OLSON, John Edward, 1937–
ADDITION THEOREMS IN ELEMENTARY ABELIAN
GROUPS.

The Ohio State University, Ph.D., 1967
Mathematics

University Microfilms, Inc., Ann Arbor, Michigan
ADDITION THEOREMS IN ELEMENTARY
ABELIAN GROUPS

DISSERTATION

Presented in Partial Fulfillment of the Requirements for
the Degree Doctor of Philosophy in the Graduate
School of The Ohio State University

By

John Edward Olson, B. S.

* * * * * * *

The Ohio State University
1967

Approved by

Hans Zassenhaus
Adviser
Department of Mathematics
ACKNOWLEDGMENT

I wish to thank Professor Henry B. Mann of the University of Wisconsin Mathematics Research Center for his guidance and encouragement.
VITA

March 26, 1937  Born - Chicago, Illinois


1960-1964 . . .  Graduate Assistant, Department of Mathematics, The Ohio State University, Columbus, Ohio

1964-1965 . . .  Graduate Assistant, Department of Mathematics, The University of Wisconsin, Madison, Wisconsin

1965-1966 . . .  Instructor, The University of Wisconsin Fox Valley Campus, Menasha, Wisconsin

FIELDS OF STUDY

Major Field: Mathematics

Studies in Algebra and Number Theory. Professors H. B. Mann and Arno Cronheim

Studies in Combinatorial Mathematics. Professor H. J. Ryser

Studies in Analysis. Professor P. V. Reichelderfer

Studies in Topology. Professors Tibor Rado and F. T. Birtel
# TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACKNOWLEDGMENT</td>
<td>ii</td>
</tr>
<tr>
<td>VITA</td>
<td>iii</td>
</tr>
<tr>
<td>INTRODUCTION</td>
<td>1</td>
</tr>
<tr>
<td>Chapter</td>
<td></td>
</tr>
<tr>
<td>I. SUMS IN THE ELEMENTARY ABELIAN GROUP OF TYPE ((p, p))</td>
<td>3</td>
</tr>
<tr>
<td>II. SUMS IN THE ELEMENTARY ABELIAN GROUP</td>
<td>14</td>
</tr>
<tr>
<td>III. SUMS MODULO (p)</td>
<td>25</td>
</tr>
<tr>
<td>REFERENCES</td>
<td>35</td>
</tr>
</tbody>
</table>
INRODUCTION

In this paper we work with an Abelian group $G$ written additively. For two non-void subsets $A$ and $B$ of $G$, define their sum $A + B$ to be the set of all sums $a + b$, $a \in A$, $b \in B$. This is clearly an associative operation. Let $-B$ denote the set of all $-b$, $b \in B$, and let $A - B$ denote the set $A + (-B)$. Let $\overline{A}$ denote the complement of $A$ in $G$. If $S$ is any finite set, denote the number of elements in $S$ by $|S|$.

We make repeated use of two well-known theorems which we now state. Proofs of both are in H. B. Mann's book [5, pp. 1-5].

THEOREM 0.1 (Cauchy, Davenport). Let $A$ and $B$ be subsets of the additive group $G$ of residue classes modulo the prime $p$. If $A + B \neq G$, then

$$|A + B| \geq |A| + |B| - 1.$$  

(1)  

Theorem 0.1, proved by Cauchy and later rediscovered by H. Davenport, has been generalized by many authors (see [1], [2], and [5]). In [7] A. G. Vosper classified those pairs $A, B$ for which equality holds in (1).
THEOREM 0.2 (Vosper). Let $A$ and $B$ be subsets of the additive group $G$ of residue classes modulo the prime $p$. Then either

$$|A + B| \geq |A| + |B|$$

or one of the following obtains:

(i) $G = A + B$

(ii) $|A| = 1$ or $|B| = 1$

(iii) $|A + B| = p - 1$ and $B = g - A$, $g \not\in A + B$

(iv) $A$ and $B$ are in arithmetic progression with the same difference. That is, there exists $d \in G$ such that

$$A = \{a, a + d, \ldots, a + md\}, \quad |A| = m + 1,$$

and

$$B = \{b, b + d, \ldots, b + nd\}, \quad |B| = n + 1.$$
CHAPTER I

SUMS IN THE ELEMENTARY ABELIAN

GROUP OF TYPE \((p, p)\)

In this chapter let \(p\) be a prime and let \(G\) be the elementary Abelian group of type \((p, p)\). A conjecture of P. Erdős states that if \(\alpha_1, \alpha_2, \ldots, \alpha_{2p-1}\) is a sequence of elements of \(G\), then some sub-sequence has sum 0. The main theorem of this chapter (Theorem 1.5) states: If \(\alpha_1, \alpha_2, \ldots, \alpha_{2p-1}\) are distinct non-zero elements of \(G\), then every element of \(G\) occurs as the sum over a subsequence of \(\alpha_1, \alpha_2, \ldots, \alpha_{2p-1}\).

We first prove some preliminary lemmas.

**Lemma 1.1.** Let \(A = \{a_0 + \lambda a \mid \lambda = 0, 1, \ldots, s\}\) be a set of residue classes modulo \(m\) with \((a, m) = 1\) and \(1 \leq s \leq m-3\). If \(A = \{b_0 + \lambda b \mid \lambda = 0, 1, \ldots, s\}\), then \(a = \pm b \pmod{m}\).

**Proof.** We may assume without loss of generality that \(a_0 = 0 \pmod{m}\) and \(a \equiv 1 \pmod{m}\). The lemma is evident if \(s = 1\); assume \(2 \leq s \leq m-3\). We have \(0 \equiv b_0 + \mu b\), for some \(0 \leq \mu \leq s\), and therefore

\[
A = \{0, 1, \ldots, s\} = \{\lambda b \mid -\mu \leq \lambda \leq s - \mu\}.
\]

Hence either \(b \in A\) or \(-b \in A\). In any case
\[ A = \{0, 1, \ldots, s\} = \{\lambda c \mid -\tau \leq \lambda \leq s - \tau\}, \]

where \(1 \leq c \leq s\) and \(c \equiv \pm b \pmod{m}\). Now if \(1 < c\), then \(s+1-c\) and \(s+2-c\) are in \(A\). But \(s+1\) and \(s+2\) are not in \(A\). Hence\(s+1-c = s+2-c = (s-\tau)c\), which is impossible. Therefore \(c = 1\) and \(b \equiv \pm 1 \pmod{m}\).

**Lemma 1.2.** Let \(a_1, a_2, \ldots, a_s\) be distinct non-zero residue classes modulo \(p\). Let \(A_0\) be a set of residue classes modulo \(p\) with \(|A_0| \geq 2\). Form the sets \(A_i = \{a_i' + \lambda a_i \mid \lambda = 0, 1, \ldots, t_i\}\) where \(1 \leq t_i\) and the \(a_i'\) are residues modulo \(p\) \((i = 1, 2, \ldots, s)\), and the set \(C = A_0 + A_1 + \ldots + A_s\).

