# RESTRICTED SET ADDITION: THE EXCEPTIONAL CASE OF THE ERDŐS–HEILBRONN CONJECTURE

GYULA KÁROLYI[1] Department of Algebra and Number Theory, Eötvös University, Pázmány P. sétány 1/C, Budapest, H–1117 Hungary

Abstract. Let $A \neq B$ be nonempty subsets of the group of integers modulo a prime $p$. If $p \geq |A|+|B|-2$, then at least $|A|+|B|-2$ different residue classes can be represented as $a+b$, where $a \in A$, $b \in B$ and $a \neq b$. This result complements the solution of a problem of Erdős and Heilbronn obtained by Alon, Nathanson, and Ruzsa.

## 1. The Result

For nonempty subsets $A, B$ of an abelian group $G$ define their restricted sumset as

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

Concerning a conjecture of Erdős and Heilbronn [10, 11], in 1994 Dias da Silva and Hamidoune [6] established the inequality

$$|A \dot{+} A| \geq \min\{p, 2|A| - 3\}$$

via exterior algebra methods in the case when $G = \mathbb{Z}/p\mathbb{Z}$ is a cyclic group of prime order. With an application of the polynomial method of Alon and Tarsi

[1]Visiting I.H.É.S. Research partially supported by Hungarian Scientific Research Grants OTKA T043623 and T043631.

[4], Alon, Nathanson, and Ruzsa [2, 3] obtained the more comprehensive result

$$|A\dot{+}B| \geq \min\{p, |A|+|B|-2\} \tag{1}$$

whenever $|A| \neq |B|$, which clearly implies the relation

$$|A\dot{+}B| \geq \min\{p, |A|+|B|-3\}$$

in general. Some ramifications in elementary abelian $p$-groups have been explored in a series of papers by Eliahou and Kervaire [7, 8, 9].

However, $|A\dot{+}B| \geq |A|+|B|-2$ holds in every torsion free abelian group whenever $A \neq B$ (see e.g. [14]), thus (1) has been expected to be also valid in $\mathbb{Z}/p\mathbb{Z}$ when $A \neq B$, but the existing methods do not work under the condition $|A| = |B|$, $A \neq B$. The purpose of the present paper is to circumvent this seemingly technical problem employing the Combinatorial Nullstellensatz of Alon [1]. Thus we prove

**Theorem 1.** *Let $A \neq B$ be nonempty subsets of the additive group of a field of characteristic $p$. Then $|A\dot{+}B| \geq \min\{p, |A|+|B|-2\}$.*

Coupled with the results of [15] this yields the following

**Corollary 2.** *Let $A, B$ be nonempty subsets of the additive group of a field of characteristic $p \geq |A|+|B|-2$. Then $|A\dot{+}B| \geq |A|+|B|-2$, unless $A = B$ and one of the following holds:*

(i) $|A| = 2$ *or* $|A| = 3$*;*
(ii) $|A| = 4$*, and* $A = \{a, a+d, c, c+d\}$*;*
(iii) $|A| \geq 5$*, and $A$ is an arithmetic progression.*

## 2. The Proof

Denote the field of characteristic $p$ at issue by $F$. If $|A|+|B|-2 > p$, then there exist nonempty subsets $A' \subseteq A$ and $B' \subseteq B$ such that $|A|+|B|-2 = p$ and $A' \neq B'$. Since $A'\dot{+}B' \subseteq A\dot{+}B$, it is enough to prove Theorem 1 for the pair $A', B'$. Thus we may assume that $p \geq |A|+|B|-2$. The statement is obvious if $p = 2$, so we also assume that $p$ is an odd prime, or $p = \infty$.

If $A$ and $B$ are *arbitrary* nonempty subsets of $F$ with $p \geq |A|+|B|-2$, then $|A\dot{+}B| \geq |A|+|B|-3$. Indeed, if $|A| \neq |B|$, then in fact $|A\dot{+}B| \geq |A|+|B|-2$ as it was proven by Alon, Nathanson, and Ruzsa in [2], see Theorem 1 therein.

Although it is formally stated only for prime fields, the proof works in arbitrary fields, as they mention it at the end of the paper. If $|A| = |B| \geq 2$, then this applied for the sets $A$ and $B' = B \setminus \{b\}$ for any $b \in B$ gives

$$|A\dot{+}B| \geq |A\dot{+}B'| \geq |A| + |B'| - 2 = |A| + |B| - 3.$$

If one of the sets has only one element, then the statement is obvious. Accordingly, we only have to prove the following version of Theorem 1.

