + \cdots + \rho_d h_d = 0,$$

or

$$\tau_0 + \tau_1 j_1 + \cdots + \tau_e j_e = 0.$$

- If  $\vartheta \neq 0$ , then by Lemma 3.4, there exists a set of

$$\exp(B_d \log H / \log \log H)$$

pairs  $\Omega = \{(\omega_1, \omega_2)\}$  such that any solution to (4.21) satisfies

$$\rho_0 + \rho_1 h_1 + \cdots + \rho_d h_d = \omega_1, \quad \tau_0 + \tau_1 j_1 + \cdots + \tau_e j_e = \omega_2,$$

for some  $(\omega_1, \omega_2) \in \Omega$ .

Taking a maximum over the above two cases, we see that there exists some  $\zeta \in \mathbb{C}$  and some  $i = 1, 2$  such that

$$I_p(\mathcal{A}, \mathcal{B}, \lambda) \leq \exp(B_d \log H / \log \log H) J_i(\mathcal{A}, \mathcal{B}, \lambda),$$

where  $J_1(\mathcal{A}, \mathcal{B}, \lambda)$  counts the number of solutions to

$$(4.22) \quad (\alpha_0 + \alpha_1 h_1 + \cdots + \alpha_d h_d)(\beta_0 + \beta_1 j_1 + \cdots + \beta_e j_e) \equiv \lambda \pmod{p},$$

and

$$(4.23) \quad \rho_1 h_1 + \cdots + \rho_d h_d = \zeta,$$

with variables  $\mathbf{h} \in \mathcal{H}, \mathbf{j} \in \mathcal{J}$  and  $J_2(\mathcal{A}, \mathcal{B}, \lambda)$  counts the number of solutions to (4.22) and

$$\tau_1 j_1 + \cdots + \tau_e j_e = \zeta,$$

with variables  $\mathbf{h} \in \mathcal{H}, \mathbf{j} \in \mathcal{J}$ .

Suppose first that

$$(4.24) \quad I_p(\mathcal{A}, \mathcal{B}, \lambda) \leq \exp(B_d \log H / \log \log H) J_1(\mathcal{A}, \mathcal{B}, \lambda);$$

the case

$$(4.25) \quad I_p(\mathcal{A}, \mathcal{B}, \lambda) \leq \exp(B_d \log H / \log \log H) J_2(\mathcal{A}, \mathcal{B}, \lambda),$$

may be treated with a similar argument which we indicate at the end of the proof.

**4.5 Application of geometry of numbers to derive the desired inequality.** Let  $\mathcal{L}$  denote the lattice

$$\mathcal{L} = \{(n_1, \dots, n_d) \in \mathbb{Z}^d : \rho_1 n_1 + \cdots + \rho_d n_d = 0\},$$

and  $D$  the convex body

$$D = \{(n_1, \dots, n_d) : |n_i| \leq H\}.$$

Assuming  $J_1(\mathcal{A}, \mathcal{B}, \lambda) \neq 0$ , there exists some  $\mathbf{h}^* = (h_1^*, \dots, h_d^*) \in D \cap \mathbb{Z}^d$  such that if  $\mathbf{h} = (h_1, \dots, h_d)$  satisfies (4.23) then

$$(4.26) \quad \mathbf{h} - \mathbf{h}^* \in \mathcal{L} \cap 2D.$$

By (4.20) we have

$$\dim \mathcal{L} < d.$$

Hence we may consider two cases: either

$$(4.27) \quad \dim(\mathcal{L} \cap 2D) < d - 1,$$

or

$$(4.28) \quad \dim(\mathcal{L} \cap 2D) = d - 1.$$

Suppose that we have (4.27). Let  $\mathcal{L}^*$  denote the lattice generated by  $\mathcal{L} \cap 2D$ , so that  $\dim \mathcal{L}^* = r$  for some  $r < d - 1$ . By Lemma 3.2 there exists a basis  $\lambda_1, \dots, \lambda_r$ , for  $\mathcal{L}^*$  such that each  $\mathbf{h}$  satisfying (4.26) may be expressed in the form

$$(4.29) \quad \mathbf{h} - \mathbf{h}^* = k_1 \lambda_1 + \dots + k_r \lambda_r,$$

where from (4.26)

$$k_1, \dots, k_r \ll \frac{\|\mathbf{h} - \mathbf{h}^*\|}{\|\lambda_j\|} \ll H.$$

