PROD. TYPE: FTP
PP: 1-10 (col.fig.: nil)
DISC5951 MODC+
ED: Smitha Gowda
PAGN: Prakash – SCAN: nil
ARTICLE IN PRESS
Available online at www.sciencedirect.com
SCIENCE DIRECT®
ELSEVIER
Discrete Mathematics ■■■ (■■■■) ■■■–■■■
DISCRETE MATHEMATICS
www.elsevier.com/locate/disc

Contributions to zero-sum problems

S.D. Adhikari[a], Y.G. Chen[b], J.B. Friedlander[c], S.V. Konyagin[d], F. Pappalardi[e]

[a] *Harish-Chandra Research Institute, (Former Mehta Research Institute) Chhatnag Road, Jhusi, Allahabad 211 019, India*
[b] *Department of Mathematics, Nanjing Normal University, Nanjing 210097, PR China*
[c] *Department of Mathematics, University of Toronto, ON, Canada M5S 3G3*
[d] *Department of Mechanics and Mathematics, Moscow State University, Vorobjovy Gory, 119992 Moscow, Russia*
[e] *Dipartimento di Matematica, Università degli Studi Roma Tre, Largo S. L. Murialdo, 1, I-00146 Roma, Italia*

Received 31 July 2003; received in revised form 1 September 2005; accepted 4 November 2005

Abstract

A prototype of zero-sum theorems, the well-known theorem of Erdős, Ginzburg and Ziv says that for any positive integer n, any sequence $a_1, a_2, \ldots, a_{2n-1}$ of $2n-1$ integers has a subsequence of n elements whose sum is 0 modulo n. Appropriate generalizations of the question, especially that for $(\mathbf{Z}/p\mathbf{Z})^d$, generated a lot of research and still have challenging open questions. Here we propose a new generalization of the Erdős–Ginzburg–Ziv theorem and prove it in some basic cases.

Keywords: Zero-sum problems

1. Introduction

The famous Erdős–Ginzburg–Ziv theorem [5] states that, given any sequence of $2n-1$ integers, there are n of them that add up to a multiple of n. Furthermore, a sequence of $2n-2$ integers does not always enjoy this property (consider for example the sequence of $n-1$ zeros and $n-1$ ones). Therefore we have that, if $E(n)$ is the least integer t such that any sequence of t integers contains n integers that add up to a multiple of n, then

$$E(n) = 2n - 1.$$

A number of different proofs of this result are presented in the book [1].

Various generalizations and variations of the above property have been considered in the past (see for example [6,2]). Here we consider a different one that (at least to our knowledge) is new.

If n is a positive integer, we will identify $\mathbb{Z}/n\mathbb{Z}$ with the set of the integers $\{0, \ldots, n-1\}$.

Let $n \in \mathbb{N}$ and assume $A \subseteq \mathbb{Z}/n\mathbb{Z}$. We consider the function $E_A(n)$ defined as the least $t \in \mathbb{N}$ such that for all sequences $(x_1, \ldots, x_t) \in \mathbb{Z}^t$ there exist indices $j_1, \ldots, j_n \in \mathbb{N}$, $1 \leqslant j_1 < \cdots < j_n \leqslant t$, and $(\vartheta_1, \ldots, \vartheta_n) \in A^n$ with

$$\sum_{i=1}^{n} \vartheta_i x_{j_i} \equiv 0 \pmod{n}.$$

E-mail addresses: adhikari@mri.ernet.in (S.D. Adhikari), ygchen@njnu.edu.cn (Y.G. Chen), frdlndr@math.toronto.edu (J.B. Friedlander), konyagin@ok.ru (S.V. Konyagin), pappa@mat.uniroma3.it (F. Pappalardi).

0012-365X/$ - see front matter © 2005 Published by Elsevier B.V.
doi:10.1016/j.disc.2005.11.002

To avoid trivial cases, we will always assume that A does not contain 0 and it is non-empty. It is clear that $E_{\{1\}}(n)=E(n)$ and that

$$E_A(n) \leqslant E(n) = 2n - 1.$$

Further, if we consider the sequence with $n-1$ zeros and one 1, we deduce that

$$E_A(n) \geqslant n + 1.$$

We propose the problem of enumerating $E_A(n)$. Here we consider the case $A = \{1, n-1\} = \{1, -1\}$. We denote $E_A = E_\pm$ in this case, which is perhaps the most basic one aside from the classical Erdős, Ginzburg, Ziv problem.