**Theorem 3.** *Let $A, B$ be subsets of a field $F$ of characteristic $p > 2$ such that $|A| = |B| = k \geq 2$ and $p \geq 2k - 1$. If $|A\dot{+}B| = 2k - 3$, then $A = B$.*

Assume that $A = \{a_1, a_2, \ldots, a_k\}$, $B = \{b_1, b_2, \ldots, b_k\}$, and put

$$C = A\dot{+}B = \{c_1, c_2, \ldots, c_{2k-3}\}.$$

The polynomial $f \in F[x, y]$ defined as

$$f(x, y) = (x - y) \prod_{i=1}^{2k-3} (x + y - c_i)$$

has the property that $f(a_i, b_j) = 0$ for any $1 \leq i, j \leq k$. Recall the Combinatorial Nullstellensatz of Alon [1]:

**Lemma 4.** *Let $F$ be an arbitrary field and let $f = f(x_1, \ldots, x_k)$ be a polynomial in $F[x_1, \ldots, x_k]$. Let $S_1, \ldots, S_k$ be nonempty finite subsets of $F$ and define $g_i(x_i) = \prod_{s \in S_i}(x_i - s)$. If $f(s_1, s_2, \ldots, s_k) = 0$ for all $s_i \in S_i$, then there exist polynomials $h_1, h_2, \ldots, h_k \in F[x_1, \ldots, x_k]$ satisfying* $\deg(h_i) \leq \deg(f) - \deg(g_i)$ *such that $f = \sum_{i=1}^k h_i g_i$.*

Accordingly, we introduce the polynomials

$$g(x) = \prod_{i=1}^{k}(x - a_i) = x^k - \alpha_1 x^{k-1} + \alpha_2 x^{k-2} - \ldots + (-1)^k \alpha_k$$

and

$$h(y) = \prod_{i=1}^{k}(y - b_i) = y^k - \beta_1 y^{k-1} + \beta_2 y^{k-2} - \ldots + (-1)^k \beta_k,$$

where $\alpha_i = \sigma_i(A)$ and $\beta_i = \sigma_i(B)$ are the elementary symmetric functions of $a_1, a_2, \ldots, a_k$ resp. $b_1, b_2, \ldots, b_k$. In view of Lemma 4, there exist polynomials $q, r \in F[x, y]$ of degree at most $k - 2$ such that

$$f(x, y) = q(x, y)g(x) - r(y, x)h(y). \tag{2}$$

Writing

$$q(x,y)=\sum_{i=0}^{k-2} q_i(x,y), \quad r(x,y)=\sum_{i=0}^{k-2} r_i(x,y) \quad \text{and} \quad f_i(x,y)=(x-y)(x+y)^{i-1},$$

where $p_i, r_i, f_i$ are homogeneous polynomials of degree $i$, with the additional notations $\gamma_i=\sigma_i(C)$ $(1\le i\le 2k-3)$ and

$$q_{-1}=q_{-2}=r_{-1}=r_{-2}=0, \quad \alpha_0=\beta_0=\gamma_0=1,$$

Eq. (2) implies the following equations of homogeneous polynomials of degree $2k-2-t$ for every integer $0\le t\le k$:

$$(3) \qquad (-1)^t\gamma_t f_{2k-2-t}(x,y) = \sum_{j=0}^{t}(-1)^{t-j}\{\alpha_{t-j}q_{k-2-j}(x,y)x^{k-t+j} - \beta_{t-j}r_{k-2-j}(y,x)y^{k-t+j}\}.$$

Finally writing

$$q_i(x,y)=\sum_{u+v=i} A_{uv}x^u y^v \qquad \text{and} \qquad r_i(x,y)=\sum_{u+v=i} B_{uv}x^u y^v$$

we find that the equations (3) encode certain relations between the coefficients $A_{uv}, B_{uv}$ and the numbers $\alpha_i, \beta_i, \gamma_i$. The careful study of these relations, after a technical elimination process that we postpone until the next section, results in the following

**Lemma 5.** *For every integer $1\le t\le k$, $\alpha_t=\beta_t$ and $u+v=k-2-t$ implies $A_{uv}=B_{uv}$.*

Consequently, $g(z)=h(z)$. It means that $a_1,a_2,\dots,a_k$ and $b_1,b_2,\dots,b_k$ are the roots of the same polynomial of degree $k$, hence $A=B$ as claimed. It only remains to prove Lemma 5.

