CONDITIONS FOR A ZERO SUM MODULO n

BY

J. D. BOVEY, PAUL ERDÖS AND IVAN NIVEN

In this paper the following result is proved.

THEOREM. *Let $n>0$ and $k \geq 0$ be integers with $n-2k \geq 1$. Given any $n-k$ integers*

(1)
$$a_1, a_2, a_3, \ldots, a_{n-k}$$

there is a non-empty subset of indices $I \subset \{1, 2, \ldots, n-k\}$ such that the sum $\sum_{i \in I} a_i \equiv 0 \pmod{n}$ if at most $n-2k$ of the integers (1) lie in the same residue class modulo n.

The result is best possible if $n \geq 3k-2$ in the sense that if "at most $n-2k$" is replaced by "at most $n-2k+1$" the result becomes false. This can be seen by taking $a_j = 1$ for $1 \leq j \leq n-2k+1$ and $a_j = 2$ for $n-2k+2 \leq j \leq n-k$, noting that the number of 2's here is $n-k-(n-2k+1)=k-1 \leq n-2k+1$.

LEMMA 1. *Let n be a positive integer. For $i=1, 2, \ldots, r$ let A_i be a set of v_i positive integers, incongruent modulo n, and none $\equiv 0 \pmod{n}$. If $\sum_{i=1}^{r} v_i \geq n$ then the set $\sum_{i=1}^{r} (\{0\} \cup A_i)$ contains some non-zero multiple of n.*

Proof. Suppose the result is false. We may presume that A_r is not empty. We use a result of J. H. B. Kemperman and P. Scherk [1] as follows. Let A be the union of r incongruent residue classes $0, a_1, a_2, \ldots, a_{r-1} \pmod{n}$ and B the union of s incongruent classes $0, b_1, b_2, \ldots, b_{s-1} \pmod{n}$. Suppose that if $a \in A$ and $b \in B$ and $a+b \equiv 0 \pmod{n}$ then $a \equiv b \equiv 0 \pmod{n}$. Then $A+B$ is the union of at least $\min(n, r+s-1)$ distinct residue classes modulo n. If we apply this result to the two sets $\{0\} \cup A_1$ and $\{0\} \cup A_2$ we conclude that the set

$$[\{0\} \cup A_1] + [\{0\} \cup A_2]$$

contains representatives from at least $\min(n, v_1+v_2+1)$ distinct classes modulo n. Continuing by induction we conclude that

$$\sum_{i=1}^{r-1} (\{0\} \cup A_i)$$

contains representatives from at least

$$\min\left(n, 1+\sum_{i=1}^{r-1} v_i\right) \geq n-v_r+1$$

distinct residue classes modulo n, and so it contains representatives from at least $n-v_r$ distinct non-zero residue classes modulo n. But $-A_r$ has representatives from v_r non-zero residue classes modulo n, and so there must be a representative from a non-zero residue class in common because there are only $n-1$ such classes. From this observation the lemma follows.

If S is a set of integers (not necessarily distinct) we let $\sum S$ denote the set of distinct non-zero residue classes (mod n) represented by sums of integers in S. We call a set of three integers which are incongruent modulo n a *triple*, and any incongruent pair of integers a *double*.

LEMMA 2. *If S is a triple with no subset having a zero sum modulo n then $|\sum S| \geq 5$, and if S does not contain $n/2 \pmod n$ then $|\sum S| \geq 6$. (The notation $|\sum S|$ has the usual meaning, the number of elements in $\sum S$.)*

Proof. Let $S = \{a, b, c\}$. If two of the congruences

(2) $\qquad a+b \equiv c, \qquad a+c \equiv b, \qquad b+c \equiv a \pmod n$

are false, say $a+b \not\equiv c$, $a+c \not\equiv b$, then $\sum S$ contains the six distinct non-zero residue classes $a, b, c, a+b, a+c, a+b+c \pmod n$, because for example if $a+b+c \equiv a$ then we have the contradiction $b+c \equiv 0 \pmod n$.

Therefore we may assume that at least two of the congruences in (2) hold, say $a+b \equiv c$ and $a+c \equiv b$. In this case, by addition we see that $2a \equiv 0$, i.e. $a \equiv n/2 \pmod n$, and $\sum S$ contains the five distinct non-zero residue classes $a, b, c, b+c, a+b+c \pmod n$, because for example if $b+c \equiv a$ we obtain the contradiction $a+b+c \equiv 2a \equiv 0 \pmod n$.

