ON THE CAUCHY-DAVENPORT INEQUALITY FOR THE SUM OF SUBSETS OF A CYCLIC GROUP

by

CLAYTON HERBERT CHISUM

A THESIS

submitted to

OREGON STATE UNIVERSITY

in partial fulfillment of
the requirements for the
degree of

MASTER OF SCIENCE

June 1962

APPROVED:

Redacted for privacy

Associate Professor of Mathematics

In Charge of Major

Redacted for privacy

Chairman of Department of Mathematics

Redacted for privacy

Chairman of School Graduate Committee

Redacted for privacy

Dean of Graduate School

Date thesis is presented May 18, 1962

Typed by Jolán Erőss

TABLE OF CONTENTS

ON THE CAUCHY-DAVENPORT INEQALITY FOR THE SUM OF SUBSETS OF A CYCLIC GROUP

CHAPTER I

INTRODUCTION

In 1935 H. Davenport [6], published the following theorem on the addition of sets of residue classes.

<u>Theorem 1.1</u>: Let $a_1, a_2, \cdots, a_n$ be m different residue classes modulo a prime p, and let $b_1, b_2, \cdots, b_n$ be n different residue classes modulo p. Let $c_1, c_2, \cdots, c_\ell$ be all the different residue classes representable as $a_i + b_j$, $1 \leq i \leq m$, $1, \leq j \leq n$. Then

$$(1.1) \qquad \ell \geq m + n - 1$$

if $m + n - 1 \leq p$, otherwise $\ell = p$.

In this paper we are going to investigate some of the consequences of this publication by Davenport.

Shortly after Davenport's publication appeared, and also in 1935, I. Chowla [3] published a statement of the extension of Theorem 1.1 to the case of a composite modulus (cf. Theorem 2.1). However, the proof, which is almost identical with Davenport's proof of Theorem 1.1, did not appear until 1937 [4]. It is interesting to note that A. Cauchy ([1], [2]) had used essentially the same method to prove Theorem 1.1 in 1813 [7]. Because of these results Theorem 1.1 will be referred to as the "Cauchy-Davenport Theorem", and the extension of Theorem 1.1 to the composite modulus case will be called "Chowla's Theorem".

Since the set of all residue classes modulo an integer m forms a cycle group of order m, we may restate Theorem 1.1 in terms of subsets of a cyclic group. However, before restating the theorem we introduce some definitions.

Definition 1.1: By the symbol $[A]$ we shall mean the number of elements in the set A.

Definition 2.1: By the sum C of the sets A and B we mean

$$C = A + B = \{a+b / a \in A, b \in B\}.$$

In general, capital letters will be used to denote sets of group elements, and small letters will be used to denote the elements themselves. Unless otherwise stated, the letter C will be used to designate the sum of two sets.

Theorem 1.1 now becomes:

Theorem 1.1(a): Let G be the group of residue classes modulo a prime p, and let A, B and $C = A + B$ be subsets of G. Then

$$(1.1(a)) \qquad [C] \geq \min(p, [A] + [B] - 1) .$$

The inequality 1.1(a), with the modulus arbitrary, will be referred to as the Cauchy-Davenport inequality.

In 1952 H. B. Mann [11] published a new proof of Chowla's Theorem in which he used a transformation he had previously used to prove the famous $\alpha\beta$ Theorem of Additive Number Theory. Mann did not apply his transformation directly to Chowla's Theorem, but instead he proved Theorem 3.2 which permits him to give a non-inductive proof of Chowla's Theorem. I have applied Mann's transformation directly and obtained a new proof of the Cauchy-Davenport Theorem. Also, by combining the transformation with double induction I have obtained another proof of Chowla's Theorem. Mann [12] also uses Theorem 3.2 to prove Theorem 3.4 which is similar to Chowla's Theorem and which is true for abelian groups in general.

Since Mann was able to prove Chowla's Theorem by using his famous transformation, I considered a transformation which F. J. Dyson [8] used for an alternate proof of the $\alpha\beta$ Theorem. This resulted in a new proof of Chowla's Theorem (cf. Theorem 4.1). Using Dyson's transformation the proofs of the Cauchy-Davenport Theorem and

Chowla's Theorem are essentially the same. Also, one can use Dyson's transformation to obtain the Cauchy-Davenport inequality under several different hypotheses. This has been done by P. Scherk [14], J. H. B. Kemperman and P. Scherk [15], and the author. These theorems are presented in Chapter IV with the other work concerning Dyson's transformation.

If one experiments with the Cauchy-Davenport inequality he discovers that equality will sometimes hold, but generally there is strict inequality. Thus one is led to speculate on the nature of the sets for which equality holds. For the case of a prime modulus A. G. Vosper [16] [17] has solved this problem by characterizing the sets for which equality holds in Theorem 1.1(a). Vosper offers two proofs of his theorem. The first proof is given here in Chapter II as the proof of Theorem 2.2, and the second proof, which uses Dyson's transformation, appears as the proof of Theorem 4.5. Mann [5] has offered a somewhat simpler proof of Vosper's Theorem which uses a transformation similar to the one used to prove Theorem 3.2. Mann's proof appears as the proof at Theorem 3.8. It might be remarked that many of the original proofs are difficult to read and have been presented here in a more readable form.

Some work has been done towards extending the results for cyclic groups to the more general abelian groups. In Chapters III, IV and V I present these results.

As a final remark I present two unsolved problems. Throughout the text we give several sufficient conditions for the validity of the Cauchy-Davenport inequality, but nowhere have we stated a necessary condition when the modulus is composite. Also, we have not found a generalization of Vosper's Theorem to the case of a composite modulus.

CHAPTER II

PROOFS BY CHOWLA AND VOSPER

In this chapter we consider Chowla's generalization of the Cauchy-Davenport Theorem and Vosper's first proof of his theorem which characterizes those sets for which equality holds in the Cauchy-Davenport inequality. We consider first Chowla's theorem:

<u>Theorem 2.1</u>: Let G be the group of residue classes modulo an integer m. Let A, B and $C = A + B$ be non-empty subsets of G with $0 \in B$, and for every $b \in B$, if $b \neq 0$ then $(b,m) = 1$. Then

$$(2.1) \qquad [C] \geq \min(m, [A] + [B] - 1).$$

<u>Proof</u>: Since there is nothing to prove if $[A] + [B] - 1 \geq m$, we assume that $[A] + [B] - 1 < m$ and show that $[C] \geq [A] + [B] - 1$. We prove the theorem by induction on $[B]$. For $[B] = 1$ the assertion is trivially true. Suppose that the assertion is false for $[B] = 2$, and denote the non-zero element of B by b_1. Then $a+b_1$ must be in A for every $a \in A$. Hence, adding b_1 k times, we have $a + kb_1 \in A$ for every

natural number k. Since $(b_1, m) = 1$, $a + kb_1$ generates G, and therefore $A = G$; which contradicts the assumption that $[A] + [B] - 1 < m$. Thus the assertion is true for $[B] = 2$.

Assume that Theorem 2.1 is true if $[B] < n$ and consider the case where $[B] = n$. As before, we may assume that $[C] < m$. Then there is a residue class $d \in G$ such that $d \notin C$, and $d-b \in C$ for some $b \in B$. For if not, we apply the same argument as before and obtain $d - kb \notin C$ for any natural number k and any non-zero $b \in B$. Therefore C is empty, and we have a contradiction to the hypothesis that A and B are non-empty. We use d then to define the new sets B^*, B^{**} and C^* as

$$B^* = \{b_i \mid d-b_i \in C, \ b_i \in B\},$$

$$B^{**} = \{b_j \mid d-b_j \notin C, \ b_j \in B\},$$

and

$$C^* = \{c_i \mid c_i = d-b_i, \ b_i \in B^*\} .$$

By these definitions we immediately have that

$$[B^{**}] = [B] - [B^*] .$$

Also, since $c_i - b_j = a$, $(b_j \in B^{**}$ and $c_i \in C^*)$, implies that $a + b_j = c_i = d - b_i$, and hence that $a + b_i = d - b_j$, which is impossible since $b_j \in B^{**}$, we have that $c_i - b_j \notin A$ for any $c_i \in C^*$. We define next the set C^{**} as $C^{**} = A + B^{**}$. Then since $c_j - b_j \in A$, for $c_j \in C^{**}$ and $b_j \in B^{**}$, we have that $C^* \cap C^{**}$ is empty. Therefore

$$[C^{**}] \leq [C] - [C^*] = [C] - [B^*] .$$

Also, since $0 \in B$, we know that B^{**} is not empty. Then by the inductive hypothesis

$$\begin{aligned}[C] - [B^*] \geq [C^{**}] &\geq [A] + [B^{**}] - 1 \\ &\geq [A] + [B] - [B^*] - 1,\end{aligned}$$

or

$$[C] \geq [A] + [B] - 1,$$

which completes the proof.

If we require m to be a prime then the condition that $(b,m) = 1$ for $b \neq 0$ is automatically satisfied. Thus, to obtain the Cauchy-Davenport theorem we need only show that we may assume that $0 \in B$. This is easily accomplished, for if $0 \notin B$, form the set B' defined as

$$B' = \{b_i - b_1 \mid b_i \in B, \ i = 1, 2, \cdots, [B]\} .$$

Then $0 \in B'$, and

$$\begin{aligned}[C] = [A+B] &= [A+B'] \\ &\geq [A] + [B'] - 1 \\ &= [A] + [B] - 1,\end{aligned}$$

and we have the result. Note that when m is not a prime the above transformation may be incompatible with the hypothesis that $(b,m) = 1$.