## 3. Details

For $1\le i\le 2k-3$, let

$$f_i(x,y)=(x-y)(x+y)^{i-1}=\sum_{u+v=i} C_{uv}x^u y^v.$$

Then $C_{i,0}=1$, $C_{0,i}=-1$, and in case $u,v\ne 0$ we have

$$C_{uv}=-C_{vu}=\binom{i-1}{u-1}-\binom{i-1}{u}=\frac{2u-i}{u}\binom{i-1}{u-1}.$$

Since $i < p$, $C_{uv} = 0$ if and only if $i$ is even and $u = v = i/2$. Consider $C_{uv} + C_{u-1,v+1}$. If $u = i$, then it is

$$C_{i,0} + C_{i-1,1} = 1 + \binom{i-1}{i-2} - \binom{i-1}{i-1} = i - 1,$$

a nonzero element in $F$ if $i > 1$. Similarly in the case $u = 1$,

$$C_{1,i-1} + C_{0,i} = 1 - i \neq 0.$$

In general, if $2 \leq u \leq i-1$, then

$$\begin{aligned} C_{uv} + C_{u-1,v+1} &= \frac{2u-i}{u}\binom{i-1}{u-1} + \frac{2u-2-i}{u-1}\binom{i-1}{u-2} \\ &= \left\{\frac{2u-i}{u}\cdot\frac{i-u+1}{u-1} + \frac{2u-2-i}{u-1}\right\}\binom{i-1}{u-2} \\ &= \frac{i(i-2v-1)}{u(u-1)}\binom{i-1}{u-2}. \end{aligned}$$

Thus we proved:

**Claim 6.** *If $i > 1$, then $C_{uv} + C_{u-1,v+1} = 0$ if and only if $i - 2v - 1 = 0$.*

We prove Lemma 5 by induction on $t$. Note that if $t > k-2$, then by definition $u + v = k - 2 - t$ implies $A_{uv} = B_{uv} = 0$. For the initial step, $\alpha_0 = \beta_0 = 1$ by definition. Let $u + v = k - 2$. To see that $A_{uv} = B_{uv}$, consider Eq. (3) for $t = 0$. It reads as

$$\sum_{u+v=2k-2} C_{uv}x^u y^v = \sum_{u+v=k-2} A_{uv}x^{u+k}y^v - \sum_{u+v=k-2} B_{uv}y^{u+k}x^v.$$

It follows that

$$B_{uv} = -C_{v,u+k} = C_{u+k,v} = A_{uv}. \tag{4}$$

For complete induction, let $1 \leq t \leq k$, and suppose that Lemma 5 has been already proved for smaller values of $t$. We start with the first statement. First we verify $\alpha_t = \beta_t$ in the case when $t$ is even, that is, $t = 2s$ for some $s \geq 1$. We have $k-1-s \geq k-1-(t-1) \geq 0$. Consider the coefficient of the term $x^{k-1-s}y^{k-1-s}$ in Eq. (3). On the left hand side this coefficient is $(-1)^t\gamma_t C_{k-1-s,k-1-s} = 0$. In the polynomial $q_{k-2-j}(x,y)x^{k-t+j}$, the coefficient of $x^{k-1-s}y^{k-1-s}$ is $A_{s-1-j,k-1-s}$ if $j \leq s-1$ and 0 otherwise, whereas in $r_{k-2-j}(y,x)y^{k-t+j}$, the coefficient of the same term is $B_{s-1-j,k-1-s}$ if $j \leq s-1$ and 0 otherwise. Thus Eq. (3) implies

$$\sum_{j=0}^{s-1}(-1)^{t-j}\left\{\alpha_{t-j}A_{s-1-j,k-1-s} - \beta_{t-j}B_{s-1-j,k-1-s}\right\} = 0.$$

Since $(s-1-j)+(k-1-s)=k-2-j$ and $s-1<t$, based on the induction hypothesis we have $A_{s-1-j,k-1-s} = B_{s-1-j,k-1-s}$ and $\alpha_{t-j} = \beta_{t-j}$ for every $1 \le j \le s-1$. The summation can thus be reduced to the first term and we obtain

$$\alpha_t A_{s-1,k-1-s} - \beta_t B_{s-1,k-1-s} = 0.$$

Here $(s-1)+(k-1-s)=k-2$, and in view of Eq. (4)

$$A_{s-1,k-1-s} = B_{s-1,k-1-s} = C_{s-1+k,k-1-s} \neq 0,$$

since $s-1+k \neq k-1-s$, given that $s \geq 1$. It follows that $\alpha_t = \beta_t$.

