Conspectus materiae tomi XVII, fasciculi 3

La revue est consacrée à la Théorie des Nombres
The journal publishes papers on the Theory of Numbers
Die Zeitschrift veröffentlich Arbeiten aus der Zahlentheorie
Журнал посвящен теории чисел

L'adresse de la Rédaction et de l'échange	Address of the Editorial Board and of the exchange	Die Adresse der Schriftleitung und des Austausches	Адрес Редакции и книгообмена

ACTA ARITHMETICA
ul. Śniadeckich 8, Warszawa 1

Les volumes IV et suivants sont à obtenir chez	Volumes from IV on are available at	Die Bände IV und die folgende sind zu beziehen durch	Томы IV и следующие можно получить через

Ars Polona, Krakowskie Przedmieście 7, Warszawa 1

Prix d'un fascicule	Prize of an issue	Preis für ein Heft	Цена номера

\$ 4.00

Les volumes I–III sont à obtenir chez	Volumes I–III are available at	Die Bände I–III sind zu beziehen durch	Томы I–III можно получить через

Johnson Reprint Corporation, 111 Fifth Ave., New York, N. Y.

PRINTED IN POLAND

WROCŁAWSKA DRUKARNIA NAUKOWA

ACTA ARITHMETICA
XVII (1970)

On a conjecture of Erdös and Heilbronn

by

E. Szemerédi (Budapest)

Let G be an Abelian group of n elements. Let $a_1, a_2, \ldots, a_k$ be k distinct elements of G. Denote by $F(k)$ the number of solutions of (e is the unit element of G)

$$e = \prod_{i=1}^{k} a_i^{\varepsilon_i}, \qquad \varepsilon_i = 0 \text{ or } 1.$$

Erdös and Heilbronn [1] conjectured that $F(k) > 0$ if $k > c\sqrt{n}$ (c is an absolute constant).

Ryavec [2] proved that $F(k) > 0$ if

$$k > 3\sqrt{6n}\cdot\exp\left(c\frac{\sqrt{\log n}}{\log\log n}\right).$$

In this paper we prove the conjecture of Erdös and Heilbronn. They further conjectured that $F(k) > 0$ if $k > 2\sqrt{n}$ and that it is not necessary to assume that G is Abelian. At present I can not decide these conjectures (¹).

Notation. Definitions. Let G be an Abelian group. Let H denote the set of elements of G. $A, B, \ldots, U, V$ possibly with subscripts always denote subsets of H. The number of elements of A will be denoted by $|A|$. Put

$$A^* = \{\textstyle\sum \varepsilon_i a_i \colon a_i \in A,\ \varepsilon_i = 0 \text{ or } 1 \text{ but not all } \varepsilon_i \text{ are } 0\}.$$

We are going to prove

THEOREM. *There exist a real number $c > 0$ and an integer n_0 such that for every $n > n_0$, for every G, and for every $A \subset H$, $|A| \geqslant c\sqrt{n}$*

$$0 \in A^*.$$

(¹) Remark of the editor. The first conjecture for n being a prime and for certain other cases has been recently proved by J. Olson [3], [4].

Proof. Assume that (1) holds.

(1) There exist $c > 100$, $D, A_1, A_2, \ldots, A_l, B_1, B_2, \ldots, B_l$ satisfying the following conditions:

(i) $\frac{1}{4}c\sqrt{n} < |D| < \frac{3}{4}c\sqrt{n}$,

(ii) $A_i - D = \{a_i\}$, $D - B_i = \{b_i\}$, $D, A_i, B_i \subset A$ $(i = 1, 2, \ldots, l)$,

(iii) $|A_i^* - D^*| \leqslant \sqrt{n}$, $|D^* - B_i^*| \leqslant \sqrt{n}$ $(i = 1, 2, \ldots, l)$,

(iv) $l > 3\sqrt{n}$.