The hypotheses of Theorem 2.1, which are due to Chowla, may be replaced by other conditions which are sufficient for the inequality 2.1. Some of these conditions are given in the following chapters.

We consider next a simple example which shown that one must add hypotheses in order to extend the Cauchy-Davenport Theorem to the case of a composite modulus.

<u>Example</u>: Let G be the group of residue classes modulo $2n$, $n \geq 2$.

Let $\qquad A = \{2k \mid k = 1, 2, \cdots, n\}$,

and $\qquad B = \{2k-1 \mid k = 1, 2, \cdots, n\}$.

Then $\qquad C = A + B = B$,

and since $\qquad [A] > 1 \quad [C] < [A] + [B] - 1$.

It is clear that equality will hold in the Cauchy-Davenport inequality for the trivial case where the min ([A], [B] = 1. The following example shows that equality will hold in less-trivial cases.

<u>Example</u>: Let G be the group of residue classes modulo a prime of the form $3n + 1$. Let $A = \{1, 4, 7, \cdots, 3n-2\}$, and let $B = \{0, 3, 6, \cdots, 3n\}$. Then

$$C = \{0, 1, 3, 4, \cdots, 3n-5, 3n-2\},$$

$$[A] = n, \ [B] = n+1 \quad \text{and} \quad [C] = 2n,$$

so that $[C] = [A] + [B] - 1.$

Since it is clear that equality will often not hold in the Cauchy-Davenport inequality, the question naturally arises as to the nature of the sets for which equality will hold. A. G. Vosper [16] has answered this question in the theorem which we consider next. Before stating Vosper's theorem we make the following definitions:

<u>Definition 1</u>: A pair of subsets (A, B) of the group of residue classes modulo a prime p is said to be a critical pair if $[C] = \min(p, [A] + [B] - 1)$.

<u>Definition 2</u>: By the difference $A-B$ of the sets A and B we mean $A-B = \{a-b \,/\, a \in A, \ b \in B\}$. The set containing the single element a will often be written as "a" instead of as $\{a\}$. Thus, in particular, $A - a_1 = \{a_i - a_1 \,/\, a_i \in A\}$.

<u>Definition 3</u>: The set A will be called a "standard" set if it can be represented as an arithmetic progression; i.e., if for some $a \in A$ and some $k \in G$ with $k \neq 0$, $A - a = \{ik \,/\, 0 \leq i \leq [A] - 1\}$. The pair (A, B) is said to be a "standard pair" if for some $a \in A$, $b \in B$ and $k \in G$ with $k \neq 0$,

$$A - a = \{ik \,/\, 0 \leq i \leq [A] - 1\},$$

and

$$B - b = \{ik \,/\, 0 \leq i \leq [B] - 1\}.$$

<u>Definition 4</u>: The complement of A in G is denoted by $\overline{A}$.

<u>Theorem 2.2</u>: Let G be the group of residue classes modulo a prime p, and let (A, B) be a pair of subsets of G. The pair (A, B) is a critical pair if and only if A and B satisfy one of the following four conditions:

(1) $[A] + [B] > p$

(2) $\min([A], [B]) = 1$

(3) $A = \overline{d-B}$ for some $d \in G$.

(4) (A, B) is a standard pair.

<u>Proof</u>: In the proof we will use the following easily verified observations:

For A, B, C and D any subsets of G, and φ the empty set:

(i) If $A-B = C-D$, then $A \cap B = \varphi$ implies $C \cap D = \varphi$.

(ii) $(A+B) \cap C = \varphi$ if and only if $A \cap (C-B) = \varphi$.

(iii) $(A-B) \cap (C+D) = \varphi$ if and only if $(A-C) \cap (B+D) = \varphi$.

We consider first the sufficiency of the four conditions. That conditions (1) and (2) are sufficient is immediate. If $A = \overline{d-B}$, for some $d \in G$, then $[A] = [\overline{d-B}] = [\overline{B}] = p - [B]$. Hence $[A] + [B] = p$. Also, $A \cap (d-B) = \varphi$, so that by (ii) $(A+B) \cap d = \varphi$. Therefore $[C] \leq p - 1 = [A] + [B] - 1$. Thus, by the Cauchy-Davenport theorem, $[C] = [A] + [B] - 1$. Therefore condition (3) is sufficient. If (A, B) is a standard pair then $A - a = \{ik \,/\, 0 \leq i \leq [A] - 1\}$ and $B - b = \{ik \,/\, 0 \leq i \leq [B] - 1\}$.

Hence,

$$(A-a) + (B-b) = \{ik \,/\, 0 \leq i \leq [A] + [B] - 2\}.$$

Since $k \neq 0$ by the definition of a standard set, k is a generator of G. Therefore

$$\begin{aligned} [C] &= [A + B] \\ &= [(A-a) + (B-b)] \\ &= [\{ik \,/\, 0 \leq i \leq [A] + [B] - 2\}] \\ &= \min(p, [A] + [B] - 1). \end{aligned}$$

For, i runs through $[A] + [B] - 1$ values, and if this number is greater than p then $C = G$. Therefore condition (4) is sufficient.

Suppose now that (A, B) is a critical pair. If $[A] + [B] > p$ we have condition (1). If $\min([A],[B])=1$ we have condition (2). If $[A] + [B] = p$ then $[C]=p-1$. Therefore $\overline{C} = d$ for some $d \in G$. Hence $(A+B) \cap d = \varphi$. Then by (ii), $A \cap (d-B) = \varphi$, so that $A \in \overline{d-B}$. But, $[A] = p - [B] = p - [d-B] = [\overline{d-B}]$. Therefore $A = \overline{d-B}$, which is condition (3). For the remainder of the proof we may assume that $2 < [A] + [B] < p$. Since we are supposing that (A, B) is a critical pair our assumption that $[A] + [B] < p$ implies that $[C] < p$. We establish the remaining condition (4) by induction, but first we prove the following four lemmas.

<u>Lemma 2.1</u>: If A is a standard set then (A, B) is a standard pair.

<u>Proof</u>: As we have shown earlier we may assume that $0 \in A$ and $0 \in B$. Therefore we may assume that $A = \{ik \,/\, 0 \leq i \leq [A] - 1\}$. Since the transformation ℓx, $\ell \not\equiv 0 \pmod p$, applied to the sets A, B and C leaves $[A]$, $[B]$ and $[C]$ unchanged, we may assume that $A = \{0, 1, 2, \cdots, [A] - 1\}$, (i.e., we may assume that $k = 1$). Denote the set of consecutive integers $m, m+1, \cdots, n$ by (m, n). The set (m, n) is said to be a "gap" in B, if for all $i \in (m, n)$, $i \notin B$. Let (r, s) be the gap of maximum length t. Then $t > [A]$, for if not $C = G$, which contradicts the hypothesis that $[C] < p$. Let $B' = B - (s+1) = \{n_i / \, 0 \leq i \leq [B]-1\}$. We will show that the n_i are consecutive, and hence that (A, B) is a standard pair. We may take $0 \leq n_i \leq n_{i+1} < p$. Since $s + 1 \in B$ we have $n_o = 0$. Since $r - 1$ is the largest $x < s$ which is in B we

have $n_{[B]-1} = p - t - 1$. Define the set A' as

$$A' = A + (p-t-1) = \{i \,/\, p-t-1 \leq i \leq p-t+[A]-2\}.$$

Since $t > [A]$ we have $p - t + [A] - 2 < p-1$. Since $n_{[B]-1} = p-t-1$ we have $A + B' \supset A' \cup B'$, and $A' \cap B' = p-t-1$.

$$\begin{aligned}[A' \cup B'] &= [A'] + [B'] - 1 \\ &= [A] + [B] - 1 \\ &= [A + B] \\ &= [A + B'].\end{aligned}$$

Hence, $A' \cup B' = A + B'$. Suppose now that $x \in B'$ for any arbitrary, but fixed x in the interval $0 \leq x < p-t-2$. Then since $1 \in A$, $x + 1 \in A + B' = A' \cup B'$, but $x + 1$ is in the interval $1 \leq x + 1 < p-t-1$, and therefore $x + 1 \in B'$. Since $n_0 = 0$, we have the n_i are consecutive, and the proof of the lemma is complete.

Corollary 1: If $[A] = 2$ or $[B] = 2$ then (A, B) is a standard pair.

Proof: If $[A] = 2$ or $[B] = 2$ then A or B is a standard set and the corollary follows from Lemma 2.1.

Lemma 2.2: If $[A] = [B] = 3$, then (A, B) is a standard pair.

Proof: Let $B = \{b_1, b_2, b_3\}$. If $[(A+b_1) \cap (A+b_2)] \leq 1$, then $[(A+b_1) \cup (A+b_2)] \geq 5 = [C]$. Therefore

$$C = ((A+b_1) \cup (A+b_2)) \supset A+b_3. \text{ Thus}$$

$$[(A+b_i) \cap (A+b_3)] \geq 2, \text{ for } i = 1 \text{ or } i = 2.$$

We may suppose that $[(A+b_1) \cap (A+b_3)] \geq 2$. Then $[(A+b_1) \cup (A+b_3)] \leq 4$. Therefore (A,B_1) is a critical pair for $B_1 = \{b_1, b_3\}$. Then (A, B_1) is a standard pair by the corollary to Lemma 2.1. Hence A is a standard set, and therefore (A, B) is a standard pair by Lemma 2.1.

Lemma 2.3: The pair $(-A, \bar{C})$ is a critical pair.

