

# The Erdős–Ginzburg–Ziv Theorem

Arthur F. Ramos

David Barros Hulak

Ruy J. G. B. de Queiroz

June 25, 2026

## Abstract

We formalize the Erdős–Ginzburg–Ziv theorem for integer multisets: every multiset of at least  $2n - 1$  integers contains a submultiset of cardinality  $n$  whose sum is divisible by  $n$ . The proof is split into a prime-modulus argument over residue multisets and a strong-induction argument for the general case, following the classical theorem of Erdős, Ginzburg, and Ziv [1]. AI assistance was used for proof engineering. The final definitions, statements, and proofs are checked by Isabelle.

## 1 Introduction

The Erdős–Ginzburg–Ziv theorem is a classical result in additive number theory. In the form formalized here, every multiset of at least  $2n - 1$  integers contains an  $n$ -element submultiset whose sum is congruent to 0 modulo  $n$ .

This Isabelle/HOL development separates the finite combinatorial arguments from the induction on the modulus. The prime case is handled on residue multisets modulo  $p$  by sorting the nontrivial case and reducing the final choice to a subset-sum problem over  $\mathbb{Z}/p\mathbb{Z}$ . The general case factors a composite modulus as  $n = mp$ , extracts many prime-sized zero-sum blocks, and applies strong induction to the multiset of block sums divided by  $p$ .

## 2 Organization

The session is split into three main theories:

- `EGZ_Basics` develops modular translations and subset-sum coverage.
- `EGZ_Prime` proves the prime-modulus theorem.
- `Erdos_Ginzburg_Ziv` derives the full theorem for arbitrary positive moduli.

## Contents

<b>1</b>	<b>Introduction</b>	<b>1</b>
<b>2</b>	<b>Organization</b>	<b>1</b>
<b>3</b>	<b>Residue and subset-sum infrastructure</b>	<b>2</b>
3.1	Residues and modular translations . . . . .	2
3.2	Growth of subset sums . . . . .	4
3.3	Realizing subset sums by index sets . . . . .	4

<b>4</b>	<b>The prime case</b>	<b>5</b>
4.1	Compatibility of reduction modulo $p$ . . . . .	5
4.2	Sorted pairings and nonzero gaps . . . . .	5
4.3	Choosing one element from each pair . . . . .	6
4.4	The residue-valued prime theorem . . . . .	6
4.5	Lifting the prime theorem back to integers . . . . .	6
<b>5</b>	<b>The full Erdős-Ginzburg-Ziv theorem</b>	<b>7</b>
5.1	Auxiliary multiset decompositions . . . . .	7
5.2	Strong induction on the modulus . . . . .	7
5.3	The monotone cardinality form . . . . .	7
<b>6</b>	<b>Overview</b>	<b>8</b>
<b>7</b>	<b>Main results</b>	<b>8</b>
<b>8</b>	<b>Proof architecture</b>	<b>8</b>

theory *EGZ\_Basics*

imports

*Main*

*HOL-Library.Multiset*

*HOL-Number\_Theory.Cong*

*HOL-Computational\_Algebra.Primes*

begin

### 3 Residue and subset-sum infrastructure

This theory isolates the finite combinatorial infrastructure used in the prime case. We work with a recursive set of subset sums modulo  $p$ , together with modular translations on the residue set *residues*  $p$ . The key output is that a list of  $p - 1$  nonzero residues modulo a prime already generates every residue class by subset summation.

#### 3.1 Residues and modular translations

**definition** *residues* ::  $nat \Rightarrow int\ set$  **where**

*residues*  $p = \{0..<int\ p\}$

**definition** *mod\_translate* ::  $nat \Rightarrow int \Rightarrow int\ set \Rightarrow int\ set$  **where**

*mod\_translate*  $p\ d\ A = ((\lambda x. (x + d) \bmod int\ p) ` A)$

**definition** *list\_index\_sum* ::  $int\ list \Rightarrow nat\ set \Rightarrow int$  **where**

*list\_index\_sum*  $xs\ I = (\sum_{i \in I} xs\ !\ i)$

**fun** *mod\_subset\_sums* ::  $nat \Rightarrow int\ list \Rightarrow int\ set$  **where**

*mod\_subset\_sums*  $p\ [] = \{0\}$

| *mod\_subset\_sums*  $p\ (d \# ds) = mod\_translate\ p\ d\ (mod\_subset\_sums\ p\ ds)$