Then
\[ |C| \geq \min \{p, \sum_{i=0}^{s} |A_i| - 2\}. \]

**Proof.** If \(s \leq 2\) or if \(t_i \geq p-2\) for some \(i\), then the lemma follows from Theorem 0.1. Assume \(s > 2\) and \(t_i \leq p-3\). If \(|A_0| \leq p-2\), then, for some \(1 \leq i \leq s\), \(A_0\) and \(A_i\) are not in arithmetic progression with the same difference; for if \(A_0\) is in arithmetic progression with difference \(d\) and \(d \neq \pm a_i\), then, by Lemma 1.1, \(A_0\) and \(A_i\) cannot be in progression with the same difference. Thus, in any case,
for some $1 \leq i \leq s$, by Theorem 0.2. We may continue this process, arriving at

$$|A_0 + A_1 + \ldots + A_k| \geq \min \{p-1, \sum_{j=0}^{k} |A_j|\}$$

where $i_0 = 0$ and $k = s-2$. By adding the two remaining sets we get

$$|C| \geq \min \{p, \sum_{i=0}^{s} |A_i| - 2\}$$

by Theorem 0.1.

**LEMMA 1.3.** Let $a_1, a_2, \ldots, a_s$ be distinct non-zero residue classes modulo $p$ ($p > 3$). If $k_1, k_2, \ldots, k_s$ are integers with $1 \leq k_i \leq p-1$ and $\sum_{i=1}^{s} k_i = 2(p-1)$, then every residue class modulo $p$ can be expressed in the form $\sum_{i=1}^{s} t_i a_i$ where $t_1, t_2, \ldots, t_s$ are integers satisfying the conditions

(i) $1 \leq t_i < k_i$ if $k_i \geq 3$,

(ii) $t_i = 0$ or $1$ if $k_i \leq 2$,

(iii) If $k_i = k_j = 2$ ($i \neq j$), then $t_i$ and $t_j$ are not both $0$,

(iv) $2 \leq \sum_{i=1}^{s} t_i \leq 2(p-2)$.

**Proof.** Arrange the notation so that $k_i \geq 3$ for $1 \leq i \leq q$, $k_i = 1$ for $q+1 \leq i \leq q+v$, and $k_i = 2$ for $q+v+1 \leq i \leq q+v+u = s$.

Set $b_i = a_{q+v+i}$ for $1 \leq i \leq u$ and set $b = \sum_{i=1}^{u} b_i$. Let
\[ A_0 = \begin{cases} 
\{0\} & \text{if } u = 0 \\
\{b, b-b_1, \ldots, b-b_u\} & \text{if } u > 0
\end{cases} \]

\[ A_i = \begin{cases} 
\{a_i, 2a_i, \ldots, (k_i-1)a_i\} & \text{if } 1 \leq i \leq q \\
\{0, a_i\} & \text{if } q+1 \leq i \leq q+v.
\end{cases} \]

Let \( S \) be the set of all sums \( \sum_{i=1}^{s} t_i a_i \) where the \( t_i \) satisfy the conditions (i), (ii), and (iii). Clearly

\[ S = A_0 + A_1 + \ldots + A_{q+v}. \]

We have

\[ \sum_{i=1}^{q} k_i + 2u + v = 2(p-1) \]

and

\[ q + u + v = s \leq p - 1. \]

We show first that \( |S| = p \).

**Case 1.** \( u = 0. \)

In this case we have, by Lemma 1.2, that either \( |S| = p \) or

\[ |S| \geq \sum_{i=1}^{q+v} |A_i| - 2 = \sum_{i=1}^{q} k_i - q + 2v - 2 \]

\[ = 2p - 4 - q + v \]

\[ \geq 2q + 2v - 2. \]
Thus if either $2p-4-q+v \geq p$ or $2q+2v-2 \geq p$ we are done. Hence we may assume that $2p-4-q+v \leq p-1$ and $2q+2v-2 \leq p-1$. Summing these two inequalities, we get

$$q + 3v \leq 4.$$  

Hence either $q \leq 1$ or $v = 0$ and $2 \leq q \leq 4$. The first possibility does not occur since (1) and (2) are incompatible with $u = 0$, $q \leq 1$. For $v = 0$ and $3 \leq q \leq 4$ we can arrange the notation so that $a_1 \neq \pm a_2$ and (in case $q = 4$) so that also $a_3 \neq \pm a_4$. Thus, for $v = 0$ and $2 \leq q \leq 4$, we have by Lemma 1.1 and Theorems 0.1 and 0.2 that either $|S| = p$ or

$$|S| \geq \sum_{i=1}^{q} |A_i| - 1 = 2p - q - 3$$

$$\geq 2q - 1.$$  

As before we may assume $2p-q-3 \leq p-1$ and $2q-1 \leq p-1$. But these inequalities give $p < 5$ which is a contradiction.

**Case 2.** $u \geq 1$.

In this case we have, by Lemma 1.2, either $|S| = p$ or

$$|S| \geq \sum_{i=0}^{q+v} |A_i| - 2 = \sum k_i - q + u + 1 + 2v - 2$$

$$= 2p - q - u + v - 3$$

$$\geq 2q + u + 2v - 1.$$  

As before, we may assume that $2p-q-u+v-3 \leq p-1$ and $2q+u+2v-1 \leq p-1$.  

Summing the inequalities, we get

\[ q + 3v \leq 2. \]

If \( q = 0 \) and \( v = 0 \), then \( |S| = |A_0| = u+1 = p \). If \( v = 0 \) and \( q = 1 \), then, by Theorem 0.1, either \( |S| = p \) or

\[
|S| \geq |A_0| + |A_1| - 1 = u + 1 + k_1 - 2
\]

\[
= 2p - u - 3
\]

\[ \geq p. \]

The only remaining case is \( v = 0, q = 2 \). If \( A_0 \) is in arithmetic progression, then the difference must be \( \pm b_i \), for some \( i \). Hence either \( A_0, A_1 \) or \( A_0, A_2 \) are not in progression with the same difference. Moreover, by (1) and (2), we have \( u \leq p-4 \). Thus by Theorems 0.1 and 0.2, either \( |S| = p \) or

\[
|S| = |A_0| + |A_1| + |A_2| - 1
\]

\[
= k_1 + k_2 + u - 2
\]

\[
= 2p - u - 4 \geq p.
\]

Note that condition (iv) is satisfied if \( u \geq 1, q + u - 1 \geq 2 \) or if \( u = 0, q \geq 2 \). Thus, by (1) and (2), we need only account for the case \( u = 1, q = 1 \). For \( u = q = 1 \) let

\[ S' = \{b\} + A_1 + \ldots + A_{q+v}. \]

By Lemma 1.2, either \( |S'| = p \) or
\[ |S'| \geq \sum_{i=1}^{q+v} |A_i| - 2 = k_1 - 1 + 2v - 2 \]
\[ = 2p - 2u + v - 5 \]
\[ = 2p + v - 7. \]

By (1), we have \( v \geq p - 3 \). Hence \( |S'| = p \) and condition (iv) is satisfied.

**Lemma 1.4.** Let \( S = \{a_1, a_2, \ldots, a_r\} \) be a set of \( r \) distinct residue classes modulo \( p \). For \( 1 < t < r \), denote
\[ S_t = \{a_{i_1} + a_{i_2} + \ldots + a_{i_t} \mid 1 \leq i_1 < i_2 < \ldots < i_t \leq r \}. \]

Then \( |S_t| \geq r \).

**Proof.** The lemma is clear if \( t = 1 \) or if \( r = p \). Assume \( r \leq p-1 \).

If \( t = 2 \), we assume that \( a_1 = 0, a_2 = 1, \) and \( 0 < 1 < a_3 < \ldots < a_r < p \).

Clearly \( 0+a_1, 0+a_3, \ldots, 0+a_r, 1+a_r \) are distinct modulo \( p \), and hence \( |S_2| \geq r \).

