# 97. Sums Congruent to Zero: the Erdős–Ginzburg–Ziv Theorem

*Every sequence of* $2n-1$ *natural numbers contains* $n$ *terms whose sum is divisible by* $n$. *This assertion is false if* $2n-1$ *is replaced by* $2n-2$.

*First Proof.* Note first that a sequence consisting of $n-1$ 0s and $n-1$ 1s does not have $n$ terms whose sum is divisible by $n$, so the assertion is certainly false with $2n-1$ replaced by $2n-2$.

Let us prove the real assertion in the case when $n$ is a prime: *if* $p$ *is a prime and* $a_1, a_2, \ldots, a_{2p-1}$ *is a sequence of integers then the sum of some* $p$ *terms is divisible by* $p$. As we are interested in divisibility by $p$, we may assume that $0 \leq a_1 \leq a_2 \leq \cdots \leq a_{2p-1} < p$. If, for some $i$, $1 \leq i \leq p-1$, we have $a_{i+p-1} = a_i$ then all $p$ terms $a_i, a_{i+1}, \ldots, a_{i+p-1}$ are equal, so their sum is a multiple of $p$. Therefore we may suppose that $a_i \neq a_{i+p-1}$ for $i = 1, \ldots, i+p-1$.

We claim that in this case considerably more is true than the assertion we have to prove: for every integer $s$ there is a set of $p$ terms of our sequence whose sum is congruent to $s$ modulo $p$. To show this, let $A_i = \{a_i, a_{i+p-1}\}$, $i-1, \ldots, p-1$ and $A_p = \{a_{2p-1}\}$ be *subsets of* $\mathbb{Z}_p$. We shall prove that $A_1 + A_2 + \cdots + A_p = \mathbb{Z}_p$, i.e., every element of $\mathbb{Z}_p$ is the sum of $p$ terms, one from each set $A_i$. This will follow if we prove that for each $i$, $1 \leq i < p$, the set $B_i = A_1 + A_2 + \cdots + A_i$ has at least $i+1$ elements.

Suppose that this is false. Then for some $i$, $1 \leq i < p-1$, the sets $B_i$ and $B_{i+1}$ have $i+1$ elements each. To simplify the notation, set $B = B_i$ and $A_{i+1} = \{c, d\}$. Then the sets $C = B + c$ and $D = B + d$ coincide, i.e., the set $C$ is invariant under the addition of $e = d - c$: if $x$ is in $C$, then so are $x + e$, $x + 2e$, etc. But then, since $p$ is prime, $C$ is the entire set $\mathbb{Z}_p$, contradicting our assumption that $|C| = |B_i| = i + 1 < p$. This contradiction completes our proof in the case when $p$ is a prime.

The general case follows easily by induction on $n$. Indeed, for $n = 1$ there is nothing to prove. Suppose that $n > 1$ and the assertion holds for smaller values of $n$. Let $p$ be a prime factor of $n$ and set $m = n/p$. Successively select disjoint $p$-subsets $I_1, \ldots, I_{2m-1}$ of $I = \{1, \ldots, 2n-1\}$ such that each $b_j = \sum_{i \in I_j} a_j$, $j = 1, \ldots, 2m-1$, is a multiple of $p$. This can be done since when we have selected $\ell < 2m-1$ such sets, we still have a sequence of $2n-1-\ell p \geq 2n-1-(2m-2)p = 2p-1$ elements to choose from.

Finally, consider the integer sequence $c_1, \ldots, c_{2m-1}$, where $c_i = b_i/p$. Since $m < n$, by the induction hypothesis there is an $m$-set $J \subset \{1, \ldots, 2m-1\}$ such that $\sum_{j \in J} c_j$ is divisible by $m$. Consequently, the $n$-set $I = \bigcup_{j \in J} I_j \subset \{1, 2, \ldots,$

$2n-1\}$ is such that $\sum_{i\in I} a_i = p\sum_{j\in J}\sum_{i\in I_j} a_i/p = p\sum_{j\in J} c_j$ is a multiple of $pm = n$, as claimed. □

*Second Proof.* Let us give another proof in the main case, i.e., when $n$ is a prime $p$. Thus, let $a_1, \ldots, a_{2p-1}$ be a sequence of $2p-1$ elements of $\mathbb{Z}_p$. Let us evaluate the sum

$$S = \sum_{I\subset\mathbb{Z}_p, |I|=p} \left(\sum_{i\in I} a_i\right)^{p-1}$$

in two different ways. First, considering $S$ as a polynomial over $\mathbb{Z}$ in the variables $a_1, \ldots, a_{2p-1}$, write $S$ as the sum of monomials of the form

$$c_{\mathbf{k}} \prod_{i\in I} a_i^{k_i},$$

where $\mathbf{k} = (k_i)_1^p$ is a sequence of $p$ non-negative integers $k_i$ summing to $p-1$. Let $|\mathbf{k}|$ be the number of non-zero terms of the sequence $\mathbf{k}$, so that $1 \le |\mathbf{k}| \le p-1$. Clearly, a $p$-set $I$ is such that $\left(\sum_{i\in I} a_i\right)^{p-1}$ contributes to $c_{\mathbf{k}}$ if $I$ contains the $|\mathbf{k}|$ non-zero indices $i$ with $k_i > 0$, and each such $p$-set contributes the same natural number. Since there are

$$\binom{2p-1-|\mathbf{k}|}{p-|\mathbf{k}|} \equiv 0 \pmod{p}$$

such sets $I$, the coefficient $c_{\mathbf{k}}$ is a multiple of $p$ so, *a fortiori*, $S = 0$ in $\mathbb{Z}_p$.