LEMMA 3. *If S is a double having no zero sum then $|\sum S| = 3$.*

The proof is obvious.

Now we turn to the theorem itself, giving a proof by contradiction. Let $a_1, a_2, \ldots, a_{n-k}$ be a sequence of $n-k$ positive integers with no zero sums modulo n, and such that at most $n-2k$ terms belong to the same residue class modulo n. We will show that there is a partition of the index set $\{1, 2, \ldots, n-k\}$ into disjoint sets $P_1 \cup \cdots \cup P_r$ in such a way that if $i, j \in P_t$ and $i \neq j$ then $a_i \not\equiv a_j \pmod n$, and so that

$$\sum_{t=1}^{r} |\sum S_t| \geq n$$

where $S_t = \{a_i \mid i \in P_t\}$ for $1 \leq t \leq r$. Then Lemma 1 gives us the required contradiction.

First suppose that the sequence (1) contains no integer $\equiv n/2 \pmod n$. Select from the sequence (1) in any manner whatsoever, triples of elements if possible until all that is left in the sequence (1) is a single repeated element a modulo n, or two repeated elements a and b modulo n, with $a \not\equiv b$. Suppose by this process we get j triples, with $j \geq 0$, and the remaining elements a (with say λ occurrences)

and b (with say μ occurrences), and we may presume $\lambda \geq \mu \geq 0$. Since there are $n-k$ elements in the sequence (1) we see that

$$n-k = 3j+\lambda+\mu, \quad j = \tfrac{1}{3}(n-k-\lambda-\mu).$$

In addition to the j triples we form μ doubles of the form $\{a, b\}$ and $\lambda-\mu$ singles of the form $\{a\}$. Call the triples S_i with $1 \leq i \leq j$, the doubles S_i with $j+1 \leq i \leq j+\mu$, and the singles S_i with $j+\mu+1+ \leq i \leq j+\lambda$. By Lemmas 2 and 3 we conclude that

$$\sum_{i=1}^{j+\lambda} |\textstyle\sum S_i| = 6j+3\mu+(\lambda-\mu) = n+(n-2k)-\lambda \geq n,$$

the last inequality holding because $n-2k \geq \lambda$, there being at most $n-2k$ identical elements modulo n in the sequence (1).

Finally, suppose that $n/2$ is in the sequence (1). It can occur only once since $n/2+n/2 \equiv 0 \pmod{n}$. By the same process as in the first part we choose j triples $S_1, \ldots, S_j$ without using the element $n/2$, so that what remains in the sequence (1) are the element $n/2$ once, the element a occurring λ times, and the element b occurring μ times, again with $\lambda \geq \mu \geq 0$. We deal with three special cases: $\lambda > \mu$; $\lambda = \mu > 0$; $\lambda = \mu = 0$. In all cases we have $n-k = 3j+\lambda+\mu+1$.

In case $\lambda > \mu$ we choose μ doubles of the form $\{a, b\}$ and an additional double $\{a, n/2\}$, and also $\lambda-\mu-1$ singles of the form $\{a\}$. Thus we get   ·

$$\sum_i |\textstyle\sum S_i| \geq 6j+3(\mu+1)+(\lambda-\mu-1) = n+(n-2k)-\lambda \geq n$$

as before.

In case $\lambda = \mu > 0$ we have, in addition to the j triples without the element $n/2$ also the triple $\{n/2, a, b\}$ and the $\lambda-1$ doubles of the form $\{a, b\}$. This gives us

$$\sum_i |\textstyle\sum S_i| \geq 6j+5+3(\lambda-1) = n+(n-2k)-\lambda \geq n.$$

In case $\lambda = \mu = 0$ we have one single $\{n/2\}$ and we get

$$\sum_i |\textstyle\sum S_i| \geq 6j+1 = n+(n-2k)-1 \geq n.$$

REFERENCE

1. H. Halberstam and K. F. Roth, *Sequences I*, Oxford, 1966, p. 50, Theorem 15′.

UNIVERSITY OF YORK
UNIVERSITY OF COLORADO
and
UNIVERSITY OF OREGON