It follows that the lemma is true for all \( t \) and \( r \) such that \( 1 \leq t < r \leq 5 \), for clearly \( |S_t| = |S_{r-t}| \) if \( 1 \leq t \leq \frac{r}{2} \). Assume \( t \geq 3 \), \( r \geq 6 \), and that the lemma is true for all smaller values of \( t \). We may assume that \( t < r-1 \), since \( |S_{r-1}| = |S_1| = r \). Since \( r \geq 6 \) we may rearrange the \( a_i \) so that \( \{a_1, a_2, a_3\} \) is not in arithmetic progression. Thus \( A = \{a_1 + a_2, a_2 + a_3, a_1 + a_3\} \) is also not in arithmetic progression. Set \( S^* = \{a_4, a_5, \ldots, a_r\} \). By induction \( |S^*_{t-2}| \geq r - 3 \). Hence, by Theorem 0.2,
\[ |A + S_{t-2}^*| \geq \min \{p-1, r\} = r. \]

Since \( S_t \supseteq A + S_{t-2}^* \), it follows that \( |S_t| \geq r \).

**THEOREM 1.5.** Let \( G \) be the elementary Abelian group of type \((p, p)\). If \( S \) is any set of \( 2p-1 \) non-zero elements of \( G \), then every element of \( G \) can be expressed as the sum over some subset of \( S \).

Moreover, if \( p > 3 \), then every element \( \alpha \in G \) is the sum over some subset \( T_\alpha \) of \( S \) of size \( 1 < |T_\alpha| < 2p-2 \).

**Proof.** The theorem is trivial if \( p \leq 3 \); assume \( p \geq 5 \). We shall write the elements of \( G \) as ordered pairs \((a, b)\) of residues modulo \( p \) with coordinate-wise addition.

Since \( |S| = 2p-1 \), \( S \) cannot contain two members of each of the \( p+1 \) subgroups of \( G \) of order \( p \). Hence, without loss of generality, we may assume that the residue 0 occurs at most once as a first entry in the pairs of \( S \). Let \( a_1, a_2, \ldots, a_s \) be the distinct non-zero first entries that occur in the pairs of \( S \). Let \( k_i \) be the number of appearances of \( a_i \) \((i = 1, \ldots, s)\). Thus \( \sum_{i=1}^{s} k_i \geq 2p-2 \), and \( 1 \leq k_i \leq p \). Set

\[ B_i = \{ b \mid (a_i, b) \in S \} \]

Clearly \( |B_i| = k_i \).

**Case 1.** Assume \( k_i \leq p-1 \), for \( i = 1, \ldots, s \).

Let \((x, y)\) be an arbitrary element of \( G \). By Lemma 1.3 we have
\[ x = \sum_{i=1}^{s} t_i a_i \]

where

(3) \[ 1 \leq t_i < k_i \text{ if } k_i \geq 3 , \]

(4) \[ t_i = 0 \text{ or } 1 \text{ if } k_i \leq 2 , \]

(5) \[ k_i = k_j = 2 \ (i \neq j) \text{ implies } t_i, t_j \text{ not both } 0 , \]

and

(6) \[ 2 \leq \sum_{i=1}^{s} t_i \leq \sum_{i=1}^{s} k_i - 2 . \]

Arrange the subscripts so that \( t_i \geq 1 \) if \( 1 \leq i \leq k \) and \( t_i = 0 \) if \( i > k \).

Thus

\[ x = \sum_{i=1}^{k} t_i a_i . \]

By (3), (4), and (5) we have

\[ \sum_{i=k+1}^{s} k_i \leq s-k+1 \leq p-k , \]

and hence

\[ \sum_{i=1}^{k} k_i \geq \begin{cases} p+k-1 & \text{if } \sum_{i=1}^{s} k_i = 2p-1 \\ p+k-2 & \text{if } \sum_{i=1}^{s} k_i = 2p-2 . \end{cases} \]

For each \( 1 \leq i \leq k \) let \( E_i \) be the set of sums of exactly \( t_i \) elements
from the set $B_i$. By Lemma 1.4, we have

$$|E_i| \geq k_i.$$  

If $(0,b)$ occurs in $S$, let $E_0 = \{0,b\}$. Set

$$D = \begin{cases} E_1 + \ldots + E_k & \text{if } (0,b) \notin S \\ E_0 + E_1 + \ldots + E_k & \text{if } (0,b) \in S. \end{cases}$$

It suffices to show that $y \in D$, for then $(x,y)$ is the sum of $r$ elements of $S$, where, by (6), $1 < r < 2p-2$.

If $(0,b) \notin S$, then $\sum_{i=1}^{s} k_i = 2p-1$ and $\sum_{i=1}^{k} |E_i| \geq \sum_{i=1}^{k} k_i \geq p+k-1$.

If $(0,b) \in S$, then $\sum_{i=1}^{k} k_i = 2p-2$ and $\sum_{i=0}^{k} |E_i| \geq p+k$. In either case, we have $|D| = p$ by Theorem 0.1, and therefore $y \in D$.

**Case 2.** $k_i = p$ for some $i$.

We may assume that $k_1 = p$. Thus

$$S_1 = \{(a_1,0), (a_1,1), \ldots, (a_1,p-1)\} \subset S.$$  

Clearly every element of $G$ of the form $(x,y)$, $x \neq 0$ is a sum over a subset of $S_1$. Let $(a,b) \in S$, $a \neq 0$. Then every element of $G$ is a sum over a subset of $S_1 \cup \{(a,b)\}$. Since $|S| > p+1$, it follows that every element $a$ of $G$ is a sum over some subset $T_\alpha$ of $S$ where $1 < |T_\alpha| \leq p+2$. This completes the proof of the theorem.

**COROLLARY 1.5.1.** If $p > 2$ and $S$ is a subset of $G$ of size $|S| = 2(p-1)$, then $0$ occurs as the sum over some subset of $S$. 

Proof. This is easy to verify if \( p = 3 \). Assume \( p > 3 \). Let \( \alpha \) be the sum over \( S \). If \( 0 \) does not occur as a sum, then the set \( S^* = S \cup \{\alpha\} \) consists of \( 2p-1 \) non-zero elements. It follows also that \( \alpha \) cannot be written as the sum of \( r \) elements of \( S^* \) if \( 1 < r < 2p-2 \), but this contradicts Theorem 1.5.

It may be conjectured that, in Theorem 1.5, if \( p > 3 \) and \( |S| = 2p-2 \), then every element of \( G \) occurs as the sum over some subset of \( S \). The size of \( S \) cannot be further reduced, however, as shown by the following example. For any prime \( p > 3 \) let \( S \) consist of the \( 2p-3 \) elements

\[
(1,1), (2,2), \ldots, (p-1,p-1), (0,1), (1,2), \ldots, (p-3,p-2).
\]

Elements of the form \( (x,x-1) \) do not occur as sums over subsets of \( S \), hence the sums miss the complete coset

\[
(0,-1) + (x,x).
\]
CHAPTER II

SUMS IN THE ELEMENTARY ABELIAN GROUP

This chapter is devoted to theorems similar to Theorem 1.5 for sums over subsequences of a sequence in an elementary Abelian group.

THEOREM 2.1 (Mann). Let \( a_1, a_2, \ldots, a_{p-1+k} \) be a sequence of elements from the group \( G \) of prime order \( p \) such that no element is repeated more than \( k \) times. If \( b \in G \), then

\[ b = a_{i_1} + a_{i_2} + \ldots + a_{i_k}, \]

for some \( 1 \leq i_1 < \ldots < i_k \leq p+k-1 \).