Now, let us evaluate $S$ in a different way, supposing that the assertion fails, i.e., $\sum_{i\in I} a_i \neq 0$ whenever $I \subset \mathbb{Z}_p$ and $|I| = p$. Then, by Fermat's little theorem, $\left(\sum_{i\in I} a_i\right)^{p-1} = 1$ for every $p$-subset $I$ of $\mathbb{Z}_p$ so, since

$$\binom{2p-1}{p} \equiv 1 \pmod{p},$$

we see that $S = 1$. This contradiction completes our second proof. □

**Notes.** The assertion is the celebrated and extremely influential *Erdős–Ginzburg–Ziv theorem*, proved in 1961. The first proof above is the original; the second, due to N. Zimmermann, was reported by Alon and Dubiner in a beautiful survey of some of the many results related to the Erdős–Ginzburg–Ziv theorem.

The heart of the original proof is the assertion that if $A_1, A_2, \ldots, A_{p-1}$ are subsets of $\mathbb{Z}_p$, each with two elements, then $A_1 + A_2 + \cdots + A_{p-1} = \mathbb{Z}_p$. This is immediate from the Cauchy–Davenport theorem (see Problem 96); in fact, as shown above, this inequality is a consequence of the first non-trivial case of the Cauchy–Davenport theorem that if $A$ and $B$ are subsets of $\mathbb{Z}_p$, with $2 \le |A| \le p-1$ and $|B| = 2$ then $|A+B| \ge |A| + 1$.

Alon and Dubiner presented five proofs of the and Erdős–Ginzburg–Ziv theorem, including the two given above. A third proof, due to Alon, is based on the following theorem of Chevalley and Warning on polynomials over a finite field.

*Let $p$ be a prime, and for $j = 1, \ldots, n$, let $P_j(X_1, \ldots, X_m)$ be a polynomial over $\mathbb{Z}_p$ with degree $d_j$ such that*

$$\sum_{j=1}^{n} d_j < m.$$

*Then the number of common zeros of $P_1, \ldots, P_n$ in $\mathbb{Z}_p^m$ is divisible by $p$. In particular, if the polynomials have a common zero then they have at least two common zeros.*

We leave the easy proof of this result to the reader and rather show how Alon deduced from it (the heart of) the Erdős–Ginzburg–Ziv theorem.

*Third Proof.* As before, let $p$ be a prime and let $a_1, \ldots, a_{2p-1}$ be a sequence of elements of $\mathbb{Z}_p$. Define polynomials $P_1$ and $P_2$ over $\mathbb{Z}_p$ as follows:

$$P_1(X_1, \ldots, X_{2p-1}) = \sum_{i=1}^{2p-1} X_i^{p-1} \quad \text{and} \quad P_2(X_1, \ldots, X_{2p-1}) = \sum_{i=1}^{2p-1} a_i X_i^{p-1}.$$

Clearly, $\mathbf{0} = (0, \ldots, 0) \in \mathbb{Z}_p^{2p-1}$ is a zero of both $P_1$ and $P_2$. Also, the sum of the degrees of $P_1$ and $P_2$ is $2(p-1)$, which is less than the number of variables, $2p-1$. Hence, by the Chevalley–Warning theorem, $P_1$ and $P_2$ have another (this time, non-trivial) common zero $\mathbf{z} = (z_1, \ldots, z_{2p-1})$. Let $I = \{i : z_i \neq 0\}$, and note that, by the little Fermat theorem, $z_i^{p-1} = 1$ if $i \in I$ and $z_i^{p-1} = 0$ if $i \notin I$. Consequently, $P_1(\mathbf{z}) = \sum_{i \in I} 1 = 0$ and $P_2(\mathbf{z}) = \sum_{i \in I} a_i = 0$, i.e., $|I| \neq 0$ is a multiple of $p$ and $\sum_{i \in I} a_i = 0$. Since $0 < |I| < 2p-1$, we see that $|I| = p$ and $\sum_{i \in I} a_i = 0$, as claimed. □

The following beautiful extension of the Erdős–Ginzburg–Ziv theorem was conjectured by Kemnitz in 1981: every sequence of lattice points in $\mathbb{Z}^2$ consisting of $4n-3$ terms contains $n$ terms whose sum has coordinates divisible by $n$. Kemnitz himself proved that if the conjecture is true for $n$ and $m$ then it is true for $nm$ as well; in particular, it suffices to prove the conjecture in the case when $n = p$ for some prime $p$. He also checked that his conjecture holds for $p = 2, 3, 5$ and 7.

