*Periodica Mathematica Hungarica Vol. 25 (1), (1992), pp. 105–111*

# ARITHMETICAL PROGRESSIONS AND THE NUMBER OF SUMS

I. Z. RUZSA (Budapest)

## 1. Introduction

Let $A$ be a finite set of integers, $|A| = n$. Freiman (1966/1973, Theorem 2.30) proved the following theorem. If $|A + A| \le cn$ and $n > n_0(c)$, then $A$ contains a three-term arithmetical progression. We give an effective version of this result.

Let $r_k(n)$ denote the maximal number of integers that can be selected from the interval $[1, n]$ without including a $k$ term arithmetical progression and write

$$\omega_k(n) = n/r_k(n).$$

We know from Szemerédi's (1975) theorem that $\omega_k(n) \to \infty$ for every fixed $k$.

THEOREM 1. *Assume that $|A| = n$ and $A$ does not contain any $k$-term arithmetical progression. We have*

$$|A + A - A - A| \ge \frac{1}{12}\omega_k(n)n, \tag{1.1}$$

$$|A + B| \ge \frac{1}{2}\omega_k(n)^{1/4}n^{1/4}|B|^{3/4} \tag{1.2}$$

*for every set $B$,*

$$|A + B| \ge \frac{1}{2}\omega_k(n)^{1/4}n \tag{1.3}$$

*for every set $B$ such that $|B| = n$,*

$$|A + A| \ge \frac{1}{2}\omega_k(n)^{1/4}n, \tag{1.4}$$

$$|A - A| \ge \frac{1}{2}\omega_k(n)^{1/4}n. \tag{1.5}$$

* Supported by Hungarian National Foundation for Scientific Research, Grant No. 1901.

*Mathematics subject classification numbers*, 1991. Primary. 11A99

*Key words and phrases.* Progressions, number of sums.

*Akadémiai Kiadó, Budapest*
*Kluwer Academic Publishers, Dordrecht*

It is known that $\omega_3(n) \gg (\log n)^c$ with a positive constant $c$ (Heat–Brown (1987), Szemerédi (1990)). Applying this estimate we obtain the following version of Freiman's theorem.

COROLLARY 1.1. *Assume that $|A| = n$ and $A$ does not contain any 3-term arithmetical progression. With a positive absolute constant $c$ and $n > n_0$ we have*

$$|A+B| \geq \frac{1}{2} n (\log n)^c \tag{1.6}$$

*for every set $B$ such that $|B| = n$, in particular*

$$|A+A| \geq \frac{1}{2} n (\log n)^c, \tag{1.7}$$

$$|A-A| \geq \frac{1}{2} n (\log n)^c. \tag{1.8}$$

Freiman's proof is based on his main theorem, which gives a covering of a set $A$ satisfying $|A+A| \leq \alpha|A|$ by another set isomorphic (in his sense, to be defined later) to a set of lattice points in a convex region of size $Cn, C = C(\alpha)$. He gives no estimate of $C(\alpha)$. His results (Chapter 1, sect. 3) show that $C(\alpha)$ must be at least an exponential function of $\alpha$, so in his way one cannot get a better lower estimate in (1.4) than $\log \omega_k(n)$. Our proof goes along completely different lines, though we also use Freiman's fundamental concept of isomorphism.

PROBLEM. Can the exponent 1/4 in (1.4–5) be improved to 1 or at least to $1 - \varepsilon$?

## 2. A partial Freiman isomorphy

Let $G_1$, $G_2$ be commutative groups, $A_1 \subset G_1$, $A_2 \subset G_2$. We say that a mapping $\Phi : A_1 \to A_2$ is a *homomorphism of order $r$ in the sense of Freiman*, or an *$F_r$-homomorphism* for short, if for every $x_1, \ldots, x_r, y_1, \ldots, y_r \in A_1$ (not necessarily distinct) the equation

$$x_1 + x_2 + \cdots + x_r = y_1 + y_2 + \cdots + y_r \tag{2.1}$$

implies

$$\Phi(x-1) + \Phi(x_2) + \cdots + \Phi(x_r) = \Phi(y_1) + \Phi(y_2) + \cdots + \Phi(y_r). \tag{2.2}$$

We call $\Phi$ an *$F_r$-isomorphism,* if it is (1-1) and its inverse is a homomorphism as well, that is, (2.2) holds if and only if (2.1) does.