If $t$ is odd, that is, $t = 2s+1$ with some $s \geq 0$, then in Eq. (3) we consider the sum of the coefficients of the terms $x^{k-1-s}y^{k-2-s}$ and $x^{k-2-s}y^{k-1-s}$. (Note that $k-2-s \geq k-2-(t-2) \geq 0$, unless $k=t=1$, which is excluded by $k \geq 2$.) On the left hand side it is

$$(-1)^t\gamma_t(C_{k-1-s,k-2-s} + C_{k-2-s,k-1-s}) = 0.$$

Therefore Eq. (3) implies

$$\begin{aligned} 0 \quad = \quad & \sum_{j=0}^{s}(-1)^{t-j}\alpha_{t-j}A_{s-j,k-2-s} + \sum_{j=0}^{s-1}(-1)^{t-j}\alpha_{t-j}A_{s-1-j,k-1-s} \\ & -\sum_{j=0}^{s}(-1)^{t-j}\beta_{t-j}B_{s-j,k-2-s} - \sum_{j=0}^{s-1}(-1)^{t-j}\beta_{t-j}B_{s-1-j,k-1-s}. \end{aligned}$$

Since $(s-j)+(k-2-s) = (s-1-j)+(k-1-s) = k-2-j$ and $s<t$, the induction hypothesis once again allows us to reduce the above equation to

$$\begin{aligned} 0 \quad = \quad & (-1)^t\alpha_t A_{s,k-2-s} + (-1)^t\alpha_t A_{s-1,k-1-s} \\ & -(-1)^t\beta_t B_{s,k-2-s} - (-1)^t\beta_t B_{s-1,k-1-s}. \end{aligned}$$

In view of Eq. (4) this equation can be rewritten as

$$(\alpha_t - \beta_t)(C_{s+k,k-2-s} + C_{s-1+k,k-1-s}) = 0.$$

Since $(2k-2)-2(k-2-s)-1 = 2s+1 = t$ is not zero in $F$, in view of Claim 6 it follows that the second term is not zero, and we conclude that $\alpha_t - \beta_t = 0$, $\alpha_t = \beta_t$.

It remains to verify the second statement of the lemma under the additional assumption that the first statement has been already verified. Accordingly, we assume $t \leq k-2$, $\alpha_t = \beta_t$, and let $u+v = k-2-t$. On the left hand side of Eq. (3), the coefficient of $x^{u+k}y^v$ is $(-1)^t\gamma_t C_{u+k,v}$. If $0 \leq j \leq t$, then

$v \le k-2-t < k-t+j$, thus in $r_{k-2-j}(y,x)y^{k-t+j}$ the coefficient of $x^{u+k}y^v$ is 0. Therefore on the right hand side of Eq. (3), the coefficient of $x^{u+k}y^v$ is

$$\sum_{j=0}^{t}(-1)^{t-j}\alpha_{t-j}A_{t-j+u,v}.$$

Consequently, Eq. (3) implies

$$\sum_{j=0}^{t}(-1)^{t-j}\alpha_{t-j}A_{t-j+u,v} = (-1)^t\gamma_t C_{u+k,v}.$$

Looking at the coefficient of $x^v y^{u+k}$ the same way we obtain

$$-\sum_{j=0}^{t}(-1)^{t-j}\beta_{t-j}B_{t-j+u,v} = (-1)^t\gamma_t C_{v,u+k}.$$

Since $C_{v,u+k} = -C_{u+k,v}$, it follows that

$$\sum_{j=0}^{t}(-1)^{t-j}\alpha_{t-j}A_{t-j+u,v} = \sum_{j=0}^{t}(-1)^{t-j}\beta_{t-j}B_{t-j+u,v}.$$

Because $(t-j+u)+v = k-2-j$, the induction hypothesis implies $A_{t-j+u,v} = B_{t-u+j,v}$ for $0 \le j < t$. We have furthermore assumed $\alpha_{t-j} = \beta_{t-j}$ for all $0 \le j \le t$, therefore the above equality can be reduced to

$$(-1)^{t-t}\alpha_{t-t}A_{t-t+u,v} = (-1)^{t-t}\beta_{t-t}B_{t-t+u,v}.$$

Since $\alpha_0 = \beta_0 = 1$, we obtain $A_{uv} = B_{uv}$.