**lemma** *residues\_finite* [*simp*]:

*finite* (*residues*  $p$ )

*<proof>*

**lemma** *card\_residues* [*simp*]:  
**assumes**  $0 < p$   
**shows**  $\text{card } (\text{residues } p) = p$   
 $\langle \text{proof} \rangle$

**lemma** *mod\_translate\_iff*:  
 $x \in \text{mod\_translate } p \ d \ A \longleftrightarrow (\exists a \in A. x = (a + d) \bmod \text{int } p)$   
 $\langle \text{proof} \rangle$

**lemma** *mod\_translate\_subset\_residues*:  
**assumes**  $0 < p$   
**assumes**  $A \subseteq \text{residues } p$   
**shows**  $\text{mod\_translate } p \ d \ A \subseteq \text{residues } p$   
 $\langle \text{proof} \rangle$

**lemma** *mod\_translate\_inj\_on\_residues*:  
**assumes**  $0 < p$   
**shows**  $\text{inj\_on } (\lambda x. (x + d) \bmod \text{int } p) \ (\text{residues } p)$   
 $\langle \text{proof} \rangle$

**lemma** *card\_mod\_translate\_eq*:  
**assumes**  $0 < p$   
**assumes**  $A \subseteq \text{residues } p$   
**shows**  $\text{card } (\text{mod\_translate } p \ d \ A) = \text{card } A$   
 $\langle \text{proof} \rangle$

**lemma** *mod\_translate\_compose*:  
**assumes**  $0 < p$   
**shows**  $\text{mod\_translate } p \ c \ (\text{mod\_translate } p \ d \ A) = \text{mod\_translate } p \ (c + d) \ A$   
 $\langle \text{proof} \rangle$

**lemma** *mod\_subset\_sums\_contains\_zero* [*simp*]:  
 $0 \in \text{mod\_subset\_sums } p \ ds$   
 $\langle \text{proof} \rangle$

**lemma** *mod\_subset\_sums\_nonempty* [*simp*]:  
 $\text{mod\_subset\_sums } p \ ds \neq \{\}$   
 $\langle \text{proof} \rangle$

**lemma** *mod\_subset\_sums\_subset\_residues*:  
**assumes**  $0 < p$   
**shows**  $\text{mod\_subset\_sums } p \ ds \subseteq \text{residues } p$   
 $\langle \text{proof} \rangle$

**lemma** *mod\_mult\_inj\_on\_residues*:  
**assumes** *prime\_p*:  $\text{prime } p$   
**assumes** *d\_nz*:  $d \bmod \text{int } p \neq 0$   
**shows**  $\text{inj\_on } (\lambda x. (x * d) \bmod \text{int } p) \ (\text{residues } p)$   
 $\langle \text{proof} \rangle$

**lemma** *image\_mult\_residues*:  
**assumes** *prime\_p*:  $\text{prime } p$

**assumes**  $d\_nz: d \bmod \text{int } p \neq 0$   
**shows**  $((\lambda x. (x * d) \bmod \text{int } p) \text{ `residues } p) = \text{residues } p$   
 $\langle \text{proof} \rangle$

**lemma** *mod\_translate\_eq\_self\_imp\_full*:  
**assumes**  $\text{prime\_}p: \text{prime } p$   
**assumes**  $A\_sub: A \subseteq \text{residues } p$   
**assumes**  $A\_nonempty: A \neq \{\}$   
**assumes**  $A\_fix: \text{mod\_translate } p \ d \ A = A$   
**assumes**  $d\_nz: d \bmod \text{int } p \neq 0$   
**shows**  $A = \text{residues } p$   
 $\langle \text{proof} \rangle$