Proof. We may distribute the terms \( a_i \) into \( k \) non-empty sets \( A_1, \ldots, A_k \). By Theorem 0.1 we have

\[ |A_1 + \ldots + A_k| \geq \sum_{i=1}^{k} |A_i| - (k-1) = p, \]

which proves the theorem.

THEOREM 2.2 (Erdős, Ginzburg, Ziv). Let \( a_1, a_2, \ldots, a_{2p-1} \) be a sequence of elements from the group \( G \) of order \( p \), then

\[ 0 = a_{i_1} + a_{i_2} + \ldots + a_{i_p}, \]

for some \( 1 \leq i_1 < \ldots < i_p \leq 2p-1 \).
for some \( 1 \leq i_1 < \ldots < i_p \leq 2p-1 \).

**Proof.** If an element occurs \( p \) or more times in the sequence, then the theorem is clear. Otherwise, the theorem follows from Theorem 2.1 with \( k = p \).

By a straightforward induction argument on the group order, Erdős, Ginzburg, and Ziv in [3] extend Theorem 2.2 to finite solvable groups:

If \( G \) is a solvable group of order \( n \) (written additively) and \( a_1, a_2, \ldots, a_{2n-1} \) is a sequence of elements of \( G \), then

\[
0 = a_{i_1} + a_{i_2} + \ldots + a_{i_n},
\]

for some \( 1 \leq i_1 < \ldots < i_n \leq 2n-1 \).

Another consequence of Theorem 2.2 is the following special case of the conjecture stated in Chapter I: If \( \alpha_1, \alpha_2, \ldots, \alpha_{2p-1} \) is a sequence of elements from the elementary Abelian group \( G \) of type \((p,p)\) and if all of the \( \alpha_i \) lie in the same coset of a proper subgroup, then some subsequence has sum 0.

We now introduce some notation. If \( \alpha_1, \ldots, \alpha_s \) are group elements, let

\[
S(\alpha_1, \alpha_2, \ldots, \alpha_s)
\]

denote the set of all sums \( \sum_{i=1}^{s} \epsilon_i \alpha_i \), where the \( \epsilon_i \) are the integers 0 or 1, but not all \( \epsilon_i = 0 \).
LEMMA 2.3. Let $a_1, a_2, \ldots, a_s$ be a sequence of non-zero elements from the group $G$ of prime order $p$.

(i) If $s > p-1$, then $S(a_1, a_2, \ldots, a_s)$ contains all non-zero elements of $G$.

(ii) If $s > p$, then $S(a_1, a_2, \ldots, a_s) = G$.

Proof. Apply Theorem 0.1 to the sum $T = \{0, a_1\} + \ldots + \{0, a_s\}$ to get $|T| = p$. This proves (i) and (ii) follows from (i).

THEOREM 2.4. Let $\alpha_1, \alpha_2, \ldots, \alpha_s$ be a sequence of non-zero elements from the elementary Abelian group $G$ of type $(p, p)$.

(i) If $s > 2(p-1)$, then $S(\alpha_1, \alpha_2, \ldots, \alpha_s)$ includes a coset $\beta + P$ where $P$ is a subgroup of order $p$.

(ii) If $s > 3(p-1)$ and each proper subgroup of $G$ contains at most $s - (p-1)$ of the terms $\alpha_1$, then $S(\alpha_1, \alpha_2, \ldots, \alpha_s) = G$.

Proof. To prove (i), let $Q$ be a subgroup of order $p$ which contains the maximal number $k$ of the terms $\alpha_1$. If $k \geq p$, then (i) follows by Lemma 2.3. Assume that $k \leq p-1$, and rearrange terms so that

$$\alpha_1 \notin Q, \quad 1 \leq i \leq p-1;$$

$$\alpha_i \in Q, \quad p-1 < i \leq p-1 + k;$$

$$\alpha_i \notin Q, \quad p-1 + k < i.$$
If \( p \leq r \), then at least \( p-1 \) of the terms \( \alpha_1, \ldots, \alpha_{r-1} \) are not in the subgroup \( (\alpha_r) \) generated by \( \alpha_r \). Hence (by applying Lemma 2.3 to the factor group \( G/(\alpha_r) \)) we have that for \( r \geq p \), \( S(\alpha_1, \alpha_2, \ldots, \alpha_{r-1}) \) contains at least one element from each of the \( p-1 \) cosets \( \beta + (\alpha_r) \), \( \beta \neq (\alpha_r) \), of \( (\alpha_r) \) in \( G \). Therefore

\[
(1) \quad |S(\alpha_1, \alpha_2, \ldots, \alpha_{p-1})| \geq p-1 ,
\]

and either

\[
(2) \quad S(\alpha_1, \alpha_2, \ldots, \alpha_r) \text{ includes a complete coset of } (\alpha_r), \text{ for some } p \leq r \leq 2(p-1),
\]

or

\[
(3) \quad |S(\alpha_1, \alpha_2, \ldots, \alpha_r)| \geq |S(\alpha_1, \alpha_2, \ldots, \alpha_{r-1})| + p ,
\]

for all \( p \leq r \leq 2(p-1) \).

If (2) holds we are done. Otherwise (by (1) and (3)) we have

\[
|S(\alpha_1, \alpha_2, \ldots, \alpha_{2(p-1)})| \geq p^2 - 1 .
\]

But this implies (i).

To prove (ii), assume first that some subgroup \( P \) of order \( p \) contains \( p \) or more of the terms \( \alpha_i \). By hypothesis, at least \( p-1 \) of the \( \alpha_i \) are not in \( P \). Rearrange terms so that

\[
\alpha_i \in P, \quad 1 \leq i \leq p ;
\]

\[
\alpha_i \notin P, \quad p < i \leq 2p-1 .
\]
By Lemma 2.3, $S(\alpha_1, \alpha_2, \ldots, \alpha_p) = P$ and $S(\alpha_{p+1}, \alpha_{p+2}, \ldots, \alpha_{2p-1})$ contains at least one element from each coset $\beta + P$, $\beta \neq P$. It follows that $S(\alpha_1, \alpha_2, \ldots, \alpha_{2p-1}) = G$.

Assume now that each proper subgroup of $G$ contains at most $p-1$ of the terms $\alpha_1$. We may assume also that $p \geq 3$; for if $p = 2$, then $\alpha_1, \alpha_2, \alpha_3$ are distinct and $\alpha_1 + \alpha_2 + \alpha_3 = 0$.

We show next that the terms may be so rearranged that there exist integers $v$ and $w$ and subgroups $V$ and $W$ of order $p$ such that

$1 \leq v \leq \frac{1}{2}(p-1)$ and $1 \leq w \leq \frac{1}{2}(p-1)$ ;

$\alpha_1 \not\in V$, $1 \leq i \leq p-1$ ;

$\alpha_1 \in V$, $p \leq i \leq p-1 + v$ ;

$\alpha_1 \in W$, $2p-1-w \leq i \leq 2(p-1)$ ;

$\alpha_1 \not\in W$, $2p-1 \leq i \leq 3(p-1)$ ;

and

For each proper subgroup $P$ of $G$, at least $p-1$ of the terms $\alpha_1, \ldots, \alpha_{p-1+v}$ are not in $P$ and at least $p-1$ of the terms $\alpha_{2p-1-w}, \ldots, \alpha_3(p-1)$ are not in $P$.