Proof: By the definition of $\bar{C}$ we have that $(A+B) \cap \bar{C} = \varphi$. Therefore, by (ii), $B \cap (\bar{C}-A) = \varphi$. Let $D = \bar{C}-A$, then $B \subset D$. Also, $D \cap (\bar{C}-A) = \varphi$, so that, by (ii), $(A+D) \cap \bar{C} = \varphi$. Therefore $A+D \subset C$. Since $B \subset D$, $A+D = C$, and hence

$$\begin{aligned}[A] + [B] - 1 &= [A+B] \\ &= [A+D] \\ &= \min (p, [A] + [B] - 1.\end{aligned}$$

Therefore $[B] = [D]$, which implies that $B = D$. Therefore $\bar{C} - A = \bar{B}$, so that $[\bar{C} - A] = P - [B]$. Since $[\bar{C}] = p - [A] - [B] + 1$, we have $p - [B] = [\bar{C}] + [A] - 1$. Therefore

$[\overline{C} - A] = \min (p, [\overline{C}] + [-A] - 1,$ and

$(\overline{C},-A)$ is a critical pair.

<u>Corollary 2</u>: If $[A] = [B] = \frac{1}{2}(p-1)$ then (A,B) is a standard pair.

<u>Proof</u>: By Lemma 2.3 $(-A, \overline{C})$ is a critical pair. Then by the corollary to Lemma 2.1 $(-A, \overline{C})$ is a standard pair if $[\overline{C}] = 2$. If $[A] = [B] = \frac{1}{2}(p-1)$ then $[A] + [B] - 1 = p-2$, and $[\overline{C}] = 2$, so that $(-A, \overline{C})$ is a standard pair. Thus $-A$, and hence A, is a standard set, so that by Lemma 2.1 (A,B) is a standard pair.

<u>Lemma 2.4</u>: If $[B] \geq [A] \geq 3$ and $[B] \geq 4$ then, unless $[A] = [B] = \frac{1}{2}(p-1)$, there are elements b_1 and b_2 in B such that

$$(C+B) \cap (\overline{C+b_1}) \cap (\overline{C+b_2}) \neq \varphi .$$

<u>Proof</u>: Form the set $C+B$. Since $[C] = [A] + [B] - 1$, we have by Theorem 2.1 that $[C+B] \geq \min (p, [A] + 2[B]-2)$. Suppose that Lemma 2.4 is false. Then the sets D_i defined by

$$D_i = (C+B) \cap (\overline{C+b_1}), \quad i = 1, 2, \cdots; [B],$$

are all disjoint. Since $(C+b_i) \subset (C+B)$, for $i = 1, 2, \cdots [B]$, we have that for each i,

$$[D_i] = [C+B] - [C+b_i]$$
$$= [C+B] - [A] - [B] + 1.$$

Also, $D_i \subset C+B$ for each i, so that

$$[\bigcup_{i=1}^{[B]} D_i] \leq [C+B] .$$

Therefore,

$$[B]([C+B] - [A] - [B] + 1) \leq [C+B],$$

or

$$(I) \quad [B]([A] + [B] - 1) \geq [C+B]([B] - 1).$$

We consider now three cases, each of which leads to a false conclusion.

<u>Case 1</u>: $p \geq [A] + 2[B] - 2$.
Then $[C+B] \geq [A] + 2[B] - 2$. Hence, by (I), $[B]([A] + [B] - 1) \geq ([A] + 2[B] - 2)([B] - 1)$. Therefore, $[B]^2 \leq 3[B] + [A] - 2 \leq 4[B] - 2$, which cannot be true since $[B] \geq 4$.

<u>Case 2</u>: $p < [A] + 2[B] - 2$ and $[A] \leq [B] - 1$.
Then $[C+B] = P$. Since $p \geq [A] + [B] + 1$, we have by (I) that

$$[B]([A] + [B] - 1) \geq ([A] + [B] + 1)([B] - 1).$$

Therefore $[A] \geq [B] - 1$, and hence $[A] = [B] - 1$. Since p is a prime and $p \geq [A] + [B]+1 = 2[B]$, we have that $p \geq 2[B] + 1$. Therefore by (I),

$[B](2[B]-2) \geq (2[B]+1)([B]-1)$, which cannot be true with $[B] \geq 4$.

<u>Case 3</u>: $p < [A] + 2[B] - 2$ and $[A] = [B]$. Then $[C+B] = p \geq 2[B] + 1$. Since we are assuming the lemma false the case that $[A] = [B] = \frac{1}{2}(p-1)$ is excluded. Therefore we may assume that $p \geq 2[B] + 3$. Then by (I) we have that

$$[B](2[B]-1) \geq (2[B]+3)([B]-1),$$

so that $3 \geq 2[B]$, which again is false since $[B] \geq 4$.

Since the three cases exhaust all possibilities, Lemma 2.4 is established.

We now complete the proof of the theorem by induction on $[A] + [B]$. If $[A] = [B] = 2$, then (A, B) is a standard pair by Corollary 1. Assume that (A, B) is a standard pair if $3 \leq [A]$, $3 \leq [B]$ and $[A] + [B] \leq n$, and consider the case that $3 \leq [A]$, $3 \leq [B]$ and $[A] + [B] = n+1$. Suppose that (A,B) is not a standard pair. If $[A] = [B] = \frac{1}{2}(p-1)$ then by Corollary 2, (A, B) is a standard pair, and we are through. Therefore if $[A] = [B]$ we assume that $[A] \neq \frac{1}{2}(p-1)$. Also, we may assume that $[A] \leq [B]$ and that $[B] \geq 4$. Then by Lemma 2.4 there exist b_1, b_2 and b_3 in B, $c \in C$ and $d \in C+B$ such that

$$d = (c+b_3) \in (C+B) \cap (\overline{C+b_1}) \cap (\overline{C+b_2}).$$

Define B_1 and B_2 by

$$B_1 = \{b \,/\, b \in B \text{ and } (d-b) \subset C\}$$

and $B_2 = B \cap \overline{B}_1$.

Since $b_1 \in B_2$, $b_2 \in B_2$ and $b_3 \in B_1$, we have that $2 \leq [B_2] \leq n$. Now, $(d-B_2) \cap C = \varphi$, and therefore $(d-B_2) \cap (A+B_1) = \varphi$. Hence by (iii), $(d-B_1) \cap (A+B_2) = \varphi$. Therefore, since $(d-B_1) \subset C$ and $(A+B_2) \subset C$,

$$[A+B_2] \leq [C] - [d-B_1] = [C] - [B_1] .$$

Hence,
$$\begin{aligned} [C] &\geq [A+B_2] + [B_1] \\ &> [A] + [B_2] - 1 + [B_1] \\ &= [A] + [B] - 1, \end{aligned}$$

which contradicts the hypothesis that (A,B) is a critical pair. Therefore (A,B) is a standard pair, and the proof is complete.

CHAPTER III

PROOF BY MANN'S TRANSFORMATIONS

In this chapter we will consider results that have been obtained using two transformations attributed to H. B. Mann. The first of these transformations was used to prove the $\alpha\beta$ Theorem of additive number theory and is used here to prove Chowla's Theorem. The second transformation is used to prove Chowla's Theorem and Vosper's Theorem. These transformations are also used to establish some other interesting results such as Theorem 3.4 which gives a sufficient condition for the Cauchy-Davenport inequality when G is simply an abelian group.

We prove first Theorem 3.1, which will be useful in proving later theorems.

<u>Theorem 3.1</u>: Let G be a finite abelian group, and let A and B be subsets of G. Then either $A+B = G$, or

$$[G] \geq [A] + [B].$$

<u>Proof</u>: If $A+B \neq G$ let $\bar{c}$ be an element of $\overline{A+B}$. Then $a \neq \bar{c}-b$ for any $a \in A$ and any $b \in B$. Therefore $[\bar{A}] \geq [B]$, and hence $[G] - [A] \geq [B]$, which proves

the theorem.

The following theorem is proved using Mann's famous transformation and furnishes a basis from which Mann proves Chowla's Theorem.

<u>Theorem 3.2</u>: Let A, B and $C = A+B$ be subsets of an abelian group G, and let $\bar{c}$ be an element of $\bar{C}$. Then there is a $B^* \supset B$ such that

(i) $\bar{C}^* = \overline{A+B}^* = \bar{c} + H$ for some subgroup H of G.

(ii) $[C^*] - [C] = [B^*] - [B]$.

<u>Proof</u>: The proof is by induction on $[\bar{C}]$. The assertion is trivially true for $[\bar{C}] = 1$ and $H = \{0\}$. Assume then that the theorem is true for $[\bar{C}] < n$ and consider the case where $[\bar{C}] = n$. Let $\bar{C} = \{\bar{c}_1, \bar{c}_2, \cdots \bar{c}_n\}$, and set $\bar{c}_1 - \bar{c}_i = d_i$. Let H be the subgroup of G generated by the d_i. We have then two cases to consider.

<u>Case 1</u>: For every i and every k, $(i = 1, 2, \cdots, n;$ $k = 1, 2, \cdots, n)$ there is an m such that $\bar{c}_i - d_k = \bar{c}_m$.

Since $\bar{c}_i = \bar{c}_1 - d_i$, and hence $\bar{c}_1 - d_i - d_k = \bar{c}_m$ for every i and k, we have that for every $h \in H$ there is an m such that $\bar{c}_1 + h = \bar{c}_m$. Since also $\bar{c}_1 - \bar{c}_m = d_m$ implies that $\bar{c}_1 - d_m = \bar{c}_m$, so that

$\bar{c}_m = \bar{c}_1 + h$ for every m, we have that $\bar{C} = \bar{c}_1 + H$. Let $B^* = B$ and for Case 1 we have the theorem.