It is easy to see that

$$E_\pm(n) \geqslant n + \lfloor \log n \rfloor, \tag{1.1}$$

where here and throughout the paper log will mean the base 2 logarithm. Indeed, consider the sequence of integers:

$$(\overbrace{0, 0, \ldots, 0}^{n-1 \text{ times}}, 1, 2, \ldots, 2^r),$$

where r is defined by $2^{r+1} \leqslant n < 2^{r+2}$. Any combination with signs of n integers of the sequence gives rise to a number whose absolute value is $\leqslant 2^{r+1} - 1$ and is not zero by the uniqueness of the binary expansion. Furthermore, the sequence has $n + r = n + \lfloor \log n \rfloor - 1$ elements.

We will prove that

Theorem 1.1. *For any positive integer n, we have*

$$E_\pm(n) = n + \lfloor \log n \rfloor.$$

We will illustrate a number of different approaches to the problem. Whereas the approach of Section 2 leads to the solution in the even case in Theorem 2.2, the approach in Sections 4 and 5 will lead to that in the odd case in Theorem 5.1. In Section 3, we give a number of results for odd prime modulus, which imply Theorem 1.1 in this particular case. Although not really needed due to the other results presented, this argument, which uses the Cauchy–Davenport inequality, seems to us of independent interest.

In the concluding Section 6 we make a few remarks about the problem for other sets A.

2. A conditional result and the even case

It turns out to be easier to deal with sequences where one or more of the elements is in the zero class. We have

Theorem 2.1. *Let $n \in \mathbb{N}$. Assume that $N \geqslant n + \lfloor \log n \rfloor$ is an integer. Given any sequence $(x_1, \ldots, x_N) \in \mathbb{Z}^N$ with at least one multiple of n, there exist $m = N - \lfloor \log n \rfloor$ indices $\{j_1, \ldots, j_m\} \subseteq [N]$ and signs $\varepsilon_1, \ldots, \varepsilon_m \in \{1, -1\}$ such that*

$$\varepsilon_1 x_{j_1} + \cdots + \varepsilon_m x_{j_m} \equiv 0 \pmod{n}.$$

Here, and throughout the paper, $[N]$ will denote the set $\{1, \ldots, N\}$.

We will make use more than once of the following:

Lemma 2.1. *Let $n \in \mathbb{N}$ and $(y_1, \ldots, y_s)$ be a sequence of integers with $s > \log n$. Then there exists a non-empty $J \subseteq [s]$ and $\varepsilon_j \in \{\pm 1\}$ for each $j \in J$ such that*

$$\sum_{j \in J} \varepsilon_j y_j \equiv 0 \pmod{n}.$$

Proof of Lemma 2.1. This is an application of the pigeonhole principle. Consider the sequence of $2^s > n$ integers

$$\left(\sum_{j\in I} y_j\right)_{I\subseteq[s]}$$

that cannot contain distinct integers modulo n. Therefore, there are $J_1, J_2 \subseteq [s]$ with $J_1 \neq J_2$ such that

$$\sum_{j\in J_1} y_j \equiv \sum_{j\in J_2} y_j \pmod n.$$

Set $J = J_1 \cup J_2 \backslash J_1 \cap J_2$ and

$$\begin{cases} \varepsilon_j = 1 & \text{if } j \in J_1, \\ \varepsilon_j = -1 & \text{if } j \in J_2. \end{cases}$$

It is clear that J is non-empty and it has the required property. □

Proof of Theorem 2.1. Let us reorder the sequence in such a way that, modulo n,

$$x_1 = 0, \quad x_2 = x_3, \quad x_4 = x_5, \ldots, x_{2t} = x_{2t+1}$$

and $x_{2t+2}, \ldots, x_N$ are all distinct. Hence $N - 2t - 1 \leqslant n$ and $2t + 1 \geqslant N - n \geqslant \lfloor \log n \rfloor$.