Substituting (4.29) into (4.22), there exist  $\tilde{\alpha}_0, \dots, \tilde{\alpha}_r \in \mathbb{F}_p$  such that for any  $\mathbf{h} \in \mathcal{H}$ ,  $\mathbf{j} \in \mathcal{J}$  satisfying (4.22) and (4.23) there exist  $\ell_1, \dots, \ell_r$  such that

$$(\tilde{\alpha}_0 + \tilde{\alpha}_1 \ell_1 + \dots + \tilde{\alpha}_r \ell_r)(\beta_0 + \beta_1 h_1 + \dots + \beta_e h_e) \equiv \lambda \pmod{p},$$

and

$$\tilde{\alpha}_0 + \tilde{\alpha}_1 \ell_1 + \dots + \tilde{\alpha}_r \ell_r = \alpha_0 + \alpha_1 h_1 + \dots + \alpha_d h_d.$$

Let  $\tilde{d} = r$  and let  $\tilde{\mathcal{A}}$  denote the generalized arithmetic progression

$$\tilde{\mathcal{A}} = \{\tilde{\alpha}_0 + \tilde{\alpha}_1 \tilde{h}_1 + \dots + \tilde{\alpha}_{\tilde{d}} \tilde{h}_{\tilde{d}} : |\tilde{h}_i| \leq \tilde{C}_d H, i = 1, \dots, \tilde{d}\}.$$

From construction of  $\mathcal{H}$ , for each  $a \in \mathcal{A}$  there exists a unique  $\mathbf{h} \in \mathcal{H}$  such that

$$a = \alpha_0 + \alpha_1 h_1 + \dots + \alpha_d h_d.$$

For each  $\mathbf{h} \in \mathcal{H}$ , there exists some  $\tilde{\mathbf{h}}$  satisfying

$$|\tilde{h}_i| \leq \tilde{C}_d H, \quad i = 1, \dots, \tilde{d},$$

such that

$$\alpha_0 + \alpha_1 h_1 + \cdots + \alpha_d h_d = \tilde{\alpha}_0 + \tilde{\alpha}_1 \tilde{h}_1 + \cdots + \tilde{\alpha}_{\tilde{d}} \tilde{h}_{\tilde{d}}.$$

The above implies we may choose a set

$$\tilde{\mathcal{H}} \subseteq [-\tilde{C}_d H, \tilde{C}_d H]^{\tilde{d}},$$

such that the points

$$\tilde{\alpha}_0 + \tilde{\alpha}_1 \tilde{h}_1 + \cdots + \tilde{\alpha}_{\tilde{d}} \tilde{h}_{\tilde{d}}, \quad \tilde{\mathbf{h}} \in \mathcal{H}_0,$$

are distinct and for each  $\mathbf{h} \in \mathcal{H}$  satisfying (4.22) and (4.23) there exists some  $\tilde{\mathbf{h}} \in \mathcal{H}_0$  such that

$$\alpha_0 + \alpha_1 h_1 + \cdots + \alpha_d h_d = \tilde{\alpha}_0 + \tilde{\alpha}_1 \tilde{h}_1 + \cdots + \tilde{\alpha}_{\tilde{d}} \tilde{h}_{\tilde{d}}.$$

The above combined with (4.13) implies that

$$J_1(\mathcal{A}, \mathcal{B}, \lambda) \leq I_p(\tilde{\mathcal{A}}, \mathcal{B}, \lambda).$$

Hence, recalling (4.24), we obtain the desired result provided (4.27) holds.

If we are in the case of (4.28), then by Lemma 3.3 there exist integers  $a_i$  and  $b_i$  satisfying

$$\frac{\rho_i}{\rho_d} = \frac{a_i}{b_i}, \quad \gcd(a_i, b_i) = 1, \quad a_i, b_i \ll H^d, \quad 1 \leq i \leq d,$$

where by symmetry we assume  $j = 1$  and also use that  $\rho_1 = 1$  in our application of Lemma 3.3. By (4.4), provided that  $C_d$  is large enough, we see that

$$\text{if } a_i, b_i \neq 0 \text{ then } a_i, b_i \not\equiv 0 \pmod{p}.$$

By (4.23) and (4.26)

$$h_d - h_d^* = \frac{\alpha_1}{\alpha_d}(h_1^* - h_1) + \cdots + \frac{\alpha_{d-1}}{\alpha_d}(h_{d-1}^* - h_{d-1}),$$