Since no proper subgroup contains more than $p-1$ of the $\alpha_i$, we may rearrange terms so that each proper subgroup contains at most $\frac{1}{2}(p-1)$
of the $\alpha_i$ $(1 \leq i \leq \frac{3}{2}(p-1))$ and at most $\frac{1}{2}(p-1)$ of the $\alpha_i$ $(\frac{3}{2}(p-1) < i \leq 3(p-1))$. Let $V$ be a subgroup of order $p$ which contains exactly $v$ of the $\alpha_i$ $(1 \leq i \leq \frac{3}{2}(p-1))$ with $v$ maximal. Since $1 \leq v \leq \frac{1}{2}(p-1)$, at least $p-1$ of the $\alpha_i$ $(1 \leq i \leq \frac{3}{2}(p-1))$ are not in $V$. Hence we may rearrange the $\alpha_i$ $(1 \leq i \leq \frac{3}{2}(p-1))$ so that (5) and (6) hold. Similarly, by choosing $W$ to contain exactly $w$ of the terms $\alpha_i$ $(\frac{3}{2}(p-1) < i \leq 3(p-1))$ with $w$ maximal, we may rearrange terms so that (7) and (8) hold. Statement (9) follows by the maximality of $v$ and $w$.

If $p \leq r \leq 2(p-1)$, then (by (5), (6), and (9)) at least $p-1$ of the terms $\alpha_1, \ldots, \alpha_{r-1}$ are not in $(\alpha_r)$ and hence, by Lemma 2.3, $S(\alpha_1, \ldots, \alpha_{r-1})$ contains at least one element from each of the cosets $\beta + (\alpha_r)$, $\beta \notin (\alpha_r)$, of $(\alpha_r)$ in $G$. Therefore

\begin{equation}
|S(\alpha_1, \alpha_2, \ldots, \alpha_{p-1})| \geq p-1,
\end{equation}

and either

\begin{equation}
S(\alpha_1, \alpha_2, \ldots, \alpha_{r-1}) \text{ includes a complete coset of } (\alpha_r), \text{ for some } p \leq r \leq 2(p-1),
\end{equation}

or

\begin{equation}
|S(\alpha_1, \alpha_2, \ldots, \alpha_r)| \geq |S(\alpha_1, \alpha_2, \ldots, \alpha_{r-1})| + p,
\end{equation}

for all $p \leq r \leq 2(p-1)$.

If (12) holds, then

\begin{equation}
|S(\alpha_1, \alpha_2, \ldots, \alpha_{2(p-1)})| \geq p^2 - 1.
\end{equation}
Hence, in any case, there exists an \( r \) (\( p \leq r \leq 2(p-1) \)) and \( \beta \in G \) such that

\[
S(\alpha_1, \alpha_2, \ldots, \alpha_r) \supseteq \beta + (\alpha_r).
\]

Since \( r \leq 2(p-1) \) it follows (by (7), (8), and (9)) that at least \( p-1 \) of the \( \alpha_{r+1}, \ldots, \alpha_{3(p-1)} \) are not in \( (\alpha_r) \). Hence, by Lemma 2.3, every coset \( \gamma + (\alpha_r), \gamma \not\in (\alpha_r) \), contains an element of \( S(\alpha_{r+1}, \ldots, \alpha_{3(p-1)}) \).

Combining this with (14), we have that \( S(\alpha_1, \alpha_2, \ldots, \alpha_{3(p-1)}) \) includes every coset of \( (\alpha_r) \) in \( G \). This proves (ii).

COROLLARY 2.4.1. If \( \alpha_1, \alpha_2, \ldots, \alpha_{3(p-1)} \) is a sequence of non-zero elements from the elementary Abelian group \( G \) of type \( (p, p) \), then \( S(\alpha_1, \alpha_2, \ldots, \alpha_{3(p-1)}) \) includes a subgroup of \( G \) of order \( p \) (and hence \( 0 \in S(\alpha_1, \alpha_2, \ldots, \alpha_{3(p-1)}) \)).

Proof. If some subgroup \( P \) of \( G \) of order \( p \) contains \( p \) (or more) of the terms \( \alpha_1 \), then \( S(\alpha_1, \alpha_2, \ldots, \alpha_{3(p-1)}) \supseteq P \) by Lemma 2.3. Otherwise, by Theorem 2.4, \( S(\alpha_1, \alpha_2, \ldots, \alpha_{3(p-1)}) = G \).

We now extend Theorem 2.4 to elementary Abelian groups of order \( p^n \).

THEOREM 2.5. Let \( \alpha_1, \alpha_2, \ldots, \alpha_s \) be a sequence of non-zero elements from the elementary Abelian group of order \( p^n \) (\( n \geq 2 \)).

(i) If \( s \geq 2^{n-1}(p-1) \), then \( S(\alpha_1, \alpha_2, \ldots, \alpha_s) \) includes a coset \( \beta + P \)

where \( P \) is a subgroup of order \( p \).
(ii) If \( s > (2^{n-1})(p-1) \) and each proper subgroup of \( G \) contains at most \( s - (2^{n-1}-1)(p-1) \) of the terms \( \alpha_i \), then \( S(\alpha_1, \alpha_2, \ldots, \alpha_s) = G \).

Proof. For \( n = 2 \) the theorem is identical with Theorem 2.4.

We proceed by induction on \( n \). Assume that \( n > 2 \) and the theorem is true for \( n-1 \).

Statement (i) is clear (by Lemma 2.3) if \( p \) or more of the \( \alpha_i \) lie in a subgroup of order \( p \) and follows (by induction) if \( 2^{n-2}(p-1) \) or more of the \( \alpha_i \) lie in a proper subgroup of \( G \). We may assume, therefore, that each proper subgroup contains at most \( 2^{n-2}(p-1) \) of the \( \alpha_i \) and that each subgroup of order \( p \) contains at most \( p-1 \) of the \( \alpha_i \).

Let \( P \) be a subgroup of order \( p \) which contains the maximal number \( k \) of the \( \alpha_i \), and rearrange terms so that

\[
\alpha_i \notin P, \quad 1 \leq i \leq (2^{n-1}-1)(p-1);
\]
\[
\alpha_i \in P, \quad (2^{n-1}-1)(p-1) < i \leq (2^{n-1}-1)(p-1) + k;
\]
\[
\alpha_i \notin P, \quad (2^{n-1}-1)(p-1) + k < i \leq 2^{n-1}(p-1).
\]

Let \( (2^{n-1}-1)(p-1) < r \leq 2^{n-1}(p-1) \). Then at least \( (2^{n-1}-1)(p-1) \) of the terms \( \alpha_1, \ldots, \alpha_{r-1} \) are not in \( (\alpha_r) \). Since each proper subgroup contains at most \( 2^{n-2}(p-1) \) of the \( \alpha_i \), we may apply statement (ii) of the theorem (at stage \( n-1 \)) to the factor group \( G/(\alpha_r) \) to conclude that \( S(\alpha_1, \ldots, \alpha_{r-1}) \) contains at least one element from each coset of \( (\alpha_r) \) in \( G \). Thus either \( S(\alpha_1, \ldots, \alpha_{r-1}) \) includes a complete coset of \( (\alpha_r) \) for some \( (2^{n-1}-1)(p-1) < r \leq 2^{n-1}(p-1) \) or \( S(\alpha_1, \ldots, \alpha_s) = G \). This
proves (i).

We divide the proof of (ii) into three cases.