Let $B = \{r_1, \ldots, r_l\} \subseteq \{2t+2, 2t+3, \ldots, N\}$ be maximal with respect to the properties that there exist $\varepsilon_1, \ldots, \varepsilon_l \in \{-1, 1\}$ with

$$\sum_{j=1}^{l} \varepsilon_j x_{r_j} \equiv 0 \pmod n.$$

Now we claim that $l + 2t + 1 \geqslant m$. Indeed, if this were not the case then the set

$$C = \{2t + 2, \ldots, N\}\backslash\{r_1, \ldots, r_l\}$$

would contain $N - 2t - 1 - l > \lfloor \log n \rfloor$ elements. Hence by Lemma 2.1 there would exist a non-empty $B' \subseteq C$ and $\varepsilon_j \in \{\pm 1\}$ for each $j \in B'$ such that

$$\sum_{j\in B'} \varepsilon_j x_j \equiv 0 \pmod n.$$

So we would find that $B \cup B'$ still verifies the property above and we would contradict the maximality of B.

Hence we write $l + 2t + 1 = m + r$ and distinguish the two cases:

If $r = 2r'$ is even then we choose the sequence

$$(x_1, x_{2(r'+1)}, x_{2r'+3}, \ldots, x_{2t}, x_{2t+1}, x_{r_1}, \ldots, x_{r_l})$$

which has m elements and

$$x_1 + \sum_{j=r'+1}^{t} (x_{2j} - x_{2j+1}) + \sum_{j=1}^{l} \varepsilon_j x_{r_j} \equiv 0 \pmod n.$$

If $r = 2r' + 1$ is odd then we leave out x_1 and consider the sequence

$$(x_{2(r'+1)}, x_{2r'+3}, \ldots, x_{2t}, x_{2t+1}, x_{r_1}, \ldots, x_{r_l})$$

which has m elements and also verifies the thesis. □

When the modulus n is even it turns out to be possible to modify the above ideas so as to obtain this case of Theorem 1.1 without any hypothesis. For this we shall use the following:

Lemma 2.2. *Let $n \in \mathbb{N}$ and $(y_1, \ldots, y_s)$ be a sequence of integers with $s > \log n + 1$. Then there exists a non-empty $J \subseteq [s]$ with $|J|$ even and $\varepsilon_j \in \{\pm 1\}$ for each $j \in J$ such that*

$$\sum_{j \in J} \varepsilon_j y_j \equiv 0 \pmod{n}.$$

Proof. Just as in the proof of Lemma 2.1 above, we apply pigeonhole on the $2^{s-1} > n$ integers

$$\left(\sum_{j \in I} y_j \right)_{\substack{I \subseteq [s] \\ |I| \text{even}}}. \qquad \square$$

The following theorem takes care of the case 'n is even' in Theorem 1.1.

Theorem 2.2. *Let $n \in \mathbb{N}$ be even. Consider the integer $N = n + \lfloor \log n \rfloor$. Then, given any sequence $(x_1, \ldots, x_N) \in \mathbb{Z}^N$, there exist n indices $\{j_1, \ldots, j_n\} \subseteq [N]$ and signs $\varepsilon_1, \ldots, \varepsilon_n \in \{1, -1\}$ such that*

$$\varepsilon_1 x_{j_1} + \cdots + \varepsilon_n x_{j_n} \equiv 0 \pmod{n}.$$

Proof. Let us reorder the sequence in such a way that, modulo n,

$$x_1 = x_2, \quad x_3 = x_4, \ldots, x_{2t-1} = x_{2t}$$

and $x_{2t+1}, \ldots, x_N$ are all distinct. Hence $N - 2t \leqslant n$ and $2t \geqslant N - n = \lfloor \log n \rfloor$. Let $B = \{r_1, \ldots, r_l\} \subseteq \{2t + 1, 2t + 2, \ldots, N\}$, with $l = |B|$ even, be maximal with respect to the properties that there exist $\varepsilon_1, \ldots, \varepsilon_l \in \{-1, 1\}$ with

$$\sum_{j=1}^{l} \varepsilon_j x_{r_j} \equiv 0 \pmod{n}.$$

Now we claim that $l + 2t \geqslant n$. Indeed, if this were not the case then we have $l + 2t \leqslant n - 2$ since the numbers $l + 2t$ and n are both even, and the set

$$C = \{2t + 1, \ldots, N\} \backslash \{r_1, \ldots, r_l\}$$

would contain $N - 2t - l \geqslant \lfloor \log n \rfloor + 2 > \log n + 1$ elements. Hence by Lemma 2.2 there would exist a non-empty $B' \subseteq C$ with $|B'|$ even and $\varepsilon_j \in \{\pm 1\}$ for each $j \in B'$ such that

$$\sum_{j \in B'} \varepsilon_j x_j \equiv 0 \pmod{n}.$$

So we would find that $B \cup B'$ still verifies the property above and we would contradict the maximality of B.