## 4. Remarks

The strategy of the above proof is very similar to that of the inverse theorem contained in our previous work [15], and in fact the technical details are much more simple. In retrospect, the present paper should have preceded [15], but at that time it seemed very complicated to handle the restricted sumset of two different sets using the Combinatorial Nullstellensatz.

For any nontrivial group $G$, let $p(G)$ denote the order of the smallest nontrivial subgroup in $G$. In [12, 13] we extended the result of Dias da Silva and Hamidoune proving that

$$|A \dot{+} A| \ge \min\{p(G), 2|A|-3\}$$

holds in any abelian group $G$. Further developing this technique and the method of group extensions introduced in [16], Balister and Wheeler [5] established

$$|A \dot{+} B| \geq \min\{p(G), |A| + |B| - 3\}$$

in every group. It is quite plausible, that Theorem 1 and Corollary 2 can also be generalized in the same spirit.

**Acknowledgment** Part of this work has been achieved thanks to the support of the European Commission through its 6th Framework Programme "Structuring the European Research Area" and the contract Nr. RITA-CT-2004-505493 for the provision of Transnational Access implemented as Specific Support Action.

## References

[1] N. Alon, Combinatorial Nullstellensatz, *Combin. Prob. Comput.* **8** (1999) 7–29
[2] N. Alon, M.B. Nathanson, and I.Z. Ruzsa, Adding distinct congruence classes modulo a prime, *Amer. Math. Monthly* **102** (1995) 250–255
[3] N. Alon, M.B. Nathanson, and I.Z. Ruzsa, The polynomial method and restricted sums of congruence classes, *J. Number Th.* **56** (1996) 404–417
[4] N. Alon and M. Tarsi, Colorings and orientations of graphs, *Combinatorica* **12** (1992) 125–134
[5] P. Balister and J.P. Wheeler, The Erdős–Heilbronn conjecture for finite groups, *Acta Aritmetica*, to appear
[6] J.A. Dias da Silva and Y.O. Hamidoune, Cyclic spaces for Grassmann derivatives and additive theory, *Bull. London Math. Soc.* **26** (1994) 140–146
[7] S. Eliahou and M. Kervaire, Sumsets in vector spaces over finite fields, *J. Number Th.* **71** (1998) 12–39
[8] S. Eliahou and M. Kervaire, Restricted sums of sets of cardinality $1+p$ in a vector space over $F_p$, *Discrete Math.* **235** (2001) 199–213
[9] S. Eliahou and M. Kervaire, Restricted sumsets in finite vector spaces: the case $p=3$, *Integers* **1** (2001), Research paper A2, 19 pages (electronic)
[10] P. Erdős, Some problems in number theory, in: Computers in Number Theory (A.O.L. Atkin and B.J. Birch, eds.), Acedemic Press, 1971, pp. 405–414
[11] P. Erdős and R.L. Graham, Old and New Problems and Results in Combinatorial Number Theory, *L'Enseignement Mathématique*, Geneva, 1980
[12] Gy. Károlyi, On restricted set addition in abelian groups, *Ann. Univ. Sci. Budapest. Eötvös Sect. Math.* **46** (2003) 47–54
[13] Gy. Károlyi, The Erdős–Heilbronn problem in abelian groups, *Israel J. Math.* **139** (2004) 349–359

[14] Gy. Károlyi, A compactness argument in the additive theory and the polynomial method, *Discrete Math.* **302** (2005) 124–144
[15] Gy. Károlyi, An inverse theorem for the restricted set addition in abelian groups, *J. Algebra* **290** (2005) 557–593
[16] Gy. Károlyi, Cauchy–Davenport theorem in group extensions, *Enseign. Math.* **51** (2005) 239–254

*E-mail address*: `karolyi@cs.elte.hu`