**Case 1.** Some subgroup $P$ of order $p$ contains $p$ or more of the $\alpha_i$.

Rearrange terms so that

$$\alpha_1, \ldots, \alpha_t \notin P$$

$$\alpha_{t+1}, \ldots, \alpha_s \in P.$$  

By hypothesis $s - t \leq s - \left(2^{n-1} - 1\right)(p-1)$ and therefore

$$t \geq \left(2^{n-1} - 1\right)(p-1)$$

If $H$ is a proper subgroup of $G$ which includes $P$, then $H \cap \overline{P}$ contains at most

$$s - \left(2^{n-1} - 1\right)(p-1) - (s-t) = t - \left(2^{n-1} - 1\right)(p-1)$$

$$< t - \left(2^{n-2} - 1\right)(p-1)$$

of the $\alpha_i$. Thus we may apply the theorem (statement (ii) at stage $n-1$) to the factor group $G/P$ to conclude that $S(\alpha_1, \ldots, \alpha_t)$ contains at least one element from each coset of $P$ in $G$. Since $S(\alpha_{t+1}, \ldots, \alpha_s) = P$, it follows that $S(\alpha_1, \alpha_2, \ldots, \alpha_s) = G$.

**Case 2.** Some proper subgroup $H$ of $G$ contains $2^{n-2}(p-1)$ or more of the $\alpha_i$, but each subgroup of $G$ of order $p$ contains at most $p-1$ of the $\alpha_i$.

Rearrange terms so that $\alpha_{t+1}, \ldots, \alpha_s \in H$ where
\[ s-t = 2^{n-2}(p-1) . \]

By statement (i) (at stage \( n-1 \)), \( S(\alpha_{t+1}, \ldots, \alpha_s) \) includes a complete coset \( \beta + P \) of some subgroup \( P \) of \( H \) of order \( p \). Therefore it suffices to show that \( S(\alpha_1, \ldots, \alpha_t) \) contains an element from each coset of \( P \) in \( G \). We may assume that

\[ \alpha_1, \ldots, \alpha_u \notin P \]

\[ \alpha_{u+1}, \ldots, \alpha_t \in P \]

where \( 0 \leq t-u \leq p-1 \). By hypothesis \( s-u \leq s-(2^{n-1}-1)(p-1) \) and therefore

\[ u \geq (2^{n-1}-1)(p-1) . \]

If \( K \) is any proper subgroup of \( G \) which includes \( P \), then \( K \cap \overline{P} \)

contains at most

\[ s-(t-u)-(2^{n-1}-1)(p-1) = u - (2^{n-2}-1)(p-1) \]

of the terms \( \alpha_i \). Hence we may apply the theorem (statement (ii) at stage \( n-1 \)) to the factor group \( G/P \) to conclude that \( S(\alpha_1, \ldots, \alpha_u) \)

contains an element from each coset of \( P \) in \( G \).

**Case 3.** Each subgroup of order \( p \) contains at most \( p-1 \) of the \( \alpha_i \) and each proper subgroup of \( G \) contains at most \( 2^{n-2}(p-1) \) of the \( \alpha_i \).

We may assume that \( s = (2^{n-1})(p-1) \). If \( p = 2 \), then the \( \alpha_i \)

account for all non-zero elements of \( G \) and \( 0 = \sum_{i=1}^{s} \alpha_i \). Assume that \( p \geq 3 \). As in the proof of Theorem 2.4, the terms may be rearranged so
that if

\[(15) \quad (2^{n-1}-1)(p-1) < r \leq 2^{n-1}(p-1), \]

then at least \((2^{n-1}-1)(p-1)\) of the terms \(\alpha_1, \ldots, \alpha_{r-1}\) are not in \((\alpha_r)\)
and at least \((2^{n-1}-1)(p-1)\) of the terms \(\alpha_{r+1}, \ldots, \alpha_s\) are not in \((\alpha_r)\).

Therefore, if \(r\) satisfies \((15)\), we have, by the theorem applied to \(G/(\alpha_r)\), that each coset of \((\alpha_r)\) in \(G\) contains an element in \(S(\alpha_1, \ldots, \alpha_{r-1})\) and an element in \(S(\alpha_{r+1}, \ldots, \alpha_s)\). It follows (as in the proof of Theorem 2.4) that

\[S(\alpha_1, \ldots, \alpha_r) \supseteq \beta + (\alpha_r),\]

for some \(\beta \in G\) and some \(r\) satisfying \((15)\). Hence \(S(\alpha_1, \alpha_2, \ldots, \alpha_s) = G\).

By Corollary 2.4.1, Theorem 2.5, and an easy induction on \(n\) we have

**COROLLARY 2.5.1.** If \(\alpha_1, \alpha_2, \ldots, \alpha_s\) is a sequence of non-zero elements from the elementary Abelian group \(G\) of order \(p^n\) \((n \geq 2)\) with \(s > (2^{n-1})(p-1)\), then \(S(\alpha_1, \alpha_2, \ldots, \alpha_s)\) includes a proper subgroup of \(G\) of order \(p\) (and hence \(0 \in S(\alpha_1, \alpha_2, \ldots, \alpha_s)\)).

Theorem 2.5 and Corollary 2.5.1 say nothing of interest if \(p = 2\).

We may think of the elementary Abelian group \(G\) of order \(2^n\) as an \(n\)-dimensional vector space over the field \(\mathbb{F}(2)\). Therefore if \(\alpha_1, \alpha_2, \ldots, \alpha_{n+1}\) are non-zero elements of \(G\), they are linearly dependent and hence \(0 \in S(\alpha_1, \alpha_2, \ldots, \alpha_{n+1})\). If, in addition, no proper subgroup of \(G\) contains all of the \(\alpha_1\), then \(S(\alpha_1, \alpha_2, \ldots, \alpha_{n+1}) = G\).
CHAPTER III

SUMS MODULO p

We now turn to the following question: If $a_1, a_2, \ldots, a_s$ are distinct non-zero residue classes modulo a prime $p$, what is the size of the sum set

$$T = \{0, a_1\} + \{0, a_2\} + \ldots + \{0, a_s\}?$$

In [4] P. Erdős and H. Heilbronn show that $|T| = p$ if $s \geq 3(6p)^{1/2}$ and conjecture that $|T| = p$ if $s \geq 2p^{1/2}$. In this chapter we prove, among other things, this conjecture.

Throughout this chapter let $p$ be a fixed prime and let $G$ denote the additive group of residue classes modulo $p$. If $a_1, a_2, \ldots, a_s$ is any sequence of non-zero residue classes modulo $p$, let $T(a_1, a_2, \ldots, a_s)$ denote the sum set $\{0, a_1\} + \{0, a_2\} + \ldots + \{0, a_s\}$. Note that $0 \in T(a_1, a_2, \ldots, a_s)$ even though $0$ may have only the trivial representation.

**Lemma 3.1.** Let $a_1, a_2, \ldots, a_s$ be non-zero residue classes modulo $p$ such that $a_i \neq \pm a_j$ for $i \neq j$. If the set $X = \{0, \pm a_1, \ldots, \pm a_s\}$ is in arithmetic progression, then

$$|T(a_1, a_2, \ldots, a_s)| = \min \{p, 1 + \frac{s(s+1)}{2}\}.$$
Proof. We may assume without loss of generality that $X$ is in arithmetic progression with difference 1. Therefore we may rearrange the subscripts so that

$$a_i \equiv \pm i \pmod{p}, \quad i = 1, \ldots, s.$$ 

If $x_1, x_2, \ldots, x_s$ is any sequence of residue classes modulo $p$, then clearly

$$|T(a_1, a_2, \ldots, a_s)| = |\{x_1, x_1 + a_1\} + \ldots + \{x_s, x_s + a_s\}|.$$ 

Let

$$x_i = \begin{cases} 0 & \text{if } a_i \equiv i \pmod{p} \\ -a_i & \text{if } a_i \equiv -i \pmod{p}. \end{cases}$$

Equation (1) becomes

$$|T(a_1, a_2, \ldots, a_s)| = |\{0, 1\} + \ldots + \{0, s\}|.$$ 

Clearly $|\{0, 1\} + \ldots + \{0, s\}| = \min\{p, 1 + \frac{s(s+1)}{2}\}$, which proves the lemma.