which combined with the above implies

$$(4.30) \quad h_d \equiv h_d^* - a_1 \bar{b}_1 (h_1 - h_1^*) - \cdots - a_{d-1} \bar{b}_{d-1} (h_{d-1} - h_{d-1}^*) \pmod{p},$$

where  $\bar{x}$  denotes the multiplicative inverse of  $x$  modulo  $p$ . As before, substituting (4.30) into (4.22), there exists a generalized arithmetic progression

$$\tilde{\mathcal{A}} = \{ \tilde{\alpha}_0 + \tilde{\alpha}_1 \ell_1 + \cdots + \tilde{\alpha}_{\tilde{d}} \ell_{\tilde{d}} : |\ell_i| \leq \tilde{C}_d H, i = 1, \dots, \tilde{d} \},$$

with  $\tilde{d} < d$  such that

$$J_1(\mathcal{A}, \mathcal{B}, \lambda) \leq I_p(\tilde{\mathcal{A}}, \mathcal{B}, \lambda),$$

and the result follows combining this with (4.24).

In the case of (4.25), we apply a similar argument as before, except with the lattice

$$\mathcal{L} = \{(n_1, \dots, n_e) \in \mathbb{Z}^e : \tau_1 n_1 + \dots + \tau_e n_e = 0\},$$

and convex body

$$D = \{(n_1, \dots, n_e) : |n_i| \leq H, i = 1, \dots, e\},$$

to obtain

$$J_2(\mathcal{A}, \mathcal{B}, \lambda) \leq I_p(\mathcal{A}, \tilde{\mathcal{B}}, \lambda),$$

for some generalized arithmetic progression  $\tilde{\mathcal{B}}$  of the form

$$\tilde{\mathcal{B}} = \{\tilde{\beta}_0 + \tilde{\beta}_1 h_1 + \dots + \tilde{\beta}_{\tilde{e}} h_{\tilde{e}} : |h_i| \leq \tilde{C}_d H, i = 1, \dots, \tilde{e}\},$$

with  $\tilde{e} < e$ . Combining this with (4.25) we obtain the desired inequality under the assumption (4.4). To conclude that proof it remains to verify (ii), about the divisibility of  $Z_{d,e}$ .

**4.6 Prime divisors of  $Z_{d,e}$ .** We now show that  $Z_{d,e}$  is divisible by all primes  $p \leq H^{d+e+o(1)}$ . Fix some small  $\varepsilon > 0$  and consider generalised arithmetic progressions of the form (4.1) and (4.2).

We next use the Dirichlet pigeon-hole principle to show the statement of Lemma 4.1 fails for any prime  $H^d < p \leq H^{d+e-\varepsilon}$  provided that  $H$  is large enough. This is sufficient from (4.3) and the fact that  $Z_0|Z_{d,e}$ , (provided  $C_d > 1$ ).

Indeed, since the value of  $Z_{d,e}$  does not depend on the generalised arithmetic progressions  $\mathcal{A}_0$  and  $\mathcal{B}_0$ , we can choose

$$\alpha_0 = 0 \quad \text{and} \quad \alpha_i = (2H + 1)^{i-1}, \quad i = 1, \dots, d,$$

and

$$\beta_0 = 0 \quad \text{and} \quad \beta_j = (2H + 1)^{j-1}, \quad j = 1, \dots, e.$$

Hence  $\mathcal{A}_0$  and  $\mathcal{B}_0$  are proper and in fact contain  $(2H + 1)^d$  and  $(2H + 1)^e$  distinct residues modulo  $p$ , respectively. Next, there are  $(2H + 1)^{d+e}$  products in  $\overline{\mathbb{F}}_p$

$$(\alpha_0 + \alpha_1 h_1 + \dots + \alpha_d h_d)(\beta_0 + \beta_1 j_1 + \dots + \beta_e j_e)$$

over all choices of  $|h_i| \leq H, i = 1, \dots, d$  and  $|j_i| \leq H, i = 1, \dots, e$ , except for at most  $O(H^{d+e-1})$  choices for which this product is divisible by  $p$ . Hence, there exists a non-zero residue class  $\lambda_0$  modulo  $p$  into which at least

$$(2H + 1)^{d+e}(1 + O(H^{-1}))/p \gg H^\varepsilon$$

of such products fall, thus giving

$$I_p(\mathcal{A}_0, \mathcal{B}_0, \lambda_0) \gg H^\epsilon$$

contradicting the assumed bound.