Any affine linear function is an $F_r$-isomorphism for every $r$, and the nondegenerate ones are $F_r$-isomorphisms.

For iterated additions of a set to itself we introduce the following notation:

$$Ak = A + A + \cdots + A, \qquad k \text{ summands.}$$

THEOREM 2. *Let $A$ be a set of integers, $|A| = n, r \geq 2$ an integer and $D = Ar - Ar$. Write $|D| = N$.*

*(a) For every $m > 2r(N-1)$ there exists a set $A' \subset A, |A'| \geq n/r$ which is $F_r$-isomorphic to a set $T'$ of residues* mod $m$.

*(b) There is a set $A^* \subset A, |A^*| \geq n/r^2$ which is $F_r$-isomorphic to a set $T^*$ of integers,*

$$T^* \subset [1, 2N].$$

PROOF. (a) Select a prime $p \equiv 1 (\bmod m)$,

$$p > 4r \max_{a \in A} |a| \tag{2.3}$$

The isomorphism will be given by

$$\Phi(a) = ((aq) \bmod p) \bmod m$$

with a suitable $1 \leq q \leq p-1$; here we used $x \bmod y$ to denote the least nonnegative residue of $x$ modulo $y$.

We consider $\Phi$ as a composition of four maps:

$$\mathbf{Z} \xrightarrow{\psi_1} \mathbf{Z}_p \xrightarrow{\psi_2} \mathbf{Z}_p \xrightarrow{\psi_3} \mathbf{Z} \xrightarrow{\psi_4} \mathbf{Z}_m.$$

Here $\psi_1$ maps every integer to its residue class modulo $p, \psi_2$ is a multiplication by $q, \psi_3$ maps a residue class into its representant in $[0, p-1]$ and $\psi_4$ is the residue class modulo $m$.

Here $\psi_1$ is an $F_r$-isomorphism on $A$ by (2.3), and $\psi_2$ is one obviously. The critical point is $\psi_4$; we shall show that it is an isomorphism for a suitable choice of $q$, and we return to $\psi_3$ afterwards.

The composition of $\psi_1$, $\psi_2$, $\psi_3$ is the function

$$\vartheta(a) = (qa) \bmod p = qa - p\left[\frac{qa}{p}\right].$$

Let $U = \vartheta(A)$ be the image of $A$. We show that $\psi_4$ is an $F_r$-isomorphism between $U$ and $\psi_4(U)$ for a suitable $q$. This means that

$$\psi_4(u_1) + \psi_4(u_2) + \cdots + \psi_4(u_r) = \psi_4(v_1) + \psi_4(v_2) + \cdots + \psi_4(v_r)$$

is possible only if $u_1 + \cdots + u_r = v_1 + \cdots + v_r$, in other words,

$$m | u_1 + \cdots + u_r - (v_1 + \cdots + v_r) = z \tag{2.4}$$

with $u_i, v_j \in U$ can hold only if $z = 0$.

Let $u_i = \vartheta(a_i), v_j = \vartheta(b_j), w = a_1 + \cdots + a_k - (b_1 + \cdots + b_k)$. We have $w \in D$, and by definition we know that

$$z \equiv qw (\operatorname{mod} p),$$

and also that $|z| \le r(p-1)$, since $u_i, v_j \in [0, p-1]$. Hence

$$z = (qw) \operatorname{mod} p + xp, \qquad -r \le x \le r-1.$$

Thus to avoid (2.4) it is sufficient to exclude

$$m | (qw) \operatorname{mod} p + xp, \qquad w \in D, \qquad w \ne 0, \qquad -r \le x \le r-1. \tag{2.5}$$

We count the number of those triplets $(q, x, w)$ for which (2.5) holds. For a fixed $w \ne 0$, the value of $(qw)$ mod $p$ runs over all numbers $1, 2, \dots, p-1$, of which $\frac{p-1}{m}$ fall in each residue class modulo $m$, hence $\frac{p-1}{m}$ satisfy (2.5). Taking into account the $N-1$ possible values of $w \ne 0$ and the $2r$ values of $x$, (2.5) has altogether at most

$$2r(N-1)\frac{p-1}{m}$$

solutions. If

$$2r(N-1)\frac{p-1}{m} < p-1, \tag{2.6}$$

then there is at least one choice of $q$ without a solution. (2.6) is equivalent to the condition $m > 2r(N-1)$ of the theorem.