DEFINITION. Let $B$ be a non-empty subset of $G$. Define a mapping $\lambda_B$ from $G$ into the non-negative integers by

$$\lambda_B(x) = |(x+B) \cap \overline{B}|, \quad x \in G.$$ 

Thus $\lambda_B(x)$ is the number of representations of $x$ as a difference $x = b - \overline{b}$, $b \in B$, $\overline{b} \not\in B$.

In the next lemma we list properties of the mapping $\lambda_B$. 
LEMMA 3.2. Let $B$ be a non-empty subset of $G$ of size $|B| = k$ and let $\lambda = \lambda_B$.

(i) $\lambda(0) = 0$.

(ii) $\lambda(x) = \lambda(-x)$, $x \in G$.

(iii) $\lambda(x + y) \leq \lambda(x) + \lambda(y)$, $x, y \in G$.

(iv) If $C$ is a subset of $G$ of size $|C| = t$ and $0 \not\in C$, then

$$\sum_{c \in C} \lambda(c) \geq k(t - k + 1).$$

Proof.

(i): Clear.

(ii): $\lambda(-x) = |(-x + B) \cap \overline{B}|$

$= k - |(-x + B) \cap B|$

$= k - |B \cap (x + B)|$

$= \lambda(x)$.

(iii): $\lambda(x + y) = |(x + y + B) \cap \overline{B}|$

$= |(y + B) \cap (-x + B)|$

$= |(y + B) \cap (-x + B) \cap B| + |(y + B) \cap (-x + B) \cap \overline{B}|$

$\leq |(-x + B) \cap B| + |y + B) \cap \overline{B}|$

$= |(x + B) \cap \overline{B}| + |(y + B) \cap \overline{B}|$

$= \lambda(x) + \lambda(y)$.

(iv): $\sum_{c \in C} |(c + B) \cap B| \leq \sum_{x \in G | x \neq 0} |(x + B) \cap B| = k(k - 1).$
Thus
\[
\sum_{c \in C} \lambda(c) = \sum_{c \in C} \lfloor k - |(c + B) \cap B| \rfloor \\
\geq kt - k(k - 1) \\
= k(t - k + 1).
\]

**Lemma 3.3.** Let \(A_1, A_2, \ldots, A_r\) be subsets of \(G\) of the same size \(|A_i| = m > 1\), none of which is in arithmetic progression, and such that
\[
0 \in A_i \quad \text{and} \quad -A_i = A_i.
\]
Then
\[
|A_1 + A_2 + \ldots + A_r| \geq \min \{ p, r(m + 1) - 1 \}.
\]

**Proof.** The lemma is clearly true for \(r = 1\). Assume \(r > 1\) and that the lemma holds for \(r - 1\). Set \(C = A_1 + A_2 + \ldots + A_r\). We may assume that \(|C| < p\). Clearly \(0 \in C\) and \(-C = C\) and hence both \(m\) and \(|C|\) are odd. Therefore \(|C| < p - 1\) and Theorem 0.2 gives
\[
|C| \geq |A_1 + \ldots + A_{r-1}| + |A_r| \\
\geq (r-1)(m+1) - 1 + m \\
= r(m+1) - 2.
\]
But \(r(m+1) - 2\) is even hence \(|C| \geq r(m+1) - 1\).

**Lemma 3.4.** Let \(A\) and \(B\) be subsets of \(G\) of sizes \(|A| = n, |B| = k\). Assume \(0 \notin A, -A = A, \text{ and } A \cup \{0\}\) is not in arithmetic
progression. Let \( t \) be an integer, \( 1 \leq t \leq p-1 \), and set

\[
t = r(n+2) + q \quad (1 \leq q \leq n).
\]

Set \( \lambda = \lambda_B \) and

\[
\alpha = \max \{ \lambda(a) | a \in A \}.
\]

Then

\[
(2) \quad \alpha > \frac{2(n+2)k(t-k+1)}{t(t+n+6) + q(n-q-2)},
\]

and

\[
(3) \quad \alpha > \frac{8(n+2)k(t-k+1)}{4t(t+n+6) + (n-2)^2}.
\]

**Proof.** Equation (3) follows from (2) since \( q(n-q-2) \) has maximal value \( \frac{1}{4}(n-2)^2 \).

We construct a subset \( C \) of \( G \) with \( 0 \notin C \) of size \( |C| = t \) such that

\[
(4) \quad \sum_{c \in C} \lambda(c) \leq \alpha \left\{ \frac{t(t+n+6) + q(n-q-2)}{2(n+2)} \right\}.
\]

If \( t \leq n \) and therefore \( r = 0 \), \( q = t \), let \( C \) consist of \( t \) of the elements in \( A \). Thus \( \sum_{c \in C} \lambda(c) \leq \alpha t \) and (4) holds. Assume now that \( t \geq n+1 \) and therefore that \( r \geq 1 \). Let \( A^* = A \cup \{0\} \), and let

\[
C_j = \underbrace{A^* + \ldots + A^*}_{j \text{ times}}.
\]
By Lemma 3.3, $C_j$ contains at least $\min \{p, j(n+2)-1\}$ residues and hence contains at least $\min \{p-1, j(n+2)-2\}$ non-zero residues. Thus we may form a set $C$ of non-zero residues of size $t$ which contains at least $j(n+2)-2$ residues from each $C_j$ $(1 \leq j \leq r)$ and at most $q+2$ residues from $C_{r+1} \cap \overline{C_r}$. Now if $c \in C_j$, $c \neq 0$, then

$$c = a'_1 + \ldots + a'_v$$

where $a'_1, \ldots, a'_v$ are (not necessarily distinct) elements of $A$ and $1 \leq v \leq j$. Hence

$$\lambda(c) \leq \sum_{i=1}^{v} \lambda(a'_i) \leq \nu \alpha \leq j \alpha ,$$

by Lemma 3.2. It follows that

$$\sum_{c \in C} \lambda(c) \leq n \alpha + (n+2)2\alpha + \ldots + (n+2)r\alpha + (q+2)(r+1)\alpha$$

$$= \frac{\alpha}{2} \left\{ r(r+1)(n+2) + 2(q+2)(r+1)-4 \right\}$$

$$= \frac{\alpha}{2} \left\{ (r+1)(t+q+4)-4 \right\}$$

$$= \alpha \left\{ \frac{t(t+n+6) + q(n-q-2)}{2(n+2)} \right\} .$$

This establishes (4).