Hence we have  $p \mid Z_{d,e}$  for such primes. This also implies that the assumption (4.4) holds for any prime  $p \nmid Z_{d,e}$ .

## 5 Proofs of results on factorisation in generalised arithmetic progressions

**5.1 Proof of Theorem 2.1.** We proceed by induction on  $d + e$  with base case

$$d + e = 1.$$

In this case, there exists some  $\lambda_0 \in \mathbb{F}_p$  such that

$$I_p(\mathcal{A}, \mathcal{B}, \lambda) = |\{1 \leq h \leq H : h = \lambda_0\}|,$$

for which there is at most 1 solution provided  $H \leq p$ . Hence the result follows by taking

$$Z = \prod_{p \leq H} p.$$

Let  $C_*(\ell)$  be sufficiently large depending only on the implied constants in Lemma 4.1.

We next set up some notation related to our induction hypothesis. Let  $H \gg 1$ ,  $\ell \geq 2$  and for each pair of positive integers  $d, e$  satisfying

$$e \leq d \quad \text{and} \quad d + e \leq \ell,$$

let  $Z_{d,e}$  be as in Lemma 4.1. Define

$$Z_\ell = \prod_{\substack{0 < e \leq d \\ d + e \leq \ell}} Z_{d,e},$$

so that  $Z_\ell$  is  $O(H^{1/\gamma_\ell})$ -smooth and satisfies

$$\log Z_\ell \ll \log H \sum_{3 \leq j \leq \ell} \sum_{\substack{0 < e \leq d \\ d + e = j}} H^{j(d+1)(e+1)} \ll H^{(\ell-1)(\ell+2)^2/4} \log H$$

where we have used

$$j(d+1)(e+1) \leq j \left( \frac{d+e+2}{2} \right)^2 \leq \ell \frac{(\ell+2)^2}{4}.$$

We formulate our induction hypothesis as follows. There exists a constant  $b_{\ell-1}$  such that for any positive integers  $e \leq d$  satisfying  $d + e \leq \ell - 1$  and prime

$$(5.1) \quad p \geq C_*(\ell)H^{\ell-1}$$

not dividing  $Z_{\ell-1}$  (which by Lemma 4.1 (ii) holds for any  $p \nmid Z_{\ell-1}$ ), for any  $\lambda \in \mathbb{F}_p$  and generalized arithmetic progressions

$$\begin{aligned} \mathcal{A} &= \{\alpha_0 + \alpha_1 h_1 + \cdots + \alpha_d h_d : 1 \leq h_i \leq H, i = 1, \dots, d\}, \\ \mathcal{B} &= \{\beta_0 + \beta_1 j_1 + \cdots + \beta_e j_e : 1 \leq j_i \leq H, i = 1, \dots, e\}, \end{aligned}$$

we have

$$I_p(\mathcal{A}, \mathcal{B}, \lambda) \leq \exp(b_{\ell-1} \log(|\mathcal{A}||\mathcal{B}|) / \log \log(|\mathcal{A}||\mathcal{B}|)).$$

Let  $e \leq d$  be positive integers satisfying

$$d + e = \ell$$

and  $H \gg 1$ .

By Lemma 4.1, for any prime  $p \nmid Z_\ell$ , and thus satisfying

$$p \gg H^{d+e},$$

the following holds.

Let  $\lambda \in \overline{\mathbb{F}}_p^*$  and  $\mathcal{A}, \mathcal{B} \subseteq \overline{\mathbb{F}}_p$  be generalised arithmetic progressions as in (4.1) and satisfying (4.2) with  $d, e \geq 2$  and

$$\alpha_1, \dots, \alpha_d, \beta_1, \dots, \beta_e \in \overline{\mathbb{F}}_p^*.$$