Case 2: For some i and k, $(i = 1, 2, \cdots, n;$ $k = 1, 2, \cdots, n)$, $\bar{c}_i - d_k \in C$.

Form then the set B' consisting of all elements $b + d_j$ such that

(1) $a + b + d_j = \bar{c}_t$ for some t, $a \in A$, $b \in B$.

From (1) we have also

(2) $a + b + d_t = \bar{c}_j$.

By the definition of B' we have that $B \cap B' = \varphi$. Define the new sets B'' and C'' as $B'' = B \cup B'$ and $C'' = A+B''$. Then $\bar{c}_1 \notin C''$, for $\bar{c}_1 \in C''$ implies that $\bar{c}_1 = a+b+d_j$. Therefore $a+b = \bar{c}_1 - d_j = \bar{c}_j$, which is impossible. Thus $\bar{C}''$ is not empty. We prove now

(3) $[C''] - [C] = [B''] - [B] = [B']$.

That $[B''] = [B] \overset{+}{=} [B']$ is immediate from the fact that $B \cap B' = \varphi$. Let $\bar{c}_j \in C''$, then $\bar{c}_j = a+b'$ for some $b' \in B''$. Therefore $b' \in B'$, so that $b' = b+d_t$ for some t. Hence $\bar{c}_j = a+b + d_t$, and by (2) $a+b+d_j = \bar{c}_t$, so that $b + d_j \in B'$. On the other hand, if $b + d_j \in B'$ then $a + b + d_j = \bar{c}_t$, and by (2) $a + b + d_t = \bar{c}_j$. Hence $a + b + d_t \in A+B' \subset C''$, and we have $\bar{c}_j \in C''$.

Thus there is a 1-1 correspondence between the elements of C" not in C and the elements of B'. Hence (3) is established.

By the definition of C" we have that $[C"] > [C]$, and hence $[\overline{C}"] < [\overline{C}]$. Since also $\overline{c}_1 \notin C"$, we have by the inductive hypothesis a set $B^* \supset B" \supset B$ such that

$$\text{(i)} \quad \overline{C}^* = \overline{A+B}^* = \overline{c} + H, \quad H \text{ a subgroup of } G,$$

and

$$(4) \quad [C^*] - [C"] = [B^*] - [B"] \;.$$

Adding (4) to (3) we obtain

$$\text{(ii)} \quad [C^*] - [C] = [B^*] - [B],$$

which establishes the theorem for Case 2 and completes the proof.

With the aid of Theorem 3.1 and Theorem 3.2 we are able to give another proof of Chowla's Theorem. This proof is due to H. B. Mann [11]. For ease of reference we restate Chowla's Theorem.

<u>Theorem 3.3</u>: Let G be the group of residue classes modulo an integer m. Let A, B and $C = A+B$ be non-empty subsets of G with $0 \in A$ and $(a_i, m) = 1$ if $a_i \neq 0$. Then

$$(3.4) \quad [C] \geq \min (\overset{m}{\cancel{p}}, [A] + [B] - 1).$$

<u>Proof</u>: If $C = G$ we are through. If $C \neq G$ then by Theorem 3.2 there is a $B^* \supset B$ such that

(i) $\overline{C}^* = \overline{A+B}^* = \overline{c} + H$ for some subgroup H of G, $\overline{c} \in \overline{C}$,

and

(ii) $[C^*] - [C] = [B^*] - [B]$.

Consider the factor group (G/H). Let A' and B' be sets of cosets (mod H) that contain the elements of A and B^* respectively. Then by Theorem 3.1 we have that $[G/H] \geq [A'] + [B']$, and hence

(1) $[G] = [H]\,[G/H] \geq [H]\,[A'] + [H]\,[B']$.

Also, $0 \in H$, but $a_i \notin H$ unless $a_i = 0$, for $(a_i, m) = 1$, and since H is a subgroup, $a_i \overset{\in}{\notin} H$ would imply that $H = G$ which is contradictory to the fact that $H \neq G$ since $\overline{C} \neq \varphi$. Therefore a_i is contained in some coset f of H for every i, $(i = 1, 2, \cdots, [A]\overset{-1}{)}$. Hence

(2) $[H]\,([A'] - 1) \geq [A] - 1$.

Considering now the b_i, we have b_i ~~$\in$~~ contained in one of the cosets of B' for every $b_i \in B^*$, and thus

(3) $[H] \cdot [B'] \geq [B^*]$.

Combining (1), (2) and (3) we have

$$[G] \geq [A] + [H] + [B^*] - 1$$

or

$$[G] - [H] \geq [A] + [B^*] - 1.$$

But by (i) $[C^*] = [G] - [H]$. Therefore

$$(4) \quad [C^*] \geq [A] + [B^*] - 1.$$

Subtracting (ii) from (4) we have

$$[C] \geq [A] + [B] - 1,$$

which completes the proof.

In the introduction we stated that if was possible to give alternate conditions for the validity of the Cauchy-Davenport inequality. Using Theorem 3.1 and Theorem 3.2 we will next establish a sufficient condition for the Cauchy - Davenport inequality in the case that G is a finite abelian group. This theorem is due to Mann [12].

Theorem 3.4: Let G be an abelian group of order m, and let A, B and $C = A+B$ be non-empty subsets of G. If for every subgroup H of G,

$$[A+H] \geq \min \{m, [A] + [H] - 1\},$$

then for any subset B of G,

$$[C] \geq \min \{m, [A] + [B] - 1\} .$$

Proof: If $A+B = G$ we are through. If $A+B \neq G$ then $\overline{C} \neq \varphi$ and by Theorem 3.2 there is a set $B^* \supset B$ such that

(i) $\overline{C}^* = \overline{A+B}^* = \overline{c} + H$ for some subgroup H of G, and

(ii) $[C^*] - [C] = [B^*] - [B]$.

Let A' and B' be sets of cosets of H that contain the elements of A and B^* respectively. Consider then the factor group $[G/H]$. By Theorem 3.1 and (i) we have that $[G/H] \geq [A'] + [B']$. Since also

$[G] = [H] \cdot [G/H]$, $[B^*] \leq [H] \cdot [B']$

and $[A+H] = [H] \cdot [A']$, we have that

$[G] \geq [A+H] + [B^*]$. Then by the hypothesis it follows that

(i) $[G] \geq [A] + [H] + [B^*] - 1$.

Subtracting $[H]$ from each side and using the fact that (i) implies that $[G] - [H] = [C^*]$, we have

(2) $[C^*] \geq [A] + [B^*] - 1$.

Subtracting (ii) from (2) we get

$$[C] \geq [A] + [B] - 1,$$

and the theorem follows.

Mann was able to prove Chowla's theorem by first using his famous transformation to prove Theorem 3.2 and then giving a non-inductive proof of Chowla's Theorem. I have applied Mann's transformation directly and have thus obtained new proofs of both the Cauchy-Davenport Theorem and Chowla's Theorem. We consider first the proof of the Cauchy-Davenport Theorem.

Theorem 3.5: Let G be the group of residue classes modulo a prime p, and let A, B and $C = A+B$ be subsets of G. Then $[C] \geq \min\{p, [A] + [B] - 1\}$.

Proof: The proof is by induction on $[\overline{C}]$. If $[\overline{C}] = 0$, we are through. If $[\overline{C}] = 1$, then the assertion is false if $[C] < [A] + [B] - 1$. Since $[C] = p - 1$ it must be that $[A] + [B] > p$, but by Theorem 3.1 if $[A] + [B] > p$ then $C = G$ and we have a contradiction. Thus the Theorem is established for $[\overline{C}] = 1$. Assume now that the Theorem is true for $1 \leq [\overline{C}] < n$ and consider the case where $[\overline{C}] = n$. Form the set

$$D = \{d_i / \ d_i = \overline{c}_1 - \overline{c}_i, \ i = 2, 3, \cdots, n, \ \overline{c}_i \in \overline{C}\}.$$

Let b_0 be an element of B such that $a + b_0 + d_i \in \overline{C}$ for some a and some d_i, and define B^* as

(i) $\quad B^* = \{b_0 + d_i \ / \ a+b_0 + d_i \in \overline{C}\}.$

Since the definition of B^* depends upon the existence of a b_0 which satisfies (i) we show next that such a b_0 exists. Suppose that there is no $b \in B$ which will work as the b_0 in (i). Then $a + b + d_i \in C$ for every $a \in A$, $b \in B$ and $d_i \in D$. But $\{a+b\} = C$, and therefore $c + d_i \in C$ for every c and every d_i. Fix $d_i \neq 0$.

Then $c + kd_i \in C$ for every c and every natural number k. As before, since p is a prime, $c + kd_i$ generates G, and thus $C = G$; a contradiction to the hypothesis that $[\overline{C}] > 1$. Thus there is a $b_0 \in B$ which satisfies (i).

Now that we have established the existence of B^*, let $B_1 = B \cup B^*$ and $C_1 = A + B_1$. Then we establish the following four relationships:

(1) $B^* \cap B = \varphi$,

(2) $[C_1] > [C]$

(3) $\overline{c}_1 \notin C_1$

(4) $[C_1] - [C] = [B_1] - [B]$.

That the relations (1) and (2) are valid is immediate from the definitions. Suppose that $\overline{c}_1 \in C_1$, then $a + b_0 + d_k = \overline{c}_1$ for some d_k. But $d_k = \overline{c}_1 - \overline{c}_k$, and therefore $a + b_0 + \overline{c}_1 - \overline{c}_k = \overline{c}_1$, or $a + b_0 = \overline{c}_k$ which is a contradiction. Thus (3) is verified. Finally, $a + b + d_j = \overline{c}_k$ if and only if $a + b + d_k = \overline{c}_j$, so that there is a 1-1 correspondence between the elements of B^* and the elements of C_1 which are not in C. This establishes (4).