Since both l and n are even, from $l + 2t = n + r$, we see that r is even. If $r = 2r'$ then we choose the sequence

$$(x_{2r'+1}, x_{2r'+2}, \ldots, x_{2t}, x_{r_1}, \ldots, x_{r_l})$$

which has n elements and

$$\sum_{j=r'+1}^{t} (x_{2j} - x_{2j-1}) + \sum_{j=1}^{l} \varepsilon_j x_{r_j} \equiv 0 \pmod{n}. \qquad \square$$

3. The case $n = p$ with p an odd prime and the Cauchy–Davenport inequality

We will state and prove a couple of results that have their own interest.

Lemma 3.1. *Let p be an odd prime. If $N \geqslant p-1$ is an integer and $(x_1, \ldots, x_N) \in \mathbb{Z}^N$ is any sequence of integers not divisible by p, then for every $b \in \mathbb{Z}$ there exist signs $\varepsilon_1, \ldots, \varepsilon_N \in \{1, -1\}$ such that*

$$\varepsilon_1 x_1 + \cdots + \varepsilon_N x_N \equiv b \pmod{p}.$$

The above is a direct consequence of the famous:

Lemma 3.2 (*Cauchy–Davenport inequality*). *Let A and B be two non-empty subsets of $\mathbb{Z}/p\mathbb{Z}$. Then*

$$|A+B| \geqslant \min\{p, |A|+|B|-1\},$$

where

$$A+B = \{x \in \mathbb{Z}/p\mathbb{Z} \mid x \equiv a+b \pmod{p},\ a \in A, b \in B\}$$

and $|K|$ denotes the cardinality of the subset K of $\mathbb{Z}/p\mathbb{Z}$.

This was first proved by Cauchy [3] in 1813 and later rediscovered by Davenport [4] in 1947. By iterating the Cauchy–Davenport inequality we immediately obtain:

Lemma 3.3. *Let $A_1, A_2, \ldots, A_h$ be non-empty subsets of $\mathbb{Z}/p\mathbb{Z}$. Then*

$$|A_1 + A_2 + \cdots + A_h| \geqslant \min\left\{p, \sum_{i=1}^{h} |A_i| - h + 1\right\}.$$

By choosing $A_i = \{x_i, -x_i\}$, we deduce that

$$|\{x_1, -x_1\} + \{x_2, -x_2\} + \cdots + \{x_N, -x_N\}| \geqslant p$$

which immediately implies Lemma 3.1.

The statements of Lemma 3.1 and Theorem 2.1 imply the result of Theorem 1.1 when the modulus p is an odd prime since the first statement deals with the case when none of the elements of the sequence are 0 modulo p and the second statement deals with the case when the sequence contains an element which is 0 modulo p.

4. Complete sequences of integers

We are not aware whether the notion in the following definition has already appeared in the literature. However, it appears natural in this context.

Definition. Let $\underline{x} = (x_1, \ldots, x_N) \in \mathbb{Z}^N$. We say the sequence $\underline{x}$ is *complete with respect to a positive integer m* if for every positive $d \mid m$ we have

$$|\{j \in [N] \mid x_j \not\equiv 0 \pmod{d}\}| \geqslant d-1. \tag{4.1}$$

A complete sequence of integers with respect to a prime p is a sequence that contains $p-1$ elements which are not divisible by p.

Let us collect some properties of complete sequences:

Lemma 4.1. *If $(x_1, \ldots, x_N) \in \mathbb{Z}^N$ is complete with respect to m and $N \geqslant m$ then there is $j_0 \in \mathbb{N}$, $1 \leqslant j_0 \leqslant N$, such that*

$$(x_1, \ldots, x_{j_0-1}, x_{j_0+1}, \ldots, x_N) \in \mathbb{Z}^{N-1}$$

is complete with respect to m.

