AN ABSTRACT OF THE THESIS OF

Dale E. Green for the degree of Master of Arts in Mathematics presented on June 7, 1989.

Title: Existence of Small Zero-Sum Subsets of Large Sets of Residue Classes

Abstract approved: Redacted for Privacy
Robert D. Stalley

R. Stalley conjectured and N. Alon proved that if $A \subseteq Z_n$ and $|A| > (\frac{1}{3} + \epsilon)n$, where $\epsilon > 0$, then A contains a non-empty zero-sum subset of at most three residue classes provided that $n > n_0(\epsilon)$. Stalley considered sets $A \subseteq Z_{2q}$ such that $|A| = q-h$, where $h = 0$ or $h = 1$, and determined the least integers $q_0(h)$ such that for $q \geq q_0(h)$ the conclusion of Alon's result holds. In this thesis we consider sets $A \subseteq Z_{2q+1}$, impose corresponding restrictions on $|A|$, and obtain corresponding results. We also give a brief history of events leading up to this thesis. Furthermore, we investigate limitations on the improvement of Alon's result.

Existence of Small Zero-Sum Subsets of Large Sets of Residue Classes

by

Dale E. Green

A THESIS

submitted to

Oregon State University

in partial fulfillment of
the requirements for the
degree of

Master of Arts

Completed June 7, 1989

Commencement June 1990

APPROVED:

Redacted for Privacy

Professor of Mathematics in charge of major

Redacted for Privacy

Chairman of Department of Mathematics

Redacted for Privacy

Dean of Graduate School

Date thesis is presented June 7, 1989

Typed by the author Dale E. Green

ACKNOWLEDGEMENTS

I wish to express my deepest gratitude to Professor Robert D. Stalley for his patient advice and counsel during the preparation of this thesis and for leading the author to see that mathematics and its exposition is an art as well as a science.

TABLE OF CONTENTS

LIST OF TABLES

EXISTENCE OF SMALL ZERO-SUM SUBSETS OF LARGE SETS OF RESIDUE CLASSES

CHAPTER 1

INTRODUCTION

We begin by mentioning several standard conventions that we use. We let Z_n denote the commutative group of residue classes modulo n under addition, and we write $R \subseteq Z_n$ to denote that R is a subset of the set of elements of Z_n. The number of elements in the set R is denoted by $|R|$ and we refer to this as the size or cardinality of R. Unless specified otherwise, we assume that all sets are nonempty.

Small latin letters denote both residue classes and residues. The meaning of the notation is made clear by its context. If the sum of the elements of a set of residue classes is equal to zero, we call the set a zero-sum set. We take the sum of a single element to be the element itself.

Consider an arbitrary nonempty set A of residue classes modulo n. We obtain results related to the following two problems. Find how large A must be in order that A contains a nonempty zero-sum subset S with

no restriction on the size of S, or with a maximum size specified for S.

There are many other problems involving sets A of residue classes mod n, zero-sum subsets S of A, and the cardinality of one or both. We now list some of these problems most of which to the author's knowledge are new. These problems together with the two problems in the preceding paragraph may be considered a branch of additive modular number theory. How large must A be in order that A contains a zero-sum subset of some specified minimum size? Note that this is a companion to the second of the two problems mentioned above. How many zero-sum subsets S does A contain with no restriction, or with some specified restriction, on the size of S? Guy[5] reports that Erdös and Heilbronn asked how large A can be while remaining free of zero-sum subsets. Other problems are obtained from those listed above by replacing "zero-sum subset" with "r-sum subset" where r is an arbitrary residue class, by imposing a particular structure on A, by replacing the words "set" and "subset" with the words "multi-set" and "multi-subset", or by doing some or all of these things. Finally, one may seek either finite or asymptotic results.

To the author's knowledge results have not been obtained for any of these problems except for the two

defining problems of this thesis, which are given above, together with an r-sum subset variation on the first of these two problems, the problem posed by Erdös and Heilbronn as reported by Guy, and some problems related to multi-sets.

In 1964 Erdös and Heilbronn[3] obtained a condition of the form $|A| > f(p)$, where p is prime, which guarantees that any residue class r mod p can be represented as a sum of elements from A. Furthermore, they conjectured that their condition could be improved and extended in its improved form to composite moduli provided that $r = 0$. In 1984 and 1987 N. Alon[1,2] obtained conditions of the form $|A| > f(n,k)$ which guarantee that A contains a zero-sum subset S of maximum size k for n sufficiently large.

In Chapter 2 we give a more complete but still brief history of developments in the area of our research from the work of Erdös and Heilbronn up through current results including our work and the work of Alon. The first section of the chapter is expository. In the last two sections we tie off two loose ends.

In Chapter 3 we concern ourselves mainly with the question of whether Alon's results can be improved.