Since (2) and (3) imply that $[\overline{C}_1] < [\overline{C}]$, and that $\overline{C}_1$ is not empty, the induction hypothesis yields

$$(5) \quad [C_1] \geq [A] + [B_1] - 1.$$

Subtracting (1) from (5) we obtain

$$[C] \geq [A] + [B] - 1,$$

which completes the proof.

As the reader is by now probably well aware, the above proof would also hold for Chowla's Theorem if we could establish the existence of the b_0 used to define B^*. However, this is impossible as is shown by the following example.

Example 3.1: Let G be the cyclic group of integers mod 16, and set $A = \{0, 1, 3\}$,

$B = \{0, 4, 8, 12\}$ and $C = A+B$. Then

$C = \{0, 1, 3, 4, 5, 7, 8, 9, 11, 12, 13, 15\}$,

$\overline{C} = \{2, 6, 10, 14\}$,

and

$D = \{4, 8, 12\}$.

Then $a + b + d_t \in C$ for every a, every b and every d_t. Since B satisfies Chowla's hypotheses we must extend the above proof to include the case where b_0 does not exist. This will be done in the proof of Theorem 3.6.

We consider next a direct application of Mann's transformation to prove Chowla's Theorem. This proof is somewhat simpler than Mann's proof which was discussed earlier.

<u>Theorem 3.6</u>: Let G be the group of residue classes modulo an integer m, and let A, B and $C = A+B$ be subsets of G such that $0 \in A$ and for $a_i \neq 0$, $(a_i, m) = 1$. Then $[C] \geq \min(m, [A] + [B] - 1)$.

<u>Proof</u>: The proof is by double induction on $[\bar{C}]$ and m. If $[\bar{C}] = 0$ the theorem is trivial. If $[\bar{C}] = 1$ then $(\bar{c}-a) \in \bar{B}$ for every $a \in A$. Therefore, $[A] \leq [\bar{B}]$. Hence, $[C] = m - 1 = [\bar{B}] + [B] - 1 \geq [A] + [B] - 1$, and the assertion is true for $[\bar{C}] = 1$ and $m \leq 2$. Assume that $m > 2$, $n = [\bar{C}] > 1$ and that the theorem is true for modulus less than m and for modulus m if $[\bar{C}] < n$. Let $[\bar{C}] = n$, and define the set D as

$$D = \{d_i \,/\, d_i = \bar{c}_1 - \bar{c}_i;\ \ i = 2, 3, \cdots, [\bar{C}]\}.$$

Form the sum $c_i + d_j$; $c_i \in C$ and $d_j \in D$. There are then two cases to consider.

<u>Case 1</u>: There is at least one d_j such that $c_i + d_j \notin C$ for some c_i.

In this case we define B' as

$$B' = \{b + d_j \,/\, a+b+d_j \notin C\}.$$

Then $B' \neq \varphi$. Define B'' and C'' as $B'' = B \cup B'$ and $C'' = A + B''$. Since C'' will contain at least one more element than C, the induction hypothesis yields

$$[C''] \geq \min (\min (m, [A] + [B''] - 1).$$

Also, since $a + b + d_j = \bar{c}_u$ implies $a + b + d_u = \bar{c}_j$,

$$[B''] - [B] \geq [C''] - [C] .$$

Therefore,

$$[C] \geq \min (m, [A] + [B] - 1),$$

and the assertion is true for Case 1.

Case 2: For every $c \in C$ and every $d \in D$, $c + d \in C$.

Since $c + d \in C$ for every c and every d, C consists of the union of arithmetic progressions of the form $c_k + rd_\ell$ where $c_k \in C$, $r = 0, 1, 2, \cdots$, and c_k and d_ℓ are fixed for each progression. Therefore, C is the union of arithmetic progressions of the form $c_m + re$ where $c_m \in C$ and $e = \text{g.c.d} (d_j)$, $j=2,3,\cdots,n$. Note that if $e = 1$ we are through, since then $C = G$, and we have a contradiction. Thus, if m is a prime the proof is complete. Assuming m is not a prime, C is also the union of arithmetic progressions of the form $c_n + rd$ where $c_n \in C$ and $d = (e, m)$. Let H be the normal subgroup of G generated by d, and consider the factor group G/H. Let A', B' and C' be the sets of cosets which contain elements of A, B and C respectively. Denote the index of H by h. Then $h \cdot [C'] = [C]$, and $h \cdot [B'] \geq [B]$. Since $0 \in A$ and $(a_i, d) = 1$ for every non-zero a in A, there is one coset $S \in A'$ whose only element in A is zero. Therefore, $h \cdot [A'] \geq [A]+h-1$. Since G/H is isomorphic to the group of residue classes mod d, and since the non-zero elements of A' are relatively prime to d, the induction hypothesis gives

$$[C'] \geq \min (d, [A'] + [B'] - 1).$$

Therefore,

$$h \cdot [C'] \geq \min (hd, h \cdot [A'] + h . [B'] - h).$$

If we substitute our above results we get

$$[C] \geq \min (m, [A] + [B] - 1),$$

and the proof is complete.

We consider next an unpublished proof of Chowla's Theorem by R. D. Stalley, which uses a second transformation attributed to Mann.

Theorem 3.7: Let G be the group of residue classes modulo an integer m, and let A, B and $C = A+B$ be non-empty subsets of G such that $0 \in A$ and for $a_i \neq 0$, $(a_i, m) = 1$. Then $[C] \geq \min (m, [A] + [B] - 1)$.

Proof: The proof is by double induction on m and $n = [\overline{B}]$. If $[\overline{C}] = 0$ the theorem is trivial. If $[\overline{C}] = 1$ then $(\overline{c}-a) \in \overline{B}$ for every $a \in A$, $\overline{c} \in \overline{C}$. Hence $[A] \leq [\overline{B}]$ so that
$$[C] = m-1 = [\overline{B}] + [B]- 1 \geq [A] + [B] - 1.$$
Therefore the theorem is true for $m \leq 2$ and for $n \leq 1$. Assume then that the theorem is true if $m < m_0$ and $n < n_0$, and consider the case where $m = m_0$ and $n = n_0$. Also we may assume that $[\overline{C}] \geq 2$. Let $\overline{C} = \{\overline{c}_1, \overline{c}_2, \cdots, \overline{c}_n\}$, and let $d_i = \overline{c}_1 - \overline{c}_i$, $i = 2, \cdots, n$. We have then two cases to consider.

Case 1: There is a $b_0 \in B$ and a $d_t = \overline{c}_1 - \overline{c}_t$ such that $b_0 + d_t \notin B$.

Define the sets B', B^* and C^* by
$$B' = \{b_0 + d_u / b_0 + d_u \notin B\},$$
$$B^* = B \cup B' \text{ and } C^* = A + B^*.$$
Then, since $B' \cap B = \varphi$ and $B' \neq \varphi$, we have $[B^*] > [B]$. Therefore $[B^*] < [\overline{B}]$, and by the induction hypothesis we have

(i) $[C^*] \geq [A] + [B^*] - 1$.

Since $a + b_0 + d_u = \overline{c}_v$ implies that $a + b_0 + d_v = \overline{c}_u$, and hence that $b_0 + d_v \in \bar{B}$, we have

$$\text{(ii)} \quad [C^*] - [C] \leq [B^*] - [B].$$

Subtracting (ii) from (i) we have $[C] \geq [A] + [B] - 1$; which proves the theorem for Case 1.

Case 2: We have $b + d_t \in B$ for all $b \in B$ and all d_t. Then B, and therefore C, is the union of arithmetic progressions with common difference

$$e = \text{g.c.d.}\ \{d_u/2 \leq u \leq n\},$$

and hence with common difference $d = (e, m)$. Let H be the subgroup generated by d, and consider the factor group G/H. Denote the index of H by h. Let A_1, B_1 and C_1 denote the sets of cosets mod H which contain elements of A, B and C respectively. Then

$$h[B_1] \geq [B] \quad \text{and} \quad h[C_1] = [C].$$

Let $a \neq 0$ be an element of A_1. Since $(a + kd, m) = 1$ and d divides m we have $(a, m) = 1$. Since $[\bar{C}] > 0$, we have $d > 1$, so that $(kd, m) > 1$ if $k > 0$. Since $0 \in A$, we have $h\,[A_1] \geq [A] + h - 1$. Since $[\bar{C}] \geq 2$, we have $d \leq d_2 < m$. Finally, $C_1 = A_1 + B_1$, and by the induction hypothesis

$$[C] = h[C_1] \geq h \min (d, [A_1] + [B_1] - 1)$$

$$\geq \min (hd, h[A_1] + h[B_1] - 1)$$

$$\geq \min(m, [A] + [B] - 1) ;$$

which establishes the theorem for Case 2 and completes the proof.

As the concluding theorem for this chapter we consider next Mann's proof of Vosper's Theorem [5]. This proof is not simple and is presented here in detail. However, Mann's proof is shorter and simpler than Vosper's own proof. For reference I restate Vosper's Theorem:

<u>Theorem 3.8</u>: Let G be the group of residue classes modulo a prime p and let (A, B) be a pair of subsets of G. The pair (A, B) is a critical pair if and only if A and B satisfy one of the following four conditions:

(1) $[A] + [B] > p$

(2) $\min([A], [B]) = 1$

(3) $A = \overline{d - B}$ for some $d \in G$

(4) (A, B) is a standard pair.