Proof. Let $d_1, d_2, \ldots, d_s$ be the divisors d of m that satisfy

$$|\{j \in [N] \mid x_j \not\equiv 0 \pmod{d}\}| = d - 1.$$

Assume also that $m \geqslant d_1 > d_2 > \cdots > d_s$, set $D_k = \operatorname{lcm}[d_1, \ldots, d_k]$ and

$$U_k = \{j \in [N] \mid x_j \not\equiv 0 \pmod{d_k}\}.$$

Our goal is to show that

$$|U_1 \cup \cdots \cup U_s| < m$$

so that we can choose $j_0 \in [N] \backslash U_1 \cup \cdots \cup U_s$ and the sequence $(x_1, \ldots, x_{j_0-1}, x_{j_0+1}, \ldots, x_N)$ will still verify the hypothesis of completeness.

Note that

$$U_1 \cup \cdots \cup U_k = \{j \in [N] \mid x_j \not\equiv 0 \pmod{D_k}\}$$

and that $U_1 \cup \cdots \cup U_k = U_1 \cup \cdots \cup U_{k-1}$ if $D_k = D_{k-1}$. Thus,

$$U_1 \cup \cdots \cup U_s = U_1 \cup \bigcup_{D_k > D_{k-1}} U_k.$$

Now, for those k participating in this formula we have $D_k > D_{k-1}$ and so $D_k = [D_{k-1}, d_k] \geqslant 2D_{k-1}$. This implies, for these $k > 1$, that

$$D_k - D_{k-1} \geqslant D_{k-1} \geqslant d_{k-1} > d_k - 1,$$

while $D_1 > d_1 - 1$. We deduce that

$$\begin{aligned} |U_1 \cup \cdots \cup U_s| &\leqslant |U_1| + \sum_{D_k > D_{k-1}} |U_k| \\ &= d_1 - 1 + \sum_{D_k > D_{k-1}} (d_k - 1) \\ &< D_1 + \sum_{k=2}^{s} (D_k - D_{k-1}) \\ &= D_s \leqslant m. \end{aligned}$$

This completes the proof. □

Lemma 4.2. *If $(x_1, \ldots, x_N) \in \mathbb{Z}^N$ is complete with respect to m then there exist indices $\{j_1, \ldots, j_{m-1}\} \subseteq [N]$ such that the sequence $(x_{j_1}, \ldots, x_{j_{m-1}}) \in \mathbb{Z}^{m-1}$ is complete with respect to m.*

Proof. From the definition of complete sequence in (4.1) we deduce that $N \geqslant m - 1$. By applying Lemma 4.1 several times we can eliminate elements from the sequence until we arrive at exactly $m - 1$ elements. □

Theorem 4.1. *If $(x_1, \ldots, x_N) \in \mathbb{Z}^N$ is complete with respect to m, then for every integer b there is a choice of coefficients $\varsigma_1, \ldots, \varsigma_N \in \{0, 1\}$ such that*

$$\sum_{j=1}^{N} \varsigma_j x_j \equiv b \pmod{m}.$$

Proof. We prove the theorem by induction on m. The case $m = 1$ is clear. Now we assume that $k \geqslant 2$ and the theorem is true for $m < k$. Suppose that the sequence $x_1, x_2, \ldots, x_N$ of N integers is complete with respect to k. Without loss of generality, we may assume that $k \nmid x_1$. For any integer a, let $\overline{a}$ be the residue class of $a \bmod k$. For any set A of integers, let

$$\overline{A} = \{\overline{a} \mid a \in A\}.$$

Let $A_1 = \{0, x_1\}$ and $i_1 = 1$. Then $|\overline{A_1}| = 2$. Now, if possible, we choose an index $i_2 \neq i_1$ such that

$$\overline{A_1} + \{0, \overline{x_{i_2}}\} \neq \overline{A_1}.$$

If such an i_2 exists, then let $A_2 = A_1 + \{0, x_{i_2}\}$. We continue this procedure and suppose that the procedure stops at A_t. Noting that

$$A_1 \subset A_2 \subset \cdots \subset A_t,$$

we have

$$|\overline{A_t}| \geqslant |\overline{A_{t-1}}| + 1 \geqslant \cdots \geqslant t + 1. \tag{4.2}$$

To complete the proof, it is enough to prove that $|\overline{A_t}| \geqslant k$. By (4.2), we may assume that $t \leqslant k - 2$. Without loss of generality, we may assume that $i_j = j \ (j = 1, 2, \ldots, t)$.