From Lemma 3.2 we get

$$\sum_{c \in C} \lambda(c) \geq k(t-k+1) .$$

Equation (2) follows from (4) and (5).
THEOREM 3.5. Let \( a_1, a_2, \ldots, a_s \) be non-zero residue classes modulo \( p \) such that \( a_i \neq \pm a_j \) for \( i \neq j \). If

\[
\begin{cases}
  s^2 + s \leq p + 1, & s \equiv 0 \pmod{2} \\
  2s^2 + 3s \leq 2p + 5, & s \equiv 1 \pmod{2},
\end{cases}
\]

then

\[ T(a_1, a_2, \ldots, a_s) \geq 1 + \frac{s(s+1)}{2}. \]

And in any case

\[
T(a_1, a_2, \ldots, a_s) \geq \begin{cases}
  \min \left\{ \frac{p+3}{2}, 1 + \frac{s(s+1)}{2} \right\} & \text{if } s \equiv 0 \pmod{2} \\
  \min \left\{ \frac{p+3}{2}, \frac{s(s+1)}{2} \right\} & \text{if } s \equiv 1 \pmod{2},
\end{cases}
\]

Proof. Set \( B = T(a_1, a_2, \ldots, a_s) \), \( \lambda = \lambda_B \), and \( \alpha = \max \{ \lambda (a_i) \mid i = 1, \ldots, s \} \). Arrange the notation so that \( \lambda (a_s) = \alpha \).

Let \( A = \{ \pm a_1, \pm a_2, \ldots, \pm a_s \} \) and note that \( \alpha = \max \{ \lambda (a) \mid a \in A \} \). If \( s > 1 \) put \( B^* = T(a_1, a_2, \ldots, a_{s-1}) \). We show first that

\[ |B| \geq |B^*| + \alpha. \]

If \( b \in B \) and \( a_s + b \not\in B \), then clearly \( b \not\in B^* \). Hence

\[ |B| \geq |B^*| + |(a_s + B) \cap \overline{B}| \geq |B^*| + \alpha. \]

We prove the first part of the theorem by induction on \( s \). Clearly (7) holds if \( s = 1 \). Assume \( s > 1 \), \( s \) satisfies (6), and

\[ |B^*| \geq 1 + \frac{(s-1)s}{2}. \]
Because of Lemma 3.1 we may assume that $A \cup \{0\}$ is not in arithmetic progression. We show next that

$$(11) \quad |B| \geq \frac{s(s+1)}{2}.$$ 

Set $n = |A| = 2s$, $k = |B|$, and $t = 2k - 2$ in (3). We may assume that $|B| \leq \frac{s(s+1)}{2}$, and hence $t \leq p - 1$ by (6). By (3) and the inequality $k \geq 1 + \frac{(s-1)s}{2}$ we get $\alpha > s - 2$. Therefore $\alpha \geq s - 1$.

Equation (11) now follows from (9) and (10). Assume now that equality holds in (11). To prove (7) it suffices to show that $\alpha > s - 1$. We get this from (2) by setting $n = 2s$, $k = \frac{s(s+1)}{2}$,

$$t = \begin{cases} 
2s + s - 2 & \text{if } s \equiv 0 \pmod{2} \\
2s + \frac{3s-7}{2} & \text{if } s \equiv 1 \pmod{2}
\end{cases},$$

and therefore

$$q = \begin{cases} 
2s & \text{if } s \equiv 0 \pmod{2} \\
\frac{3s-5}{2} & \text{if } s \equiv 1 \pmod{2}
\end{cases}.$$ 

Statement (8) holds if $s$ satisfies (6). Let $s_0$ be the smallest positive integer which fails to satisfy (6). We are done if

$$|T(a_1, a_2, \ldots, a_{s_0})| \geq \frac{p+3}{2}.$$ 

Put $s = s_0$ and assume $|B| \leq \frac{p+1}{2}$.

By (7) we have

$$(12) \quad |B^*| \geq 1 + \frac{(s_0-1)s_0}{2}.$$
Again we may assume that $A \cup \{0\}$ is not in arithmetic progression.

Set $n = 2s$, $t = 2k - 2$ in (3). Using $k \geq 1 + \frac{(s_0 - 1)s_0}{2}$ we get

$\alpha > s_0 - 2$. Therefore $\alpha \geq s_0 - 1$ and

\begin{equation}
|T(a_1, a_2, \ldots, a_s)| \geq \frac{s_0(s_0 + 1)}{2}.
\end{equation}

If $s_0 \equiv 0 \pmod{2}$, we have $s_0(s_0 + 1) \leq p + 1$ and hence $s_0$ does not satisfy (6) contradicting the significance of $s_0$. Hence we must have

\begin{equation}
|T(a_1, a_2, \ldots, a_s)| \geq \frac{p + 3}{2}.
\end{equation}

If $s_0 \equiv 1 \pmod{2}$, we have shown that (8) holds with $s = s_0$. In this case it suffices to show

\begin{equation}
|T(a_1, a_2, \ldots, a_s)| \geq \frac{p + 3}{2}, \text{ where } s = s_0 + 1.
\end{equation}

Deny (14). Thus $k = |B| \leq \frac{p + 1}{2}$, $k \geq \frac{s(s-1)}{2}$. By setting $t = 2k - 2$, $n = 2s$ in (3) we get $\alpha > s - 3$. Hence

\begin{equation}
|T(a_1, a_2, \ldots, a_s)| \geq \frac{s(s-1)}{2} + s - 2 \geq \frac{p + 3}{2}.
\end{equation}

This completes the proof of the theorem.

**THEOREM 3.6.** Let $a_1, a_2, \ldots, a_s$ be distinct non-zero residue classes modulo $p$. If $s > (4p - 3)^{1/2}$, then every residue class $x$ can be expressed in the form

\begin{equation}
x = \epsilon_1 a_1 + \epsilon_2 a_2 + \ldots + \epsilon_s a_s,
\end{equation}

where $\epsilon_1 = 0$ or 1 but not all $\epsilon_1 = 0$. 
Proof. We give the proof for the case $s \equiv 3 \pmod{4}$; the proofs for the other three cases are similar. Put $u = \frac{s-1}{2}$, $v = \frac{s+1}{2}$, $S = T(a_1, \ldots, a_u)$, and $T = T(a_{u+1}, \ldots, a_s)$ with the notation arranged so that $a_i \neq a_j$ if either $1 \leq i < j \leq u$ or $u+1 \leq i < j \leq s$. By Theorem 3.5 we have

$$|S| \geq \min \left\{ \frac{u(u+1)}{2}, \frac{p+3}{2} \right\} \geq \frac{p+1}{2}$$

$$|T| \geq \min \left\{ 1 + \frac{v(v+1)}{2}, \frac{p+3}{2} \right\} = \frac{p+3}{2}.$$ 

Let $T'$ be the set $T$ with 0 removed. Thus by Theorem 0.1

$$|S + T'| \geq \min \{p, |S| + |T'| - 1\} = p,$$

which proves the theorem.

Following Erdős and Heilbronn [4] we remark that Theorem 3.6 is nearly best possible. If

$$a_1 = 1, a_2 = -1, a_3 = 2, \ldots, a_s = (-1)^{S-1}\left[ \frac{1}{2} (s + 1) \right]$$

and $s < 2(p^2 - 1)$, then the residue $\frac{p-1}{2}$ cannot be expressed in the form (15).
REFERENCES

1. Cauchy, A.
Recherches sur les nombres,
Jour. Ecole Polytechn. 9 (1813) 99-123.

2. Davenport, H.
On the addition of residue classes,

Theorem in the additive number theory,

4. Erdös, P. and Heilbronn, H.
On the addition of residue classes mod p,
Acta Arith. 9 (1964) 149-159.

5. Mann, H. B.
Addition Theorems,

6. Mann, H. B.
Two addition theorems,

7. Vosper, A. G.
The critical pairs of subsets in a group of prime order,