<u>Proof</u>: The proof is by induction on $[\overline{C}]$ and will make use of the following lemma:

<u>Lemma 3.1</u>: Theorem 3.6 is true if A is a standard set.

<u>Proof</u>: As we have shown earlier we may assume that $0 \in A \cap B$, and that $A = \{0, 1, 2, \cdots, [A] - 1\}$, (refer to the proof of Lemma 2.1). Also, because of (2), we may

assume that $\min([A], [B]) \geq 2$. Consider then the gaps in B. If B has no gaps of length greater than or equal to [A], then $[A] + [B] > p$ and we have condition (1). If B has one gap of length at least [A], and no other gaps, then B is a standard set with common difference 1, and we have condition (4). If B has one gap of length at least [A] and at least one other gap, then C will contain besides [B] at least [A] elements in the gap in B of length at least [A]. Therefore $[C] \geq [A] + [B]$, and the lemma is established.

We now prove the theorem. Conditions (1) and (2) are immediate. If $[C] = p - 1$, then $\overline{C} = \overline{c}$ and $\overline{B} \supset \overline{c} - A$, so that $[\overline{B}] \geq [A]$. Therefore,

$$\begin{aligned} [A] + [B] &= [A] + p - [\overline{B}] \\ &\leq [A] + p - [A] \\ &= [C] + 1. \end{aligned}$$

Since equality will hold if and only if $\overline{B} = \overline{c} - A$ we have established condition (3). We now establish condition (4) by induction on $[\overline{C}]$. Assume that the assertion of Theorem 3.7 is true if $2 \leq [\overline{C}] < n$ and consider the case where $[\overline{C}] = n$. Also we may assume that conditions (1), (2) and (3) are not satisfied. Let $\overline{c}_1, \cdots, \overline{c}_n$ be the elements of $\overline{C}$ and set $\overline{c}_1 - \overline{c}_i = d_i$, $i = 2, 3, \cdots, n$. We have then two cases to consider.

Case 1: There is a $b \in B$ and indices s and t such that $b + d_s \in B$ and $b + d_t \notin B$.

In this case we form the sets

$$B' = \{b + d_u / b + d_u \notin B\},$$

$$B^* = B \cup B' \text{ and } C^* = A + B^*.$$

Since $a + b + d_u = \bar{c}_v$ implies $a + b + d_v = \bar{c}_u$, and therefore that $b + d_v \notin B$; we have

$$\text{(i)} \quad [C^*] - [C] \leq [B^*] - [B] .$$

As a consequence of the definitions we have

$$\text{(ii)} \quad \bar{c}_1 \notin C^*, [B^*] > [B] \text{ and } [C^*] > [C] .$$

Now, conditions (1) and (2) are clearly not satisfied by A, B^* and C^*. Suppose that $[C^*] = p - 1$. Then, since $[\bar{C}] = n$ implies that $[C] = p - n$ and therefore that $[C^*] - [C] = p - 1 - (p-n) = n-1$, it follows from (i) that $[B^*] - [B] \geq n-1$. But $[B^*] - [B] = [B']$, so that $[B'] \geq n-1$, which contradicts the hypothesis that $b + d_s \in B$ for some index s. Hence A, B^* and C^* do not satisfy (3). Then since $[C^*] > [C]$, $[\bar{C}^*] < [\bar{C}]$, and therefore by induction either (4) is satisfied, or

$$\text{(iii)} \quad [C^*] > [A] + [B^*] - 1.$$

Subtracting (i) from (3) we get

$$[C] > [A] + [B] - 1,$$

and have the proof for Case 1.

<u>Case 2</u>: Either $b + d_t \in B$ or $b+d_t \notin B$ for all $b \in B$ and all d_t.

Then either B is a standard set with common difference d_2, and we are through by the lemma, or there are elements b_1 and b_2 in B such that $b_1 + d_2 \notin B$ and $b_2 + d_2 \notin B$. Form then the sets

$$B' = \{b_1 + d_u / b_1 + d_u \notin B\},$$

$$B'' = \{b_2 + d_u / b_2 + d_u \notin B\},$$

$$B^* = B \cup B' \cup B''$$

and

$$C^* = A + B^*.$$

Then again we have $\bar{c}_1 \notin C^*$. Also,

$$\sum_{u=2}^{n} (b_1 + d_u) - \sum_{u=2}^{n} (b_2 + d_u) = (n-1)(b_1 - b_2) \not\equiv 0 \pmod{p}.$$

Hence $B' \neq B''$, and $[B' \cup B''] \geq n$.

Therefore

(iv) $[B^*] \geq B + n$.

Since $p = [C] + n$ and $\bar{c}_1 \notin [C^*]$, we have $[C^*] \leq [C] + n-1$. Then by (iv) and the Cauchy-Davenport Theorem

$$[C] + n-1 \geq [C^*] \geq [A] + [B^*] - 1$$
$$\geq (A] + [B] + n - 1.$$

Thus,

$$[C] \geq [A] + [B],$$

and the proof is complete.

CHAPTER IV

PROOFS BY DYSON'S TRANSFORMATION

In this chapter we will use Dyson's transformation to prove Chowla's Theorem, Vosper's Theorem and several theorems which yield the Cauchy-Davenport Inequality under different hypotheses. In particular, Theorem 4.2 is true for abelian groups in general.

Before proceeding to the theorems we first prove the following lemma which makes use of Dyson's transformation:

<u>Lemma 4.1</u>: Let G be the group of residue classes modulo m; let A, and B ~~and $C = A + B$~~ be non-empty subsets of G with $0 \in B$, $[B] \geq 2$, and such that there is an $a_1 \in A$ for which $a_1 + b \notin A$ for some $b \in B$. Then there are non-empty sets A_1, B_1 and $C_1 = A_1 + B_1$ such that

(1) $[A_1] + [B_1] = [A] + [B]$

(2) $[B_1] < [B]$

and

(3) $C_1 \subset C$.

<u>Proof</u>: Define the sets A' and B' by

$$B' = \{b \,/\, \overset{b \in B_1}{a_1 + b} \notin A\},$$

and

$$A' = \{a_1 + b \,/\, b \in B'\}.$$

Let $B_1 = \overset{B-B'}{B \cap \overline{B}'}$ and $A_1 = A \cup A'$; then we immediately have:

$$\text{(i)} \quad [B_1] = [B] - [B']$$

$$\text{(ii)} \quad [A_1] = [A] + [A']$$

and

$$\text{(iii)} \quad [A'] = [B'].$$

Substituting (iii) into (i) and adding to (ii) we get $[A_1] + [B_1] = [A] + [B]$, and thus establish (1). Since we stipulated that a_1 exists, B' is not empty, and therefore $[B_1] < [B]$, which is (2). Also $0 \in B$ and $0 \notin B'$, so that B_1 and C_1 are not empty. We next establish that $C_1 \subset C$. Let c' be an element of C_1. Then $c' = a' + b'$ with $a' \in A_1$ and $b' \in B_1$. If $a' \in A_1$ then either $a' \in A$ or $a' \in A'$. If $a' \in A$ then, since $B_1 \subset B$, $c' \in C$. If $a' \in A'$ then $a' = a_1 + b$, and therefore $c' = a_1 + \overset{\in B_1}{b} + \overset{\in B_1}{b'}$. But $a_1 + b' \in A$, for if $a_1 + b' \notin A$ then $b' \in B'$, and we have a contradiction to the fact that $b' \in B_1$. Therefore $c' \in C$, and hence $C_1 \subset C$. This completes the proof of the lemma.

We next use Lemma 4.1 to prove a Theorem which yields Chowla's Theorem as a special case.

Theorem 4.1: Let G be the group of residue classes modulo an integer m; let A, B and $C = A + B$ be subsets of G for which $(b_i - b_0, m) = 1$ for some b_0 and every $b_i \neq b_0$, $b_i \in B$. Then

$$[C] \geq \min\{[A] + [B] - 1, m\}.$$

It is apparent that Theorem 4.1 implies Chowla's Theorem, for if $b_0 = 0$ then $0 \in B$ and $(b_i, m) = 1$ for every $b_i \neq b_0$, and these results are precisely Chowla's hypotheses. Actually we may assume $0 \in B$, for if $0 \notin B$ we transform B into B_0 by $B_0 = B - b_0$ and define C_0 as $C_0 = A + B_0$. Then $[B_0] = [B]$, $[C_0] = [C]$, $0 \in B_0$, $(b_i, m) = 1$ if $b_i \in B_0$ and $b_i \neq 0$, and we just need to prove the theorem for A, B_0 and C_0. We now prove the theorem with the assumption that $0 \in B$.

Proof: Since there is nothing to prove if $C = G$ we assume that $C \neq G$ and show that $[C] \geq [A] + [B] - 1$. The proof is by induction on $[B]$. If $[B] = 1$ the assertion is trivial. Therefore we assume that the theorem is true for all sets B where $1 \leq [B] < r \overset{<}{\leq} m$ and consider the case where $[B] = r$. Then there is an $a_1 \in A$ such that $a_1 + b \notin A$ for ~~any~~ some non-zero $b \in B$. For if not, then $a + b \in A$ for every $a \in A$, and every non-zero $b \in B$. We choose b so that $(b, m) = 1$. Then ~~and therefore~~ $a + kb \in A$ for ~~every $a \in A$ and~~ every natural number k. ~~But by hypothesis $(b, m) = 1$,~~ and so ~~that~~ $a + kb$ generates G. ~~and therefore~~ $A = G$ in contradiction to our assumption that $C \neq G$. Therefore there is an $a_1 \in A$ for which $a_1 + b \notin A$ for ~~any~~ some non-zero $b \in B$. Hence by Lemma 4.1 there are non-empty sets A_1, B_1 and $C_1 = A_1 + B_1$ such that

(i) $[A_1] + [B_1] = [A] + [B]$

(ii) $[B_1] < [B]$

and

(iii) $C_1 \subset C$.