Since

$$|\{j \mid x_j \not\equiv 0 \pmod k\}| \geqslant k - 1,$$

we have $N \geqslant k - 1$. Also, rearranging the remaining elements if necessary, we can assume that $k \nmid x_{t+1}$.

By the assumption on A_t, for all $t + 1 \leqslant j \leqslant N$, we have

$$\overline{A_t} + \{0, \overline{x_j}\} = \overline{A_t}. \tag{4.3}$$

Let H be the subgroup of $\mathbb{Z}_k$ generated by $\overline{x_{t+1}}$. By (4.3), we have

$$\overline{A_t} + H = \overline{A_t}.$$

Thus, $\overline{A_t}$ is the union of some cosets of H. Let

$$\overline{A_t} = \bigcup_{i=1}^{s} (b_i + H), \tag{4.4}$$

where $b_i - b_j \notin H$ for all $i \neq j$. Then $|\overline{A_t}| = s|H|$. Let $k_1 = (x_{t+1}, k)$. Then, since $k \nmid x_{t+1}$ we have $k_1 < k$ and the sequence $x_1, x_2, \ldots, x_N$ is complete with respect to the positive integer k_1. By the induction hypothesis, we see that, for every integer b, there is a choice of coefficients $\zeta_1, \ldots, \zeta_N \in \{0, 1\}$ such that

$$\sum_{j=1}^{N} \zeta_j x_j \equiv b \pmod{k_1}. \tag{4.5}$$

By (4.3) we have

$$\left\{ \sum_{j=1}^{N} \zeta_j x_j \pmod k \mid \zeta_i = 0, 1, i = 1, 2, \ldots, N \right\} = \overline{A_t}.$$

Thus, by $k_1 | k$, $k_1 | x_{t+1}$ and (4.4), we have

$$\left\{ \sum_{j=1}^{N} \zeta_j x_j \pmod{k_1} \mid \zeta_i = 0, 1 \right\} = \{b_1 \pmod{k_1}, \ldots, b_s \pmod{k_1}\}.$$

Hence, by (4.5) we have $s \geqslant k_1$. Noting that

$$|H| x_{t+1} \equiv 0 \pmod k,$$

it follows that

$$|H| \equiv 0 \left(\mathrm{mod}\, \frac{k}{k_1}\right).$$

Since $|H| \geqslant 1$ we have $|H| \geqslant k/k_1$. Therefore,

$$|\overline{A_t}| = s|H| \geqslant k.$$

This completes the proof. □

The above theorem deals with linear combinations of the x_j having coefficients 0 and 1 whereas we are really interested in combinations with coefficients ± 1. The following result allows us to move from one to the other, but only in the case where the modulus is odd.

Corollary 4.1. *If m is odd and $(x_1, \ldots, x_N)$ is complete with respect to m, then for every integer $b \in \mathbb{Z}$ there is a choice of coefficients $\varepsilon_1, \ldots, \varepsilon_N \in \{\pm 1\}$ such that*

$$\sum_{j=1}^{N} \varepsilon_j x_j \equiv b \ (\mathrm{mod}\, m).$$

Proof. Given any integer $b \in \mathbb{Z}$, Theorem 4.1 implies that there exist $\varsigma_1, \ldots, \varsigma_N \in \{0, 1\}$ such that

$$\frac{b}{2} + \frac{x_1 + \cdots + x_N}{2} \equiv \sum_{j=1}^{N} \varsigma_j x_j \ (\mathrm{mod}\, m),$$

which is meaningful since m is odd. Consider the identity

$$\varsigma_1 x_1 + \cdots + \varsigma_N x_N = \frac{x_1 + \cdots + x_N}{2} + \frac{1}{2} \sum_{j=1}^{N} (2\varsigma_j - 1) x_j.$$

Since $\varepsilon_j = 2\varsigma_j - 1 \in \{\pm 1\}$, we obtain the claim. □

5. Proof of Theorem 1.1 in the case 'n is odd'

The result in the 'n is odd' case is a direct consequence of (1.1) and the following statement:

Theorem 5.1. *Assume that $m \in \mathbb{N}$ is odd. If $N \geqslant m + \lfloor \log m \rfloor$ and $\underline{x} = (x_1, \ldots, x_N) \in \mathbb{Z}^N$, then there exists $I_0 = \{j_1, \ldots, j_t\} \subseteq [N]$ with $|I_0| = t = N - \lfloor \log m \rfloor$ and some choice of coefficients $\varepsilon_1, \ldots, \varepsilon_t \in \{\pm 1\}$, so that*

$$\sum_{i=1}^{t} \varepsilon_i x_{j_i} \equiv 0 \ (\mathrm{mod}\, m).$$

Proof. If $\underline{x}$ is complete with respect to m, then, by Lemma 4.2, there are $m - 1$ indices $j_1, \ldots, j_{m-1} \in [N]$ such that $(x_{j_1}, \ldots, x_{j_{m-1}})$ is still complete with respect to m.

Choose arbitrarily indices $j_m, \ldots, j_t \in [N] \setminus \{j_1, \ldots, j_{m-1}\}$. Then $(x_{j_1}, \ldots, x_{j_t})$ is also complete with respect to m, and the assertion follows from Corollary 4.1.

Next suppose that $\underline{x}$ is not complete with respect to m. Then there exists a divisor d of m such that

$$|\{j \in [N] : x_j \not\equiv 0 \ (\mathrm{mod}\, d)\}| < d - 1.$$

Let D be the maximal divisor of m possessing this property. We claim that if $f \mid m$ is such that $D \mid f$ then

$$|\{j \in [N] \mid x_j \equiv 0 \ (\mathrm{mod}\, D),\ x_j \not\equiv 0 \ (\mathrm{mod}\, f)\}| \geqslant \frac{f}{D} - 1. \tag{5.1}$$

Indeed, the claim is trivial if $f = D$. If $f > D$ and (5.1) does not hold then

$$\begin{aligned}|\{j \in [N] \mid x_j \not\equiv 0 \pmod f\}| &= |\{j \in [N] \mid x_j \not\equiv 0 \pmod D\}| + |\{j \in [N] \mid x_j \\ &\equiv 0 \pmod D,\ x_j \not\equiv 0 \pmod f\}| \\ &< D + f/D - 2 \leqslant f - 1.\end{aligned}$$

This would contradict the maximality of D.

Denote

$$I_1 = \{j \in [N] \mid x_j \not\equiv 0 \pmod D\},$$
$$I_2 = \{j \in [N] \mid x_j \equiv 0 \pmod D\}.$$

Let I_3 be a maximal subset of I_1 such that for some choice of coefficients $\varepsilon'_j \in \{\pm 1\}$, $j \in I_3$, we have

$$\sum_{j \in I_3} \varepsilon'_j x_j \equiv 0 \pmod D.$$

By Lemma 2.1 we know that

$$|I_1| - |I_3| \leqslant \lfloor \log D \rfloor. \tag{5.2}$$

Let $k = t - |I_3|$. By (5.2) we have

$$k \leqslant N - |I_1| = |I_2|.$$

On the other hand,

$$k \geqslant m - |I_3| \geqslant m - |I_1| > m - D + 1 \geqslant m/D.$$

Therefore,

$$|I_2| \geqslant k \geqslant \frac{m}{D}. \tag{5.3}$$

Now set

$$\tilde{x} = \left(\frac{x_j}{D}\right)_{j \in I_2}.$$

By (5.1), $\tilde{x}$ is complete with respect to m/D.

Lemma 4.2 implies that there exists $I' = \{j_1, \ldots, j_{m/D-1}\} \subseteq I_2$, such that

$$\left(\frac{x_j}{D}\right)_{j \in I'} = \left(\frac{x_{j_1}}{D}, \ldots, \frac{x_{j_{m/D-1}}}{D}\right)$$

is complete with respect to m/D.

By (5.3), we can choose a set I'_1 such that $I' \subseteq I'_1 \subseteq I_2$ and $|I'_1| = k$. Clearly

$$\left(\frac{x_j}{D}\right)_{j \in I'_1}$$

is also complete with respect to m/D.