There exists a constant  $\tilde{C}_d$  depending only on  $d, e$ , integers  $\tilde{d}$  and  $\tilde{e}$  satisfying

$$\tilde{d} \leq d, \quad \tilde{e} \leq e, \quad \tilde{d} + \tilde{e} < d + e,$$

generalised arithmetic progressions  $\tilde{\mathcal{A}}, \tilde{\mathcal{B}}$  of the form

$$\begin{aligned} \tilde{\mathcal{A}} &= \{\tilde{\alpha}_0 + \tilde{\alpha}_1 h_1 + \cdots + \tilde{\alpha}_{\tilde{d}} h_{\tilde{d}} : |h_i| \leq \tilde{C}_d H, i = 1, \dots, \tilde{d}\}, \\ \tilde{\mathcal{B}} &= \{\tilde{\beta}_0 + \tilde{\beta}_1 j_1 + \cdots + \tilde{\beta}_{\tilde{e}} j_{\tilde{e}} : |j_i| \leq \tilde{C}_d H, i = 1, \dots, \tilde{e}\}, \end{aligned}$$

with

$$\tilde{\alpha}_1, \dots, \tilde{\alpha}_d, \tilde{\beta}_1, \dots, \tilde{\beta}_e \in \overline{\mathbb{F}}_p^*,$$

and some  $\mu \in \overline{\mathbb{F}}_p^*$  such that

$$I_p(\mathcal{A}, \mathcal{B}, \lambda) \leq \exp(B_d \log H / \log \log H) I_p(\tilde{\mathcal{A}}, \tilde{\mathcal{B}}, \mu).$$



If  $p \nmid Z_\ell$ , then we obviously have  $p \nmid Z_{\ell-1}$  (since  $Z_{\ell-1} \mid Z_\ell$ ) and also  $p$  satisfies (5.1). Therefore, by our induction hypothesis (where we can also assume that  $C_d \geq C_*(d + e - 1)$ )

$$I_p(\mathcal{A}, \mathcal{B}, \lambda) \ll \exp((B_d + b_{\ell-1}) \log H / \log \log H).$$

The result now follows by taking

$$b_\ell = \max_{d \leq \ell} B_d + b_{\ell-1}, \quad Z = Z_\ell$$

and noting that  $Z_\ell$  is  $O(H^{1/\gamma_{\ell+1}})$ -smooth and satisfies

$$\log Z_\ell \ll H^{\ell(\ell+2)^2/4} \log H.$$

## 6 Proofs of results towards the Erdős–Szemerédi conjecture

**6.1 Proof of Theorem 2.2.** The celebrated theorem of Freiman [9] states that if  $\mathcal{A} \subseteq \mathbb{Z}$  is a finite set satisfying

$$|\mathcal{A} + \mathcal{A}| \leq K|\mathcal{A}|,$$

then there exist constants  $b(K)$  and  $d(K)$  depending only on  $K$ , and some generalised arithmetic progression  $\mathcal{B}$  of rank  $d(K)$  and size

$$|\mathcal{B}| \leq b(K)|\mathcal{A}|,$$

such that

$$\mathcal{A} \subseteq \mathcal{B}.$$

The theorem of Freiman [9] has gone through a number of improvements and generalisations to sets from arbitrary abelian groups.

A version of this result convenient for our application is due to Cwalina and Schoen [6, Theorem 4], which states that we may take  $\mathcal{B}$  proper,

$$b(K) \leq \exp(cK^4(\log K + 2)) \quad \text{and} \quad d(K) \leq 2K,$$

for some absolute constant  $c$  (note the additive group of  $\mathbb{F}_p$  has no proper subgroups, so only the first alternative of [6, Theorem 4] applies).

Thus, using Corollaries 2.1 and 2.3 with  $H = |\mathcal{A}|$ ,  $d = e = d(K)$ ,

$$\delta = \gamma_{2d(K)+1} = \frac{1}{(44K + 26)2^{12K+8}} \quad \text{and} \quad c_0(K) = C_0(2K),$$

where  $C_0(d)$  is as in Corollary 2.1 (which we can assume to be monotonically increasing with respect to both  $d$  and  $e$ ), we obtain that for each  $\lambda \in \mathbb{F}_q^*$ , the number of solutions to each of the equations

$$a_1 a_2 = \lambda, \quad a_1^{-1} + a_2^{-1} = \lambda, \quad a_1^2 + a_2^2 = \lambda,$$

over  $\mathbb{F}_p$  with variables  $a_1, a_2 \in \mathcal{A}$  is  $|\mathcal{A}|^{o(1)}$  since we assume that  $K$  is fixed, from which the desired result follows.

**6.2 Proof of Theorem 2.3.** We follow the proof of Theorem 2.2, however apply Corollary 2.2 instead of Corollary 2.1.

**Acknowledgements.** The authors would like to thank Giorgis Petridis for pointing out that Theorem 2.2 is a finite field analogue of a result of Elekes and Ruzsa [8]. The authors are also grateful to Misha Rudnev for many useful comments and queries, which helped to discover a gap in the initial version.