Then by our inductive hypothesis and (ii) we have $[C_1] \geq [A_1] + [B_1] - 1$. Combining this result with (i) and (iii) we get $[C] \geq [A] + [B] - 1$, and the theorem is proved.

In the following theorem we will apply the preceeding method to prove a theorem which gives a sufficient condition for the Cauchy-Davenport inequality to hold when G is simply an additive abelian group. This theorem is attributed to L. Moser and was proved by P. Scherk [14].

Theorem 4.2: Let G be an additive abelian group of order m, and let A, B and $C = A + B$ be non-empty subsets of G with $0 \in A \cap B$, and for $a \in A$, $b \in B$, $a + b = 0$ if and only if $a = 0$ and $b = 0$. Then

$$[C] \geq \min (m, [A] + [B] - 1).$$

Proof: The proof is by induction on $[B]$. If $C = G$ there is nothing to prove, so we assume that $C \neq G$. Likewise the theorem is trivial if $[B] = 1$, so we may assume that $[B] \geq 2$. Let $[B]$ be fixed and assume that the theorem is true for all smaller values of $[B]$. Then there is an $a_1 \in A$ for which $a_1 + b \notin A$ for some $b \in B$. For, since $[B] \geq 2$, there is a non-zero $b \in B$, and this, together with the hypothesis that $a + b \neq 0$ unless $a = 0$ and $b = 0$, implies that $0 \notin A + b$. But $[A+b] = [A]$, and therefore $a_1 + b \notin A$ for some $b \in B$. Thus we have satisfied the hypotheses of Lemma 4.1, and hence there are sets A_1, B_1 and C_1 such that

(1) $[A_1] + [B_1] = [A] + [B]$,

(2) $[B_1] < [B]$

and

(3) $C_1 \subset C$.

Also, from the definitions of A_1, B_1 and C_1 in Lemma 4.1 we know that $0 \in A_1$ and $0 \in B_1$. We establish that if $a' \in A_1$ and $b' \in B_1$ then $a' + b' = 0$ if and only if $a' = 0$ and $b' = 0$. Since $B_1 \subset B$ we have the assertion immediately if $a' \in A$. Therefore let $a' + b' = 0$ and assume that $a' \notin A$. Then $a' = a_1 + b$ so that $a' + b' = a_1 + b + b' = (a_1 + b') + b = 0$. But $a_1 + b' \in A$, for otherwise $b' \in B'$. Therefore $(a_1 + b') + b = a+b = 0$, and by the hypotheses $a = 0$ and $b = 0$. But since $a_1 + b \notin A$, b cannot be zero, and we have a contradiction. Therefore $a' \in A$ and we have established that $a' + b' = 0$ if and only $a' = 0$ and $b' = 0$.

Then, since A_1, B_1 and C_1 satisfy the hypotheses of the theorem, the inductive hypothesis yields

$$[C_1] \geq \min (m, [A_1] + [B_1] - 1),$$

which together with (1), (2) and (3) gives:

$$[C] \geq \min (m, [A] + [B] - 1).$$

The proof is now complete.

In connection with the extensions of the Cauchy-Davenport Inequality to more general abelian groups than the groups of residue classes mod m, we consider briefly two theorems from a paper by J. H. B. Kemperman and P. Scherk [15]. Each of these theorems gives a sufficient condition for the Couchy-Davenport Inequality, and the first one is proved using Dyson's Transformation. The second theorem gives a condition under which the hypotheses of the first theorem are satisfied. Kemperman and Scherk offer other theorems similar to second one mentioned in that the third implies the second and so on, but these theorems are not considered here. We now investigate the first theorem in Kemperman and Scherk's paper.

<u>Theorem 4.3</u>: Let G be an arbitrary abelian group, written additively, and let A, B and $C = A + B$ be non-empty, finite subsets of G. Denote the order of G by m. If there is a $b_0 \in B$ such that $A + B \not\subset A + b_0$ then

$$[C] \geq \min(m, [A] + [B] - 1).$$

<u>Proof</u>: The proof of this theorem is so similar to the proof of Theorem 4.2 that I will only present an outline of the proof. As in the proof of Theorem 4.2 we use Lemma 4.1, (or its immediate extension if G is not finite). Since the assertion is trivial if $[B] = 1$, or if $C = G$, we may assume that $c \neq G$ and that the theorem is true if $[B] < n$. We will show that the hypotheses

of the theorem are sufficient to permit us to perform Dyson's Transformation as in Lemma 4.1, and then the result will follow as in the proof of Theorem 4.2. Since by the hypothesis $A + B \not\subset A + b$ for some $b \in B$, there is an $a_1 \in A$ and elements b_0 and b_1 in B such that $a_1 + b_1 - b_0 \notin A$. For otherwise $a_1 + b_1 - b_0 = a_0$, or $a_1 + b_1 = a_0 + b_0$ and we have a contradiction. Define then B^* as $B^* = B - b_0$. Then $[B^*] = [B]$, $0 \subset B^*$ and $b_2 = b_1 - b_0$ satisfies $a_1 + b_2 \notin A$. Therefore as in Lemma 4.1 there are sets A_1 and B_1 such that

(1) $[A_1] + [B_1] = [A] + [B^*]$

(2) $[B_1] < [B^*]$

and

(3) $C_1 \subset C$.

Then by our inductive hypothesis

$$[C_1] \geq \min (m, [A_1] + [B_1] - 1)$$

and hence

$$\begin{aligned}[C] &\geq \min (m, [A] + [B^*] - 1) \\ &\geq \min (m, [A] + [B] - 1).\end{aligned}$$

The next theorem by Kemperman and Scherk gives another sufficient condition for the Cauchy-Davenport inequality and is proved by showing that the hypotheses imply that the conditions of Theorem 4.3 are satisfied.

Theorem 4.4: Let G be an abelian group, written additively, and let A, B and $C = A + B$ be non-empty subsets of G. If there are elements b_0 and b_1 in B such that $[A](b_1 - b_0) \neq 0$ then $A + B \not\subset A + b$ for some $b \in B$.

Proof: Suppose that $A + B \subset A + b$ for some $b \in B$, and denote the b by b_0. Then $a + b - b_0 \subset A$ for every a and b. Therefore $[B] \leq [A]$, for otherwise by fixing a and letting b range through B we could determine more than $[A]$ elements in A and have a contradiction. Fix then b_1 so that $[A](b_1 - b_0) \neq 0$, and let a run through A. Since b_1 and b_0 are fixed, if a ranges through A then so will $a + b_1 - b_0$. Therefore

$$\Sigma a = \Sigma(a+b_1 - b_0) = \Sigma a + [A](b_1 - b_0), \text{ which}$$

implies that $[A](b_1 - b_0) = 0$. Again we have a contradiction and so the theorem is proved.

Following the last diversion from the proofs by Dyson's Transformation we return to this method to give a somewhat shorter proof of Vosper's Theorem. This method of proof has been published by A. G. Vosper [17] after its use was suggested to him by M. Kneser. Instead of reproving the whole theorem we will just prove the difficult part; i.e., that condition (4) is necessary. Since Vosper's Theorem is somewhat long, we restate it for reference.

Theorem 4.5: Let G be the group of residue classes modulo a prime p, and let (A, B) be a pair of subsets of G. The pair (A, B) is a critical pair if and only if A and B satisfy one of the following four conditions:

(1) $[A] + [B] > P$

(2) $\min ([A], [B] = 1$

(3) $A = \overline{d-B}$ for some $d \in G$.

(4) (A, B) is a standard pair.

Proof: Since we are here only trying to establish that (4) is necessary, we will assume some of the lemmas from Chapter II and prove two more. Also we will assume that (A, B) is a critical pair and that conditions (1), (2) and (3) are not satisfied. For reference we state the lemmas we need from Chapter II.

Lemma 2.1: If A is a standard set then (A, B) is a standard pair.

Corollary: If $\min ([A], [B])= 2$ then (A, B) is a standard set.

Lemma 2.3: $(-A, \bar{C})$ is a critical pair.

In addition to these lemmas we need the following two lemmas:

Lemma 4.2: If C is a standard set then (A, B) is a standard pair.

Proof: If C is a standard set then so is $\bar{C}$. For, if $C = \{c + ik / 0 \leq i \leq [C] - 1\}$ then $\bar{C} = \{c+ik/[C]\leq i\leq p\}$. By Lemma 2.3, $(-A\ \bar{C})$ is a critical pair. By the assumptions $[C] = p - [A] - [B] + 1 < p$ and $\min\ ([-A], [\bar{C}]) > 1$. Therefore, by Lemma 2.1, $(-A, \bar{C})$ is a standard pair. Hence $-A$, and therefore A, is a standard set. Then by Lemma 2.1 (A, B) is a standard pair.

Lemma 4.3. If $[B] \geq 3$ and $0 \in B$ then $[B] > [B_1] \geq 2$, where B_1 is defined as in Lemma 4.1.

Proof: By the corollary to Lemma 2.1 we may assume that $[A] \geq 3$. Let A^* be the subset A such that $[B_1] < [B]$ for every $a \in A^*$. (A^* is the set of all $a \in A$ which could be chosen as the a_1 in the definition of B_1.) If $A^* = A$ then $[A^*] \geq 2$. If $A^* \neq A$ let $A^{**} = A \cap \bar{A}^* \neq \varphi$. Then no $a \in A^{**}$ will work as the a_1 in the definition of B_1. Therefore $B + a \subset A$ for every

$a \subset A^{**}$. Hence $A^{**} + B \subset A$. Therefore

$$\begin{aligned}[A] \geq [A^{**} + B] &\geq [A^{**}] + [B] - 1 \\ &\geq [A^{**}] + 2.\end{aligned}$$

Hence $[A^*] = [A] - [A^{**}] \geq 2$.