Therefore, Corollary 4.1 implies that we can choose coefficients $\varepsilon''_j \in \{\pm 1\}$, $j \in I'_1$, such that

$$\sum_{j \in I'_1} \varepsilon''_j \frac{x_j}{D} \equiv -\frac{1}{D} \sum_{j \in I_3} \varepsilon'_j x_j \pmod{\frac{m}{D}}.$$

To complete the proof of Theorem 5.1, it suffices to set

$$I_0 = I_3 \cup I'_1$$

and choose

$$\varepsilon_j = \begin{cases} \varepsilon''_j & \text{if } j \in I'_1, \\ \varepsilon'_j & \text{if } j \in I_3, \end{cases}$$

and this concludes the proof. □

6. Concluding remarks

An interesting choice for the set A is that of $A = (\mathbb{Z}/n\mathbb{Z})^*$, namely, $A = \{a : (a, n) = 1\}$. It is easy to see that $E_A(n) \geqslant n + \Omega(n)$ where as usual $\Omega(n)$ denotes the number of prime factors of n, multiplicity included. Indeed, write $n = p_1, \ldots, p_s$ as product of $s = \Omega(n)$ not necessarily distinct primes. Consider the sequence consisting of $n - 1$ zeros and $\{1, p_1, p_1 p_2, \ldots, p_1 p_2 \cdots p_{s-1}\}$, giving the lower bound. Perhaps, one can show that equality holds so that $E_A(n) = n + \Omega(n)$.

An easier case is $A = (\mathbb{Z}/n\mathbb{Z})\backslash\{0\}$. As mentioned in the introduction, we always have $E_A(n) \geqslant n + 1$ and, for this particular choice of A (the maximal A, since we always exclude 0), this lower bound is achieved.

Theorem 6.1. *Let* $A = (\mathbb{Z}/n\mathbb{Z})\backslash\{0\}$. *Then* $E_A(n) = n + 1$.

Proof. We can assume that $n > 2$. We have the following observations.

Fact 1: If $r \geqslant 2$ and $(x_j, n) = 1$ for $j = 1, \ldots, r$ then there are coefficients $\vartheta_j \in A$ such that

$$\sum_{j=1}^{r} \vartheta_j x_j \equiv 0 \pmod{n}.$$

Indeed, without loss of generality, we can consider $x_j = 1$ for $j = 1, \ldots, r$. If r is even we take $\vartheta_j = (-1)^j$, otherwise we replace ϑ_2 by 2.

Fact 2: If $(x_j, n) > 1$ then there is $\vartheta_j \in A$ such that

$$\vartheta_j x_j \equiv 0 \pmod{n}.$$

Let $(x_1, \ldots, x_t) \in \mathbb{Z}^t$ where $t \geqslant n+1$. By re-ordering we can assume that $(x_j, n) = 1$ for $j = 1, \ldots, r$ and $(x_j, n) > 1$ for $j > r$. If $r \geqslant 2$, we take $i_j = j$ for $j = 1, \ldots, n$ and use Facts 1 and 2 while if $r \leqslant 1$, we take $i_j = r + j$ for $j = 1, \ldots, n$ and use Fact 2. □

It might be interesting to characterize any other sets A for which $E_A(n) = n + 1$ or even those for which $E_A(n) = n + j$ for specific small values of j.

Acknowledgements

Part of this project was realised when the first, the third and the fourth authors were visiting the Dipartimento di Matematica of the Università Roma Tre in the years 2002 and 2003. The second author was supported by the National Natural Science Foundation of China, Grant no. 10471064. The third author was supported in part by NSERC and by a Killam Research Fellowship. The last two authors were supported in part by G.N.S.A.G.A. of INDAM and by the INTAS Grant 03-51-5070.

References

[1] S.D. Adhikari, Aspects of Combinatorics and Combinatorial Number Theory, Narosa, New Delhi, 2002.
[2] Y. Caro, Zero-sum problems–a survey, Discrete Math. 152 (1996) 93–113.
[3] A.L. Cauchy, Recherches sur les nombres, J. Ecôle Polytech. 9 (1813) 99–123.
[4] H. Davenport, On the addition of residue classes, J. London Math. Soc. 22 (1947) 100–101.
[5] P. Erdős, A. Ginzburg, A. Ziv, Theorem in the additive number theory, Bull. Res. Council Israel 10 (F) (1961) 41–43.
[6] R. Thangadurai, Non-canonical extensions of Erdős–Ginzburg–Ziv theorem, Integers 2 (2002) 1–14 (#A07).