Put $d = \sum_{a \in D} a$. Let $M = \{m_{ik}\}$ be the matrix defined by the stipulation

$$m_{ik} = d - b_i + a_k \quad (i, k = 1, \ldots, l). \tag{2}$$

Obviously, $m_{ik} \in A_k^*$, and considering that by (1)(iii) $|A_k^* - D^*| \leqslant \sqrt{n}$ the kth column contains at least $l - \sqrt{n}$ elements of D^*. It follows, that there exists an i $(1 \leqslant i \leqslant l)$ such that the ith row contains at least $l - \sqrt{n}$ elements of D^*. Considering that, by (1)(iii), $|D^* - B_i^*| \leqslant \sqrt{n}$ the ith row contains at least $l - 2\sqrt{n}$ elements of B_i^*. Let m_{iq} be one of these elements. Then m_{iq} can be written in the form

$$m_{iq} = \sum_{a \in B_i} \varepsilon_a a, \quad \varepsilon_a = 0 \text{ or } 1$$

and by (2)

$$m_{iq} = d - b_i + a_q,$$

hence

$$\sum_{a \in D} a - b_i + a_q = \sum_{a \in B_i} a + a_q = \sum_{a \in B_i} \varepsilon_a a.$$

Thus $0 \in A_q^* \subset A^*$.

It follows that it is sufficient to prove that (1) holds.

Let

$$X = \{(U, V) \colon U \subset V, |V - U| = 1, |V^* - U^*| \leqslant \sqrt{n}\}. \tag{3}$$

Assume that

(4) There is an i, $\frac{1}{4}c\sqrt{n} < i < \frac{3}{4}c\sqrt{n}$, and such that

$$|\{(U, V) \in X \colon |V| = i+1\}| \geqslant \frac{4}{5}\binom{|A|}{i}(|A| - i)$$

and

$$|\{(U, V) \in X \colon |V| = i\}| \geqslant \frac{4}{5}\binom{|A|}{i-1}(|A| - i - 1).$$

Meditation shows that (4) implies

$$\big|\{U \colon |U| = i \text{ and } |\{V \colon (U, V) \in X\}| \leqslant 3\sqrt{n}\}\big| < \frac{1}{2}\binom{|A|}{i} \tag{5}$$

and

$$\big|\{V \colon |V| = i \text{ and } |\{U \colon (U, V) \in X\}| \leqslant 3\sqrt{n}\}\big| < \frac{1}{2}\binom{|A|}{i}.$$

(5) obviously implies (1), hence we only need to prove (4). We assume that (4) is false and we conclude the proof by obtaining a contradiction. Let Y be the set of all chains $(A_1, A_2, \ldots, A_q)$, satisfying the conditions

$$[\tfrac{1}{4}c\sqrt{n}] = |A_1|, \quad [\tfrac{3}{4}c\sqrt{n}] = A_q,$$

$$A_i \subset A_{i+1}, \quad |A_{i+1} - A_i| = 1 \quad (i = 1, \ldots, q-1).$$

For every chain $(A_1, A_2, \ldots, A_q) \in Y$, $(A_i, A_{i+1}) \in X$ if and only if $|A_{i+1}^* - A_i^*| \leqslant \sqrt{n}$ for $1 \leqslant i \leqslant q-1$. If (4) is false, then there must be a chain $(A_1, A_2, \ldots, A_q) \in Y$ such that

$$|\{i \colon (A_i, A_{i+1}) \notin X\}| > [\tfrac{1}{20}q].$$

Then $[\frac{1}{20}q] \geqslant \sqrt{n}$, hence

$$A_q^* > n,$$

a contradiction.

Eggleston and Erdös raised the following problem (oral communication): Let $f(k)$ be the largest integer so that if $a_1, a_2, \ldots, a_k$ are k elements of G so that the unit element is not of the form

$$\prod_{i=1}^{k} a_i^{\varepsilon_i}, \quad \varepsilon_i = 0 \text{ or } 1 \quad (\text{not all } \varepsilon_i = 0) \tag{6}$$

then there are at least $f(k)$ distinct elements of the form (6). They proved $f(2) = 3$, $f(3) = 5$, $f(4) = 8$, $f(k) \geqslant 2k-1$ and conjectured $f(k) > ck^2$. By the methods of the present paper I can prove this conjecture.

References

[1] P. Erdös and H. Heilbronn, *On the addition of residue classes* mod p, Acta Arith. 9 (1964), pp. 149–159.

[2] C. Ryavec, *The addition of residue classes modulo* n, Pacific Journ. Math. 26 (1968), pp. 367–373.

[3] J. Olson, *An addition theorem modulo* p, J. Combinatorial Theory 5 (1968), pp. 45–52.

[4] — *An addition theorem for the elementary Abelian groups*, J. Combinatorial Theory 5 (1968), pp. 53–58.

Received on 15. 5. 1969