Suppose now that it is impossible to find an $a_1 \in A^*$ for which the corresponding B_1 satisfies $[B_1] \geq 2$. Then since $0 \in B$, $B \cap (A-a) = 0$, and $(B+a) \cap A = a$ for every $a \in A^*$. Let $B^* = B \cap \{\overline{0}\}$. Then $(B^* + a) \cap A = \varphi$ for every $a \in A^*$. Hence $(B^* + A^*) \cap A = \varphi$. But $A^* + B^* \subset A + B$, and $A \subset A+B$. Therefore

$$\begin{aligned}[A^* + B^*] &\leq [A + B] - [A] \\ &= [B] - 1 \\ &= [B^*] .\end{aligned}$$

But this is impossible since $[A^*] \geq 2$, and therefore the lemma is true.

We are now ready to complete the proof of the theorem. By the corollary to Lemma 2.1, the pair (A, B) is a standard pair if $[B] = 2$. Therefore assume that the pair (A, B) is a standard pair if $[B] < n$ and consider the case where $[B] = n$. As we have shown earlier, we may assume that $0 \in B$. Therefore by Lemma 4.3, $[B] > [B_1] \geq 2$, where B_1 is defined as in Lemma 4.1. Then by Lemma 4.1 and the assumption that (A, B) is a critical pair

$$
\begin{aligned}
[A] + [B] - 1 &= [A+B] \\
&\geq [A_1 + B_1] \\
&\geq [A_1] + [B_1] - 1 \\
&= [A\ ] + [B\ ] - 1 .
\end{aligned}
$$

Hence

$$\text{(I)} \quad [A+B] = [A_1 + B_1] .$$

Therefore $[A_1 + B_1] = [A_1] + [B_1] - 1$, and the pair (A_1, B_1) is a critical pair. Since $[B_1] < [B]$, the pair (A_1, B_1) is a standard pair by the inductive hypothesis. By (I) and Lemma 4.1 (3), $A + B = A_1 + B_1$. Therefore C is a standard set. Hence, by Lemma 4.2, (A, B) is a standard pair, and the theorem is established.

CHAPTER V

FURTHER RESULTS

In this last chapter we will state two other results that have been obtained by famous mathematicians in connection with the Cauchy-Davenport Inequality. The first of these theorems appears in a short article by M. Kneser [10], and the second is the object of a monumental paper by J. H. B. Kemperman [9]. Kneser's result is similar to many of the preceeding theorems in that it gives another sufficient condition for the Cauchy-Davenport Inequality, but in this case G is only restricted to being abelian and A and B are required to be finite. In his paper Kemperman derives a result for abelian groups which is similar to Vosper's Theorem. Like Kneser's result, the group G is required to be abelian and the subsets A and B are required to be finite. No attempt is made here to prove these two theorems.

Before stating the results of Kneser and Kemperman we introduce some definitions:

Definition 5.1: Let G be an abelian group, and let H be a non-empty subgroup of G, not consisting of the identity element alone. A subset C of G is said to be "periodic" if for every element g of some subgroup H, $C + g = C$. If C is not periodic it is said to be "aperiodic". Since H is determined by C we will designate this relationship by writing $H(C)$ for H.

Definition 5.2: A subset C of G is said to be "quasi-periodic" if there is a subgroup F of G, with $[F] \geq 2$, such that C is the disjoint union of a non-empty set C' consisting of F-cosets and a set C'' contained in a remaining F-coset.

Definition 5.3: A subset C of G is said to be in arithmetic progression if C can be written as:

$$C = \{c_0 + jd \,/\, j = 0, 1, 2, \cdots, [C]-1;\ c_0 \in C;\ d \in G\}.$$

The element d is called the common difference.

We now can state Kneser's Theorem:

Theorem 5.1: Let G be an abelian group and let A, B and $C = A+B$ be non-empty subsets of G. The set C is periodic if

$$[C] \leq [A] + [B] - 2.$$

That this theorem gives us the Cauchy-Davenport Inequality is immediate; for if C is aperiodic, then $[C] \geq [A] + [B] - 1$. If G is the set of residue classes modulo a prime p, and $C \neq G$, then C is aperiodic and Theorem 5.1 yields the Cauchy-Davenport Theorem.

To continue on to Kempermann's theorem we introduce one more definition.

Definition 5.4: The pair (A_1, B_1) of non-empty subsets of G is said to be "elementary" if one of the following conditions holds:

(1) $\min [A], [B] = 1$.

(2) A_1 and B_1 are in arithmetic progression with common difference d such that the order of d is greater than or equal to $[A] + [B] - 1$.

(3) For some finite group H, each of A_1 and B_1 is contained in an H-coset while $[A_1] + [B_1] = [H] + 1$. Moreover, precisely one element c of C has only one representation as a sum $a+b$, where $a \in A_1$ and $b \in B_1$.

(4) The set A_1 is aperiodic, and for some subgroup H of G, A_1 is contained in an H-coset while B_1 is of the form $B_1 = g - (\overline{A}_1 \cap (a+H))$. Moreover, no element c of C has only one reprecentation as a sum

$a + b$ where $a \in A_1$ and $b \in B_1$.

Finally, we state Kemperman's Theorem:

Theorem 5.5: Let G be an abelian group of order not less than 2, and let A, B and $C = A + B$ be non-empty subsets of G. A necessary and sufficient condition that

(I) $[C] = [A] + [B] - 1$

and, moreover,

(II) if C is periodic then a least one element of C has only one representation as $a + b$, $a \in A$, $b \in B$, is the existence of a non-empty subset of A_1 of A, a non-empty subset B_1 of B and a subgroup F of G of order not less than 2 such that:

(i) The pair (A_1, B_1) is elementary and each of A_1 and B_1 is contained in an F-coset.

(ii) The element $\overline{c} = \sigma (A_1 + B_1)$ has $c' = \sigma A_1 + \sigma B_1$ as its only representation of the form $\overline{c} = \overline{a} + \overline{b}$, where $\overline{a} \in \sigma A$ and $\overline{b} \in \sigma B$. Here, σ represents the quotient mapping $G \rightarrow G/F$.

(iii) The complement A' of A_1 in A satisfies

$A' + F = A'$, similarly B' of B_1 satisfies $B' + F = B'$.

(iv) $[\sigma A + \sigma B] = [\sigma A] + [\sigma B] - 1$.

It is worth noting that although Kemperman's Theorem in some way resembles Vosper's Theorem, it is not a generalization of Vosper's Theorem to abelian groups. For if we specialize G to the group of residue classes modulo a prime, then $F = G$, $A' = G$, A_1 is empty and we are left with the conclusion that not both (I) and (II) can hold. Vosper's Theorem of course, only gives us necessary and sufficient conditions for (I) to hold. The problem of generalizing Vosper's Theorem is as yet unsolved, but perhaps Kemperman's work will lead to the solution.

BIBLIOGRAPHY

1. Cauchy, A. Theorie des fonctions analytiques. Journal De L'Ecole Polytechnique 9:99-116. 1813.

2. Cauchy, A. Recherches sur de Nombres, Oeuvres complètes. Vol. 1, Second series. Paris, Gaunthier Villars.1882. p. 39-63.

3. Chowla, I. A theorem on the addition of residue classes. Proceedings of the Indian Academy of Science 2:242-243. 1935.

4. Chowla, I. A theorem on the addition of residue classes. Quarterly Journal of Mathematics, Oxford Series, 8:99-102. 1937.

5. Chowla, S., H. B. Mann and E. G. Straus. Some applications of the Cauchy-Davenport Theorem, Det Kongelige Norske Vinderskabers Selskabs Forhandlinger 32(13):74-80. 1959.

6. Davenport, H. On the addition of residue classes. Journal of the London Mathematical Society 10: 30-32. 1935.

7. Davenport, H. A historical note. Journal of the London Mathematical Society 22:100-101. 1947.

8. Dyson, F. J. A theorem on the densities of sets of integers. Journal of the London Mathematical Society 20:8-14. 1945.

9. Kemperman, J. H. B. On small subsets in an abelian group. Acta Mathematica 103(1-2):63-88. 1960.

10. Kneser, M. Ein Zatz über Abelsche Gruppen mit Anwendungen auf die Geometrie der Zahlen. Mathematische Zeitschrift 61:429-434. 1955.

11. Mann, H. B. On the products of sets of group elements. Canadian Journal of Mathematics 4:64-66. 1952.

12. Mann, H. B. An addition theorem for sets of elements of abelian groups. Proceedings of the American Mathematical Society 4:423. 1953.

13. Mann, H. B. A proof of the fundamental theorem on the densities of sums of sets of positive integers. Annals of Mathematics 2(43):523-527. 1942.

14. Scherk, P. Distinc elements in a set of sums. American Mathematical Monthly 62:46. 1955.

15. Scherk, P. and J. H. B. Kemperman. Complexes in abelian groups. Canadian Journal of Mathematics 6:230-237. 1954.

16. Vosper, A. G. The critical pairs of subsets of a group of prime order. Journal of the London Mathematical Society 31:200-205. 1956.

17. Vosper, A. G. Addendum to the critical pairs of subsets of a group of prime order. Journal of the London Mathematical Society 31:280-282. 1956.