**lemma** *mod\_translate\_proper\_union\_grows*:  
**assumes**  $\text{prime\_}p: \text{prime } p$   
**assumes**  $A\_sub: A \subseteq \text{residues } p$   
**assumes**  $A\_nonempty: A \neq \{\}$   
**assumes**  $A\_proper: A \neq \text{residues } p$   
**assumes**  $d\_nz: d \bmod \text{int } p \neq 0$   
**shows**  $\text{card } (A \cup \text{mod\_translate } p \ d \ A) > \text{card } A$   
 $\langle \text{proof} \rangle$

### 3.2 Growth of subset sums

**lemma** *card\_mod\_subset\_sums\_lower\_bound*:  
**assumes**  $\text{prime\_}p: \text{prime } p$   
**assumes**  $\text{nonzero}: \forall d \in \text{set } ds. d \bmod \text{int } p \neq 0$   
**shows**  $\text{card } (\text{mod\_subset\_sums } p \ ds) \geq \min p \ (\text{Suc } (\text{length } ds))$   
 $\langle \text{proof} \rangle$

### 3.3 Realizing subset sums by index sets

**lemma** *mod\_subset\_sums\_iff\_nth*:  
 $x \in \text{mod\_subset\_sums } p \ ds \longleftrightarrow (\exists I. I \subseteq \{..<\text{length } ds\} \wedge x = \text{sum\_list } (\text{nths } ds \ I) \bmod \text{int } p)$   
 $\langle \text{proof} \rangle$

**lemma** *mod\_subset\_sums\_eq\_residues*:  
**assumes**  $\text{prime\_}p: \text{prime } p$   
**assumes**  $\text{len}: \text{length } ds = p - 1$   
**assumes**  $\text{nonzero}: \forall d \in \text{set } ds. d \bmod \text{int } p \neq 0$   
**shows**  $\text{mod\_subset\_sums } p \ ds = \text{residues } p$

The lower-bound lemma shows that each nonzero increment strictly enlarges the current set of subset sums until all  $p$  residues have been reached. Since all subset sums stay inside *residues*  $p$ , cardinality forces equality with the full residue system.

$\langle \text{proof} \rangle$

**lemma** *sum\_list\_nth\_eq\_list\_index\_sum*:  
**assumes**  $I\_sub: I \subseteq \{..<\text{length } xs\}$   
**shows**  $\text{sum\_list } (\text{nths } xs \ I) = \text{list\_index\_sum } xs \ I$   
 $\langle \text{proof} \rangle$

**lemma** *mod\_subset\_sums\_iff\_list\_index\_sum*:

$x \in \text{mod\_subset\_sums } p \text{ } ds \iff (\exists I. I \subseteq \{..<\text{length } ds\} \wedge x = \text{list\_index\_sum } ds \text{ } I \text{ mod int } p)$   
 <proof>

**lemma** *mset\_nth\_subseteq*:  
 $\text{mset } (nths \text{ } xs \text{ } I) \subseteq\# \text{mset } xs$   
 <proof>

**lemma** *list\_index\_sum\_partition*:  
**assumes**  $I\_sub: I \subseteq \{..<\text{length } xs\}$   
**shows**  $\text{list\_index\_sum } xs \text{ } (\{..<\text{length } xs\} - I) + \text{list\_index\_sum } xs \text{ } I = \text{sum\_list } xs$   
 <proof>

**lemma** *list\_index\_sum\_map2\_diff*:  
**assumes**  $len: \text{length } xs = \text{length } ys$   
**assumes**  $I\_sub: I \subseteq \{..<\text{length } xs\}$   
**shows**  $\text{list\_index\_sum } (\text{map2 } (\lambda x \ y. y - x) \text{ } xs \text{ } ys) \text{ } I = \text{list\_index\_sum } ys \text{ } I - \text{list\_index\_sum } xs \text{ } I$   
 <proof>

**end**  
**theory** *EGZ\_Prime*  
**imports**  
*EGZ\_Basics*  
**begin**

## 4 The prime case

The prime-modulus argument works entirely on residues modulo a prime  $p$ . After reducing an integer multiset modulo  $p$ , there are two possibilities: either some residue occurs at least  $p$  times, yielding an immediate zero-sum block, or every residue occurs fewer than  $p$  times. In the latter case we sort the remaining residues, pair the lower and upper halves, and use the subset-sum coverage theorem from the basics theory on the resulting list of nonzero gaps.

