ACTA ARITHMETICA
LXXXIX.4 (1999)

On a variant of the Erdős–Ginzburg–Ziv problem

by

L. Gallardo (Brest), G. Grekos (St. Etienne)
and J. Pihko (Helsinki)

1. The problem. P. Erdős, A. Ginzburg and A. Ziv [EGZ] proved in 1961 that from any finite sequence of $2n-1$ integers (not necessarily distinct) one can extract a subsequence of length n such that the sum of its n elements is congruent to zero modulo n.

The sequence

$$(0,\ldots,0,1,\ldots,1), \tag{1}$$

formed by $n-1$ zeros and $n-1$ ones, has length $2n-2$ and we cannot extract from it a subsequence of length n and of sum congruent to 0 modulo n. Thus the value $2n-1$ is best possible.

Since 1961, some different proofs have been given to the theorem, there were attempts to generalize it to various directions, and connections with graph theory were discovered. The reader may find references in [AD], [BL] and [C].

Here we are concerned with the following development due to A. Bialostocki, P. Dierker and M. Lotspeich ([BD], [BL]). In the Erdős–Ginzburg–Ziv theorem, in order to show that $2n-1$ is best possible, one has to find a sequence of length $2n-2$ failing the required property, that is, such that every subsequence of length n has sum incongruent to 0 modulo n. Such a sequence is the sequence (1) formed by integers belonging to only *two* classes modulo n.

A. Bialostocki and P. Dierker [BD] proved in 1992 that this is the only case where this happens. Precisely, they proved that "if $A=(a_1,\ldots,a_{2n-2})$ is a sequence of $2n-2$ integers and there are no indices $i_1,\ldots,i_n$ belonging to $\{1,\ldots,2n-2\}$ such that

$$a_{i_1}+\ldots+a_{i_n}\equiv 0 \pmod{n}, \tag{2}$$

then there are two residue classes modulo n such that $n-1$ of the a_i's belong

1991 *Mathematics Subject Classification*: Primary 11B50.

to one of the classes and the remaining $n-1$ of the a_i's belong to the other class".

In order to study the relation between the number of classes present in a sequence $A=(a_1,\dots,a_g)$ and the possibility to have a relation like (2), A. Bialostocki and M. Lotspeich [BL] introduced the following function.

Definition 1. Let n,k be positive integers, $1\le k\le n$. We define $f(n,k)$ to be the least integer g for which the following holds: If $A=(a_1,\dots,a_g)$ is a sequence of integers of length g such that the number of the a_i's that are distinct modulo n is equal to k, then there are n indices $i_1,\dots,i_n$ belonging to $\{1,\dots,g\}$ such that $a_{i_1}+\dots+a_{i_n}\equiv 0 \pmod n$.

This definition appears on page 99 of [BL]. There, the function f is denoted by g^*. Of course, the Erdős–Ginzburg–Ziv theorem implies that $f(n,k)$ exists and is not greater than $2n-1$. The example (1) shows that $f(n,2)=2n-1$ and the above mentioned theorem of Bialostocki and Dierker [BD] gives

$$f(n,k)\le 2n-2 \quad \text{for } 2<k\le n.$$

Trivially, we have $f(n,k)\ge n$ and $f(n,1)=n$ for all n and k.

Bialostocki and Lotspeich [BL] studied $f(n,k)$ for $k=3$ and $k=4$. In this paper we determine $f(n,k)$ for k greater than $1+n/2$.

2. Modular version and results. For given n, we can formulate the problem and work in the context of $\mathbb{Z}_n$, the cyclic group of residue classes modulo n. Let us define $f(n,k)$ in the following equivalent way.

Definition 1′. Let n,k be positive integers, $1\le k\le n$. Denote by $f(n,k)$ the least integer g for which the following holds: If $A=(a_1,\dots,a_g)$ is a sequence of elements of $\mathbb{Z}_n$ of length g such that the number of distinct a_i's is equal to k, then there are n indices $i_1,\dots,i_n$ belonging to $\{1,\dots,g\}$ such that $a_{i_1}+\dots+a_{i_n}=0$.

Remark. The order of elements in A has no influence on the existence of a subsequence of n terms having zero sum.