Alon and Dubiner made use of the Chevalley–Warning theorem to prove that the conjecture is true with $4p-3$ replaced by $6p-5$ and, for $p$ large, by $5p-2$. Rónyai came tantalizingly close to proving Kemnitz's conjecture when he showed that the assertion is true for $4p-2$ instead of $4p-3$. Finally, in October 2003, Reiher, an undergraduate, gave an elegant and simple proof of the conjecture by making clever use of the Chevalley–Warning theorem. According to Savchev and

Chen, at the same time, C. di Fiore, a high school student, independently found a similar proof.

In a different direction, Bollobás and Leader proved that if $G$ is an Abelian group of order $n$, $1 \leq r \leq n-1$, $a_1, \ldots, a_{k+r} \in G$ and 0 is not an $n$-sum, then the number of $n$-sums is at least $r+1$. The case $r = n-1$ clearly implies the Erdős–Ginzburg–Ziv theorem. The original proof of this result was not too complicated, but Yu found an even simpler proof.

There are numerous other developments stemming from the Erdős–Ginzburg–Ziv theorem: for a sample of these, see the references below.


N. Alon and M. Dubiner, Zero-sum sets of prescribed size, in *Combinatorics, Paul Erdős is Eighty*, Vol. 1, Bolyai Soc. Math. Stud., János Bolyai Math. Soc., Budapest, (1993), pp. 33–50.

A. Bialostocki, G. Bialostocki and D. Schaal, A zero-sum theorem, *J. Combin. Theory* Ser. A **101** (2003), 147–152.

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.

A. Bialostocki, P. Dierker, D. Grynkiewicz and M. Lotspeich, On some developments of the Erdős–Ginzburg–Ziv theorem, II, *Acta Arith.* **110** (2003), 173–184.

B. Bollobás and I. Leader, The number of $k$-sums modulo $k$, *J. Number Theory* **78** (1999), 27–35.

P. Erdős, A. Ginzburg and A. Ziv, Theorem in additive number theory, *Bull. Res. Council Israel* **10F** (1961), 41–43.

C. Flores and O. Ordaz, On the Erdős–Ginzburg–Ziv theorem, *Discrete Math.* **152** (1996), 321–324.

L. Gallardo, and G. Grekos, On Brakemeier's variant of the Erdős–Ginzburg–Ziv problem, in *Number Theory*, (Liptovský Jń, 1999), Tatra Mt. Math. Publ. **20** (2000), 91–98.

L. Gallardo, G. Grekos, L. Habsieger, F. Hennecart, B. Landreau and A. Plagne, Restricted addition in $\mathbb{Z}/n\mathbb{Z}$ and an application to the Erdős–Ginzburg–Ziv problem, *J. London Math. Soc.* (2) **65** (2002), 513–523.

L. Gallardo, G. Grekos and J. Pihko, On a variant of the Erdős–Ginzburg–Ziv problem, *Acta Arith.* **89** (1999), 331–336.

W.D. Gao, An improvement of the Erdős–Ginzburg–Ziv theorem (in Chinese), *Acta Math. Sinica* **39** (1996), 514–523.

W.D. Gao, On the Erdős–Ginzburg–Ziv theorem – a survey, in *Paul Erdős and his Mathematics* (Budapest, 1999), János Bolyai Math. Soc., Budapest, (1999), pp. 76–78.

Y.O. Hamidoune, On weighted sums in abelian groups, *Discrete Math.* **162** (1996), 127–132.

Y.O. Hamidoune, O. Ordaz, and A. Ortuño, On a combinatorial theorem of Erdős, Ginzburg and Ziv, *Combin. Prob. and Comput.* **7** (1998), 403–412.

A. Kemnitz, On a lattice point problem *Ars Combin.* **16** (1983), 151–160.

C. Reiher, Kemnitz' conjecture concerning lattice-points in the plane, to appear.

L. Rónyai, On a conjecture of Kemnitz, *Combinatorica* **20** (2000), 569–573.

S. Savchev and F. Chen, Kemnitz' conjecture revisited, *Discrete Math.* **297** (2005), 196–201.

Z.-W. Sun, Unification of zero-sum problems, subset sums and covers of $\mathbb{Z}$, *Electron. Res. Announc. Amer. Math. Soc.* **9** (2003), 51–60 (electronic).

C. Wang, Note on a variant of the Erdős–Ginzburg–Ziv problem, *Acta Arith.* **108** (2003), 53–59.

H.B. Yu, A simple proof of a theorem of Bollobás and Leader, *Proc. Amer. Math. Soc.* **131** (2003), 2639–2640.