During this work, B. K. was supported by Australian Research Council Grant DP160100932, Academy of Finland Grant 319180 and the Max Planck Institute for Mathematics, J. M. was supported by Australian Research Council Grant DP180100201, by NSERC and by the Max Planck Institute for Mathematics, and I. S. was supported by Australian Research Council Grants DP170100786 and DP180100201.

#### REFERENCES

- [1] E. Bombieri, J. Bourgain and S. V. Konyagin, *Roots of polynomials in subgroups of  $\mathbb{F}_p^*$  and applications to congruences*, Int. Math. Res. Not. IMRN **2009** (2009), 802–834.
- [2] J. Bourgain, M. Z. Garaev, S. V. Konyagin and I. E. Shparlinski, *On the hidden shifted power problem*, SIAM J. Comput. **41** (2012), 1524–1557.
- [3] M.-C. Chang, *Factorization in generalized arithmetic progressions and applications to the Erdős–Szemerédi sum-product problem*, Geom. Funct. Anal. **13** (2003), 720–736.
- [4] M.-C. Chang, C. D’Andrea, A. Ostafe, I. E. Shparlinski and M. Sombra, *Orbits of polynomial dynamical systems modulo primes*, Proc. Amer. Math. Soc. **146** (2018), 2015–2025.
- [5] M. Chang, B. Kerr, I. Shparlinski and U. Zannier, *Elements of large order on varieties over prime finite fields*, J. Théor. Nombres Bordeaux **26** (2014), 579–594.
- [6] K. Cwalina and T. Schoen, *A linear bound on the dimension in Green-Ruzsa’s theorem*, J. Number Theory **133** (2013) 1262–1269.
- [7] C. D’Andrea, A. Ostafe, I. Shparlinski and M. Sombra, *Reductions modulo primes of systems of polynomial equations and algebraic dynamical systems*, Trans. Amer. Math. Soc. **371** (2019), 1169–1198.
- [8] G. Elekes and I. Z. Ruzsa, *Few sums, many products*, Studia Sci. Math. Hungar. **40**, (2003), 301–308.

- [9] G. A. Freiman, *On the addition of finite sets*, Dokl. Akad. Nauk SSSR **158** (1964), 1038–1041; English translation: Sov. Math., Dokl. **5** (1964), 1366–1370.
- [10] C. Grosu,  $\mathbb{F}_p$  is locally like  $\mathbb{C}$ , J. London Math. Soc. (2) **89** (2014), 724–744.
- [11] M. Grötschel, L. Lovász and A. Schrijver, *Geometric Algorithms and Combinatorial Optimization*, Springer, Berlin, 1993.
- [12] D. R. Heath-Brown, *The density of rational points on curves and surfaces*, Ann. of Math. (2) **155** (2002), 553–595.
- [13] S. V. Konyagin, S. V. Makarychev, I. E. Shparlinski and I. V. Vyugin, *On the structure of graphs of Markoff triples*, Q. J. Math **71** (2020), 637–648.
- [14] A. Mohammadi, T. Pham and A. Warren, *A point-conic incidence bound and applications over  $\mathbb{F}_p$* , European J. Combin. **107** (2023), Article no. 103596.
- [15] B. Murphy, G. Petridis, O. Roche-Newton, M. Rudnev and I. D. Shkredov, *New results on sum-product type growth over fields*, Mathematika **65** (2019), 588–642.
- [16] I. D. Shkredov, *Modular hyperbolas and bilinear forms of Kloosterman sums*, J. Number Theory **220** (2021) 182–211.
- [17] I. E. Shparlinski, *Orders of points in families of elliptic curves*, Proc. Amer. Math. Soc. **148** (2020), 2371–2377.

*Bryce Kerr and Jorge Mello*

MAX PLANCK INSTITUTE FOR MATHEMATICS

VIVATSGASSE 7

53111 BONN, GERMANY

email: bryce.kerr89@gmail.com, jbmello@yorku.ca

*Igor E. Shparlinski*

SCHOOL OF MATHEMATICS AND STATISTICS

UNIVERSITY OF NEW SOUTH WALES

SYDNEY, NSW 2052, AUSTRALIA

email: igor.shparlinski@unsw.edu.au

(Received May 12, 2020 and in revised form June 20, 2022)