### 4.1 Compatibility of reduction modulo $p$

**lemma** *sum\_mset\_mod\_image*:  
 $\text{sum\_mset } (\text{image\_mset } (\lambda x::\text{int}. x \text{ mod } m) \text{ } M) \text{ mod } m = \text{sum\_mset } M \text{ mod } m$   
 <proof>

### 4.2 Sorted pairings and nonzero gaps

**lemma** *sorted\_nth\_gap*:  
**assumes**  $\text{prime\_}p: \text{prime } p$   
**assumes**  $\text{sorted\_}ys: \text{sorted } ys$   
**assumes**  $len: \text{length } ys = 2 * (p - 1)$   
**assumes**  $\text{count\_bound}: \forall r. \text{count } (\text{mset } ys) \text{ } r < p$   
**assumes**  $i\_lt: i < p - 1$   
**shows**  $ys \ ! \ i < ys \ ! \ (i + (p - 1))$   
 <proof>

**lemma** *pair\_differences\_nonzero*:  
**assumes**  $\text{prime\_}p: \text{prime } p$

```

assumes sorted_ys: sorted ys
assumes len: length ys = 2 * (p - 1)
assumes ys_res: set ys  $\subseteq$  residues p
assumes count_bound:  $\forall r. \text{count } (mset \text{ } ys) \text{ } r < p$ 
shows  $\forall d \in \text{set } (map2 (\lambda a \ b. b - a) (take (p - 1) \text{ } ys) (drop (p - 1) \text{ } ys)). d \bmod \text{int } p \neq 0$ 
<proof>

```

### 4.3 Choosing one element from each pair

```

lemma paired_choice_length:
assumes len_ys: length ys = 2 * n
assumes I_sub: I  $\subseteq$  {.. $n$ }
shows length (nth (take n ys) (I - I) @ nth (drop n ys) I) = n
<proof>

```

```

lemma paired_choice_subset:
  mset (nth (take n ys) (I - I) @ nth (drop n ys) I)  $\subseteq\#$  mset ys
<proof>

```

```

lemma paired_choice_sum:
assumes len_ys: length ys = 2 * n
assumes I_sub: I  $\subseteq$  {.. $n$ }
shows sum_list (nth (take n ys) (I - I) @ nth (drop n ys) I) =
  sum_list (take n ys) + list_index_sum (map2 (\lambda a \ b. b - a) (take n ys) (drop n ys)) I
<proof>

```

### 4.4 The residue-valued prime theorem

In the nontrivial branch we remove one distinguished residue  $z$ , sort the remaining residues, split them into lower and upper halves, and consider the pairwise differences. Those differences are nonzero modulo  $p$ , so the subset-sum coverage theorem from the basics theory can realize the correction term needed to turn the lower half into a  $p$ -element zero-sum submultiset.

```

lemma prime_residue_zero_sum_submultiset:
assumes prime_p: prime p
assumes size_R: size R = 2 * p - 1
assumes R_sub: set_mset R  $\subseteq$  residues p
shows  $\exists N. N \subseteq\# R \wedge \text{size } N = p \wedge \text{sum\_mset } N \bmod \text{int } p = 0$ 
<proof>

```

### 4.5 Lifting the prime theorem back to integers

```

theorem prime_egz:
assumes prime_p: prime p
assumes size_M: size M = 2 * p - 1
shows  $\exists N. N \subseteq\# M \wedge \text{size } N = p \wedge \text{sum\_mset } N \bmod \text{int } p = 0$ 
<proof>

```

**end**

**theory** Erdos\_Ginzburg\_Ziv

**imports**

EGZ\_Prime

HOL-Computational\_Algebra.Primes

begin

## 5 The full Erdős-Ginzburg-Ziv theorem

The composite-modulus case is obtained from the prime case by strong induction. Writing  $n$  as  $m * p$  with  $p$  prime, we repeatedly extract  $p$ -element zero-sum blocks, divide their sums by  $p$ , and apply the induction hypothesis to the resulting multiset of quotients.

