Reprint from
The Bulletin of the Research Council of Israel, Section F: Mathematics and Physics,
August 1961, Vol. 10 F1
THE ISRAEL MATHEMATICAL UNION

Theorem in the additive number theory

P. ERDÖS, A. GINZBURG AND A. ZIV, *Division of Mathematics, Technion–Israel Institute of Technology, Haifa*

THEOREM. *Each set of $2n-1$ integers contains some subset of n elements the sum of which is a multiple of n.*

PROOF. Assume first $n = p$ (p prime). Our theorem is trivial for $p = 2$, thus henceforth $p > 2$. We need the following

LEMMA. Let $p > 2$ be a prime and $A = \{a_1, a_2, \ldots, a_s\}$ $2 \leqq s < p$ a set of s integers each prime to p satisfying $a_1 \not\equiv a_2 \pmod p$. Then the set $\sum_{i=1}^{s} \varepsilon_i a_i$, $\varepsilon = 0$ or 1 contains at least $s+1$ distinct congruence classes.

We use induction. If $s = 2$, a_1, a_2, $a_1 + a_2$ are all incongruent (since $a_1 \not\equiv a_2$, $a_1 \not\equiv 0$, $a_2 \not\equiv 0$). Thus the lemma holds for $s = 2$. Assume that it holds for $s - 1$, we shall prove it for s.

Let $b_1, b_2, \ldots, b_k$ be all the congruence classes of the form $\sum_{i=1}^{s-1} \varepsilon_i a_i$. By assumption $k \geqq s$. If $k \geqq s+1$ there is nothing to prove. Thus we can assume $k = s < p$. But then since $a_s \not\equiv 0 \pmod p$ it is easy to see (see e.g. [1]) that at least one of the integers $b_i + a_s$, $1 \leqq i \leqq k$ is incongruent to all the b's. Thus the number of integers of the form $\sum_{i=1}^{s} \varepsilon_i a_i$, $\varepsilon_i = 0$ or 1 is at least $s + 1$, which proves the Lemma.

Let there be given $2p-1$ residues (mod p). Arrange them according to size $0 \leqq a_1 \leqq a_2 \leqq \cdots \leqq a_{2p-1} < p$.

We can assume $a_i \neq a_{i+p-1}$ (for otherwise $\sum_{j=i}^{i+p-1} a_j = pa_i \equiv 0 \pmod p$) and that $\sum_{i=1}^{p} a_i \equiv c \not\equiv 0 \pmod p$. Put $b_i = a_{p+i} - a_{i+1}$, $1 \leqq i \leqq p-1$. Clearly $-c \equiv \sum_{i=1}^{p-1} \varepsilon_i b_i$, $\varepsilon_i = 0$ or 1 is solvable. If the b's are not all congruent this follows from our Lemma and if the b's are all congruent the statement is evident.
Clearly

$$\sum_{i=1}^{p} a_i + \sum_{i=1}^{p-1} \varepsilon_i b_i \equiv 0 \pmod p$$

is the sum of p a's. Thus our Theorem is proved for $n = p$.

Now we prove that if our Theorem is true for $n = u$ and $n = v$ it also holds for $n = uv$, and this will clearly prove our Theorem for composite n.

Let there be given $2uv-1$ integers $a_1, a_2, \ldots, a_{2uv-1}$. Since our Theorem holds for u we can find u of them whose sum is a multiple of u. Omitting these u integers we repeat the same procedure. If we repeated it $2v-2$ times we are left with $2uv-1-(2v-2)\,u = 2u-1$ a's and since our Theorem holds for u we can again find u of them whose sum is a multiple of u. Thus we have obtained $2v-1$ distinct sets $a_1^{(i)}, \ldots, a_u^{(i)}$, $1 \leqq i \leqq 2v-1$ of the a's satisfying $\sum_{j=1}^{u} a_j^{(i)} = c_i\, u$, $1 \leqq i \leqq 2v-1$. Now, since our theorem holds for v too, we can find v c's say $c_{i_1}, \ldots, c_{i_v}$ satisfying $\sum_{r=1}^{v} c_{i_r} \equiv 0 \pmod{v}$.

But then clearly

$$\sum_{r=1}^{v} \sum_{j=1}^{u} a_j^{(i_r)} = u \sum_{r=1}^{v} c_{i_r} \equiv 0 \pmod{uv}.$$

which completes the proof of our Theorem. Prof. N. G. de Bruijn gave a similar proof of the above Theorem.

The same proof gives the following result:

Let G_n be an abelian group of n elements and $a_1, a_2, \ldots, a_{2n-1}$ are any $2n-1$ of its elements. Then the unit of G_n can be represented as the product of n of the a's.

We do not know if the theorem holds for non-abelian groups too.

REFERENCE

1. Landaw, *Neuere Ergebsisse in Zahlen theorie.*