Notation. A sequence like $A=(0,0,1,1,1,2,3,5)$ will be denoted also by $A=0^2,1^3,2,3,5$. The sequence in (1) will be written as $0^{n-1},1^{n-1}$. The elements of $\mathbb{Z}_n$ will be denoted by $0,1,\dots,n-1$.

In the next section we prove the following facts.

Proposition. *Let n be a positive integer. Then $f(n,n)=n$ if n is odd and $f(n,n)=n+1$ if n is even.*

Theorem 1. *Let n,k be positive integers, $n\ge 5$, $1+n/2<k\le n-1$. Then*

$$f(n,k)\le n+2. \tag{3}$$

Theorem 2. *Let n, k be positive integers, $n \ge 4$, $1 + n/2 \le k \le n - 1$. Then*

$$f(n,k) \ge n + 2. \tag{4}$$

As a direct consequence, we obtain the following equality.

Corollary. *If $n \ge 5$ and $1 + n/2 < k \le n - 1$, then $f(n,k) = n + 2$.*

Here are also some numerical results. They are obtained either from the Proposition or from the Corollary or by [BL].

$f(1,1) = 1$,
$f(2,1) = 2$, $f(2,2) = 3$,
$f(3,1) = 3$, $f(3,2) = 5$, $f(3,3) = 3$,
$f(4,1) = 4$, $f(4,2) = 7$, $f(4,3) = 6$, $f(4,4) = 5$,
$f(5,1) = 5$, $f(5,2) = 9$, $f(5,3) = 8$, $f(5,4) = 7$, $f(5,5) = 5$,
$f(6,1) = 6$, $f(6,2) = 11$, $f(6,3) = 10$, $f(6,4) = 9$, $f(6,5) = 8$, $f(6,6) = 7$,
$f(7,1) = 7$, $f(7,2) = 13$, $f(7,3) = 12$, $f(7,4) = 11$, $f(7,5) = 9$, $f(7,6) = 9$,
$f(7,7) = 7$.

3. Proofs.

The following lemma, saying that the desired property is invariant under translation, will be very useful.

Lemma 1. *Let $b, a_1, \ldots, a_g$ be elements of $\mathbb{Z}_n$. Put $A = (a_1, \ldots, a_g)$ and $A + b = (a_1 + b, \ldots, a_g + b)$. Then one can extract from A a subsequence of length n and of sum 0 if and only if one can do it for the sequence $A + b$.*

Proof. This is true because $nb = 0$ (in $\mathbb{Z}_n$). ∎

Proof of the Proposition

Case 1: *n is odd.* Any sequence $A = (a_1, \ldots, a_g)$, $g \ge n$, having n distinct a_i's belonging to $\mathbb{Z}_n$ contains at least once each of the elements $0, 1, \ldots, n-1$, so that one can always extract from A a subsequence with sum $0 + 1 + \ldots + (n-1) = n(n-1)/2$. As n is odd, $(n-1)/2$ is an integer and so $n(n-1)/2 \equiv 0 \pmod{n}$.

Case 2: *n is even.* Let $n = 2m$. Firstly, observe that $f(n,n) > n$ because the sequence $(0, 1, \ldots, n-1)$ has n distinct terms belonging to $\mathbb{Z}_n$ and its sum is $0 + 1 + \ldots + (n-1) = n(n-1)/2 = m(n-1)$, not congruent to 0 modulo $n = 2m$. Now any sequence $A = (a_1, \ldots, a_{n+1})$ with n distinct terms must contain twice an element of $\mathbb{Z}_n$ and once the other elements. As order is not important and in view of Lemma 1, we can suppose, without loss of generality, that

$$A = (0, 0, 1, 2, \ldots, m-1, m, m+1, \ldots, 2m-1).$$

Now one can extract from A the desired subsequence: since $i + (2m - i) = 2m$ for $i = 1, \ldots, m-1$, we have

$$0+0+1+\ldots+(m-1)+(m+1)+\ldots+(2m-1) = 2m(m-1) \equiv 0 \pmod{n},$$

the above sum having $2+2(m-1) = 2m$ terms. ■

In order to prove Theorem 1 we need Lemma 3. In the proof of Lemma 3 we use the following lemma, the proof of which is an easy exercise.