Now we return to $\psi_3$. We need to slect an $A' \subset A$ such that $\psi_3$ is an isomorphism on $V' = \psi_2(\psi_1(A'))$. We split $V = \psi_2(\psi_1(A)) \subset [0, p-1]$ into $r$ parts,

$$V_i = V \cap \left[\frac{i-1}{r}(p-1), \frac{i}{r}(p-1)\right], \qquad i = 1, \dots, r.$$

We show that $\psi_3$ is an isomorphism on each $V_i$. Indeed, if $u_1, \dots, u_r \in U_i$, then

$$u_1 + \cdots + u_r \in [(i-1)(p-1), i(p-1)],$$

an interval of length $p-1$, thus two such sums can be congruent modulo $p$ only if they are equal.

At least one part satisfies $|V_i| \ge n/r$. We put $V' = V_i$, and this concludes the proof of part (a).

To prove part (b), we add another map to our diagram,

$$\mathbf{Z}_m \xrightarrow{\psi_5} \mathbf{Z},$$

where $\psi_5$ is again the smallest nonnegative representation of a residue class. We put $m = 2rN$ and repeat the last argument. We split the integers of the interval $[0, m-1]$ into $r$ equal subintervals of type $[2(i-1)N, 2iN-1]$, $i = 1, \ldots, r$. The $r$-fold sums from a fixed interval lie in an interval of length $< m$, thus they are incongruent modulo $m$ unless they the equal. In this way we can achieve

$$|A^*| \geq |A'|/r \geq n/r^2.$$

The isomorphic image of $A^*$ lies in an interval of type $[2(i-1)N, 2iN-1]$, and a shift takes it into $[1, 2N]$. ■

## 3. On the size of double and multiple sums

To apply the previous results for sets where only an estimate of $|A + A|$ is known, we connect this quantity to $|Ak - Al|$.

LEMMA 3.1. *Let $1 \leq j \leq k$ be integers, $A$, $B$ subsets of an arbitrary Abelian group. Write $|B| = n$, $|B + Aj| = \alpha n$. There is a nonempty $B' \subset B$ such that*

$$|B' + Ak| \leq \alpha^{k/j}|B'|. \tag{3.1}$$

This can be proved by applying Plünnecke's (1970) method, developed to study the Schnirelman density of sumsets. (3.1) was deduced and a simplified proof of Plünnecke's theorem was given in Ruzsa (1989).

LEMMA 3.2. *For arbitrary sets $U, V, W$ (in an Abelian group) we have*

$$|U||V - W| \leq |U - V||U - W|. \tag{3.2}$$

See Ruzsa (1978).

LEMMA 3.3. *Let $A$, $B$ be subsets of an arbitrary Abelian group. Write $|B| = n, |B + A| = \alpha n$. For arbitrary positive integers $k, l$ we have*

$$|Ak - Al| \leq \alpha^{k+l}n. \tag{3.3}$$

PROOF. Without restricting generality we may assume $k \leq l$. We apply Lemma 3.1 with $j = 1$ to find a set $\emptyset \neq B' \subset B$ such that

$$|B' + Ak| \le \alpha^k |A'|. \tag{3.4}$$

Next we apply Lemma 3.1 with $A', k, l$ in the place of $A, j, k$ to get a set $\emptyset \ne B'' \subset B'$ such that

$$|B'' + Al| \le \alpha^l |B''|. \tag{3.5}$$

Substituting $U = -B'', V = Ak, W = Al$ into (3.2) and applying (3.5) we obtain

$$|B''||Ak - Al| \le |B'' + Al||B'' + Al| \le \alpha^l |B'' + Ak|.$$

Now we can divide by $|B''|$ and use (3.4) to deduce

$$|Ak - Al| \le \alpha^l |B'' + Ak| \le \alpha^l |B' + Ak| \le \alpha^l \alpha^k |A'| \le \alpha^{k+l} n.$$