### 5.1 Auxiliary multiset decompositions

**lemma** *exists\_submultiset\_of\_size:*

**fixes**  $M :: 'a::linorder\ multiset$

**assumes**  $n\_le: n \leq size\ M$

**shows**  $\exists N. N \subseteq\# M \wedge size\ N = n$

*<proof>*

**lemma** *union\_blocks\_size:*

**fixes**  $Bs :: 'a\ multiset\ multiset$

**assumes**  $blocks\_size: \forall B \in\# Bs. size\ B = n$

**shows**  $size\ (sum\_mset\ Bs) = size\ Bs * n$

*<proof>*

**lemma** *union\_blocks\_div\_sum:*

**assumes**  $blocks\_div: \forall B \in\# Bs. sum\_mset\ B\ mod\ int\ p = 0$

**shows**  $sum\_mset\ (sum\_mset\ Bs) = int\ p * sum\_mset\ (image\_mset\ (\lambda B. sum\_mset\ B\ div\ int\ p)\ Bs)$

*<proof>*

**lemma** *extract\_prime\_blocks:*

**assumes**  $prime\_p: prime\ p$

**assumes**  $size\_M: size\ M = k * p + (p - 1)$

**shows**  $\exists Bs\ R. M = sum\_mset\ Bs + R \wedge size\ Bs = k \wedge size\ R = p - 1 \wedge$   
 $(\forall B \in\# Bs. size\ B = p \wedge sum\_mset\ B\ mod\ int\ p = 0)$

*<proof>*

### 5.2 Strong induction on the modulus

The prime branch is handled directly by *prime\_egz*. For a composite modulus  $n$ , the previous lemma extracts  $2 * m - 1$  prime-sized blocks with sums divisible by  $p$ . Applying the induction hypothesis to the block sums divided by  $p$  selects enough blocks whose union has size  $n$  and total sum divisible by  $n$ .

**theorem** *erdos\_ginzburg\_ziv\_exact:*

**assumes**  $n\_pos: 0 < n$

**assumes**  $size\_M: size\ M = 2 * n - 1$

**shows**  $\exists N. N \subseteq\# M \wedge size\ N = n \wedge sum\_mset\ N\ mod\ int\ n = 0$

*<proof>*

### 5.3 The monotone cardinality form

**theorem** *erdos\_ginzburg\_ziv:*

**assumes**  $n\_pos: 0 < n$

```

assumes size_M: size M ≥ 2 * n - 1
shows ∃ N. N ⊆# M ∧ size N = n ∧ sum_mset N mod int n = 0
⟨proof⟩

end
theory Erdos_Ginzburg_Ziv_Outline
  imports
    Erdos_Ginzburg_Ziv
begin

```

## 6 Overview

This entry formalizes the Erdős-Ginzburg-Ziv theorem for integer multisets. The development is layered as follows: the basics theory develops modular subset-sum infrastructure, the prime theory proves the prime-modulus case, and the final theory derives the full theorem for arbitrary positive moduli by strong induction.

## 7 Main results

The main exported facts are *prime\_egz*, for prime moduli, and *erdos\_ginzburg\_ziv*, for the arbitrary-modulus monotone form. The latter states that every integer multiset of size at least  $2 * n - 1$  has an  $n$ -element submultiset whose sum is divisible by  $n$ .

## 8 Proof architecture

In the prime case, either some residue already occurs  $p$  times or the residues can be sorted and paired so that the lower-to-upper gaps are all nonzero modulo  $p$ . Subset sums of those gaps then cover the entire residue system and yield the required correction term.

For composite  $n$ , write  $n = m * p$  with  $p$  prime. Repeated applications of the prime theorem produce  $2 * m - 1$  disjoint  $p$ -blocks whose sums are divisible by  $p$ ; applying the induction hypothesis to the corresponding quotients selects blocks whose union gives the desired  $n$ -element zero-sum submultiset.

**end**

## References

- [1] P. Erdős, A. Ginzburg, and A. Ziv. Theorem in the additive number theory. *Bulletin of the Research Council of Israel, Section F: Mathematics and Physics*, 10F(1):41–43, 1961. Reprint: [https://renyi.hu/~p\\_erdos/1961-25.pdf](https://renyi.hu/~p_erdos/1961-25.pdf).