LEMMA 2. *In $\mathbb{Z}_n$ the equation $t+t=0$ has a single solution* (*the solution $t=0$*) *if and only if n is odd*; *the above equation has two solutions* ($t=0$ *and $t=n/2$*) *if and only if n is even.*

LEMMA 3. *Let A be a non-empty subset of $\mathbb{Z}_n$. Denote by $|A|$ its cardinality. If $|A| > n/2+1$, then each element of $\mathbb{Z}_n$ is the sum of two distinct elements of A.*

Proof. Let $x \in \mathbb{Z}_n$. We prove that x is the sum of two distinct elements of A. Let $k = |A|$ and $A = \{a_1, \ldots, a_k\}$. Consider the set $B = x - A = \{x-a_1, \ldots, x-a_k\} \subset \mathbb{Z}_n$. Its cardinality is also k, because $x - a_i = x - a_j$ if and only if $a_i = a_j$. We have

$$n = |\mathbb{Z}_n| \geq |A \cup B| = |A| + |B| - |A \cap B| = 2k - |A \cap B|.$$

This yields

$$|A \cap B| \geq 2k - n > 2(n/2+1) - n = 2,$$

that is, $|A \cap B| \geq 3$. It follows that there are three (distinct) elements a, b, c of A such that

$$a = x - a', \quad b = x - b', \quad c = x - c'$$

where a', b', c' belong to A. It remains to show that at least one of the relations $a \neq a'$, $b \neq b'$, or $c \neq c'$ is valid. We suppose the contrary: $a = a'$, $b = b'$ and $c = c'$. This gives $x = a + a = b + b = c + c$, which implies

$$(a-b)+(a-b)=0, \quad (a-c)+(a-c)=0, \quad (b-c)+(b-c)=0.$$

But, by Lemma 2, the equation $t+t=0$ has at most one non-trivial (that is, $\neq 0$) solution. So $a-b = a-c = n/2$ in $\mathbb{Z}_n$, and hence $b = c$. But this is not true. ■

Proof of Theorem 1. Let $A = (a_1, \ldots, a_{n+2})$ be a sequence of integers belonging to exactly k classes modulo n. We consider the sum of its terms in $\mathbb{Z}_n$

$$a_1 + \ldots + a_{n+2} = g. \tag{5}$$

By Lemma 3, the element g of $\mathbb{Z}_n$ is the sum of two distinct elements x_1, x_2 of A: $g = x_1 + x_2$. We remove x_1, x_2 from A. This gives us an n-term subsequence of A with zero sum, because of (5). ■

Proof of Theorem 2. We must prove that $f(n,k) > n+1$. To do this, we construct a sequence $E = (e_1, \ldots, e_{n+1})$ containing exactly k distinct elements of $\mathbb{Z}_n$, such that every n-term subsequence of E has non-zero sum. To find the sequence E, we consider the sequence

$$E^* = 0^a, 1^b, 2, 3, \ldots, k$$

with $b \in \{1, 2\}$. From E^* we shall remove an element $x \in \{2, 3, \ldots, k\}$. We must have $a + b + k - 2 = n + 1$, that is,

$$a + b + k = n + 3. \tag{6}$$

Note that (6) implies

$$a = n + 3 - b - k \geq n + 3 - 2 - (n - 1) = 2 > 0,$$

so that 0 will really appear in $E = E^* \setminus \{x\}$. Denote by s the sum of elements of E^*:

$$s = b + 2 + 3 + \ldots + k = b - 1 + k(k + 1)/2.$$

We shall choose $x \in \{2, 3, \ldots, k\}$ and $b \in \{1, 2\}$ such that

$$2x = s = b - 1 + k(k + 1)/2. \tag{7}$$

If x goes through $2, 3, \ldots, k$, then $2x$ goes through $4, 6, \ldots, 2k$, and for $b = 1$ or 2, $2x - b$ takes the values

$$2, 3, 4, 5, \ldots, 2k - 2, 2k - 1. \tag{8}$$

As $k \geq 1 + n/2$, we have $2k - 1 \geq 2(1 + n/2) - 1 = n + 1$. That is, numbers in (8) form a complete set of elements of $\mathbb{Z}_n$. Thus $-1 + k(k + 1)/2$ is one among the numbers in (8), that is, there is at least one choice of