■

By substituting $\alpha = |B+A|/|B|$, Lemma 3.3 can be rewritten in the following way:

$$|Ak - Al| \le |B + A|^{k+l} |B|^{1-k-l}$$

or

$$|A + B| \ge |B|^{1-\frac{1}{k+l}} |Ak - Al|^{\frac{1}{k+l}}. \tag{3.6}$$

## 4. Estimates on arithmetical progressions

We prove Theorem 1.

LEMMA 4.1. *If one of two $F_2$-isomorphic sets contains a $k$-term arithmetical progression, then so does the other.*

PROOF. The numbers $x_1, \dots, x_k$ form an arithmetical progression if and only if they satisfy the equations

$$x_1 + x_3 = 2x_2,$$
$$x_2 + x_4 = 2x_3,$$
$$\dots$$
$$x_{k-2} + x_k = 2x_{k-1},$$

which are preserved by an $F_2$-isomorphism. ■

PROOF OF THEOREM 1. Write $|A| = n$ and $|A2 - A2| = \beta n$. We apply the case $r = 2$ of Theorem 2, part (b). We get a set $A^* \subset A$, $|A^*| \ge n/4$ which is isomorphic to a set $T \subset [1, 2\beta n]$. By the previous lemma, $T$ contains no $k$-term arithmetical progression.

Since in an interval of length $n$ there can be at most $r_k(n)$ integers without $k$-term arithmetical progression and the interval $[1, 2\beta n]$ can be covered by $[1 + 2\beta]$ such intervals, we have

$$n/4 \le |T| \le [1 + 2\beta] r_k(n) \le 3\beta r_k(n),$$

therefore

$$\beta \ge \frac{1}{12} \frac{n}{r_k(n)},$$

which is equivalent to (1.1).

To obtain (1.2) we apply (3.6) with $k = l = 2$ and (1.1) as follows:

$$|A + B| \ge |B|^{3/4} |A2 - A2|^{1/4} \ge \frac{1}{2} |B|^{3/4} \omega_k(n)^{1/4} n^{1/4}.$$

(1.3) is the case $|B| = n$ of (1.2), while (1.4–5) are the cases $B = A$ and $B = -A$ of (1.3). ■

## REFERENCES

G. A. FREIMAN, (1966), *Foundations of a Structural Theory of Set Addition* (in Russian), Kazan Gos. Ped. Inst., Kazan.

G. A. FREIMAN, (1973), *Foundations of a Structural Theory of Set Addition*, Translation of Mathematical Monographs Vol. 37, Amer. Math. Soc., Providence, R. I., USA.

D. R. HEATH-BROWN, (1987), Integer sets containing no arithmetic progressions, *J. London Math. Soc.* **35**, 385–394.

H. PLÜNNECKE, (1970), Eine zahlentheoretische Anwendung der Graphtheorie, *J. Reine Angew. Math.* **243** 171–183.

I. Z. RUZSA, (1978), On the cardinality of $A + A$ and $A - A$, in: *Coll. Math. Soc. J. Bolyai 18, Combinatorics, Keszthely 1976,* North-Holland - Bolyai Társulat, Budapest (1978), 933–938.

I. Z. RUZSA, (1989), An application of graph theory to additive number theory, *Scientia, Ser. A* **3** 97–109.

E. SZEMERÉDI, (1975), On sets of integers containing no $k$-elements in arithmetic progression, *Acta Arithmetica* **27**, 299–345.

E. SZEMERÉDI, (1990), Integer sets containing no arithmetic progressions, *Acta Math. Acad. Sci. Hungar.* **56**, 155–158.

*(Received November 20, 1991)*

MATHEMATICAL INSTITUTE OF THE
HUNGARIAN ACADEMY OF SCIENCES
BUDAPEST, PF. 127
H–1364
HUNGARY