$$(b, x) \in \{1, 2\} \times \{2, 3, \ldots, k\}$$

satisfying (7). Now denote by E the sequence resulting from E^* after removing x. Let y be the sum of elements of E. Of course $y + x = s$. But also $2x = s$. It follows that $y = x$. The sequence E has $n+1$ elements. It remains to show that every n-term subsequence extracted from E has non-zero sum. This is true because if we remove from E an element

$$t \in \{0, 1, 2, \ldots, x - 1, x + 1, \ldots, k\},$$

then the remaining terms have sum $y - t = x - t \neq 0$. ∎

Acknowledgements. During the conference "Théorie Analytique des Nombres (8–12 septembre 1997)" at Luminy, France, in the problem session, François Dress suggested studying the function $f(n, k)$. We firstly determined $f(n, n)$ and $f(n, n-1)$. Then, searching in the literature, we found the paper [BL] by A. Bialostocki and M. Lotspeich. On page 99 the authors attribute to N. Alon the observation that "it is not difficult to prove that $f(n, k) \leq n + 2$ if $k > n/2$". As $f(6, 4) = 9$, this is not true. The phrase "if $A \subset \mathbb{Z}_n$ and $|A| > n/2$, then $A + A = \mathbb{Z}_n$" is true but, in our opinion, not sufficient; it should be replaced by our Lemma 3. Theorem 1 of our paper is the outcome of our result for $k = n-1$, after having taken into consideration and arranged Alon's idea, as reported in [BL]. (See also [C], p. 96.)

This work was done while the third named author was Visiting Professor at the University of Saint-Etienne, France, and the first named author had a short stay in Saint-Etienne, sponsored by the "Groupement de Recherche: Théorie Analytique des Nombres (responsible: Jean-Marc Deshouillers), C.N.R.S., France".

References

[AD] N. Alon and M. Dubiner, *Zero-sum sets of prescribed size*, in: Combinatorics, Paul Erdős is Eighty, Volume 1, Bolyai Soc. Math. Stud., János Bolyai Math. Soc., Budapest,1993, 33–50.

[BD] A. Bialostocki and P. Dierker, *On the Erdős–Ginzburg–Ziv theorem and the Ramsey numbers for stars and matchings*, Discrete Math. 110 (1992), 1–8.

[BL] A. Bialostocki and M. Lotspeich, *Some developments of the Erdős–Ginzburg–Ziv theorem, I*, in: Sets, Graphs and Numbers (Budapest, 1991), Colloq. Math. Soc. János Bolyai 60, North-Holland, 1992, 97–117.

[C] Y. Caro, *Zero-sum problems—A survey*, Discrete Math. 152 (1996), 93–113.

[EGZ] P. Erdős, A. Ginzburg and A. Ziv, *Theorem in the additive number theory*, Bull. Res. Council Israel Sect. F Math. Phys. 10 (1961–1962), 41–43.

Addendum (16.11.1998) **and acknowledgement of priority.** After having submitted this paper, the first named author found the article

[B] W. Brakemeier, *Eine Anzahlformel von Zahlen modulo n*, Monatsh. Math. 85 (1978), 277–282.

This work treats the same problem and our results are stated. Nevertheless, Brakemeier's paper is not self-contained. Our Lemma 3 is contained in his Hilfssatz 3. For a proof, the reader is referred to the author's thesis "Ein Beitrag zur additiven Zahlentheorie, Braunschweig, 1973" and to U. Rickert's thesis "Über eine Vermutung in der additiven Zahlentheorie, Braunschweig, 1976". Our Theorem 2 can be found in the second part of Satz 1, but there the fact is taken as given, without any references. The reader may find in [B] more information about $f(n,k)$ in the special case where n is a prime number.

Département de Mathématiques
Université de Bretagne Occidentale
6 avenue Victor Le Gorgeu
B.P. 809, 29285 Brest Cedex, France
E-mail: Luis.Gallardo@univ-brest.fr

Département de Mathématiques
Université de Saint-Etienne
23 rue du Dr Paul Michelon
42023 Saint-Etienne Cedex 2, France
E-mail: grekos@univ-st-etienne.fr

Department of Mathematics
University of Helsinki
PL 4 (Yliopistonkatu 5)
00014 Helsingin Yliopisto, Finland
E-mail: pihko@csc.fi

Received on 26.10.1998
and in revised form on 23.11.1998 (3496)