Results related to Erdös and Heilbronn's work led

R. D. Stalley[8] to consider sets $A \subseteq Z_{2q}$ such that $|A| = q-h$, where $h = 0$ or $h = 1$. He determined the least integers $q_0(h)$ such that for $q \geq q_0(h)$ A contains a zero-sum subset S of at most three elements. In Chapter 4 and Chapter 5 we obtain results for odd moduli corresponding to Stalley's results for even moduli. In Chapter 4 we let $A \subseteq Z_{2q+1}$ and $|A| = q$. We then determine the least integer $q_0(0)$ such that for all $q \geq q_0(0)$ there is a zero-sum subset $S \subseteq A$ of at most 3 elements. In Chapter 5 we let $|A| = q-1$ and determine the least such integer $q_0(1)$. The proofs of our theorems in Chapter 4 and Chapter 5 are constructive.

Finally, in Chapter 6 we introduce some interesting unsolved problems related to our work in this thesis.

The appendix provides the interested reader with statements of the theorems and conjectures that are mentioned in Chapter 2 as they appear in the literature with only slight modifications of notation for consistency. We remark that some of the results and conjectures stated in the appendix use the language of residue classes, some use the language of congruences, and some use both languages interchangeably. This is because in giving these statements we have been faithful to each author's choice of language.

We have been using and will continue to use the language of residue classes. Some of the results presented herein are finite and some are asymptotic.

CHAPTER 2

HISTORICAL DEVELOPMENT

In the first section of this chapter we provide the reader with a brief history of the area of our research up through current results including our work and a deep result that N. Alon obtained in 1987. Along the way we make some claims which are related to an earlier result of Alon. In Section 2.2 and Section 2.3 we provide the reader with proofs of these claims.

2.1 Historical Background

Paul Erdös and H. Heilbronn[3] showed in 1964 that if p is prime, $A \subseteq Z_p$, $0 \notin A$, and $|A| > (3\sqrt{6})\sqrt{p}$, then there exists a nonempty subset $S \subseteq A$ such that $\sum_{s \in S} s = r$, where r is an arbitrary residue class modp. Furthermore, they conjectured, first, that this result is true if $3\sqrt{6}$ is replaced by 2 and, secondly, that this replacement can be made if p = n is composite, provided that r = 0. After several years with no success reported in proving the second conjecture, Erdös[7] asked whether it could be proved under the stronger condition that $|A| > Kn^{(\frac{1}{2}+\epsilon)}$, where $\epsilon > 0$ and K is a positive constant independent of n.

Erdös and Heilbronn's result and conjectures may not be intuitive but are plausible. For example, if we let $|A|$ be the least integer greater than or equal to $(3\sqrt{6})\sqrt{p}$, then as $p \to \infty$, $\frac{|A|}{|Z_p|} \to 0$ but $\frac{2^{|A|} - 1}{|Z_p|} \to \infty$, where $2^{|A|} - 1$ is the number of nonempty subsets $S \subseteq A$.

J. Olson[6] proved the first conjecture in 1968. C. Ryavec[7], also in 1968, answered the later question posed by Erdös affirmatively. In 1970 E. Szemerédi[9] improved Ryavec's result by obtaining $K\sqrt{n}$ as a lower bound for $|A|$. The second conjecture is still open, and Szemerédi's theorem is the best so far. Note that the results following Olson's result are asymptotic. Guy[5] gave a brief survey of related results in 1981.

Rather than attempting to improve Szemerédi's result by, for example, showing that K may be set equal to 2 or finding a value for K such that his result holds for all composite n, we proceed in a different direction from Erdös and Heilbronn's second conjecture. We add the condition that $0 < |S| \leq 3$ and set $|A|$, where $A \subseteq Z_n$ and $n = 2q+1$, equal to a value that may be greater than Szemerédi's lower bound. We then ask for those values of n, if any exist, such that A contains a zero-sum subset S that satisfies our condition.

R. Stalley[8] worked with even moduli n, $n = 2q$. He

showed that if $|A| = \frac{n}{2} = q$ and $q \geq 5$, then A always contains a zero-sum subset S of at most three elements. He obtained the same conclusion if $|A| = \frac{n}{2} - 1 = q - 1$ provided that $q \geq 8$.

After discussing these results with Stalley in 1983, M. Filaseta and D. Richman[4] showed that for every positive integer h and modulus n such that $n > n_0(h)$, if $|A| > \frac{n}{2} - h$, then A contains a zero-sum subset S of at most three elements. A result of N. Alon[1], which was communicated to M. Filaseta at MIT in 1984, implies this same conclusion if $|A| > (\frac{2}{5} + \epsilon)n$, where $\epsilon > 0$ and $n > n_0(\epsilon)$. In Section 2.2 we provide the reader with a formal statement and proof of this corollary to Alon's result[1]. We call this corollary Alon's two-fifths result. In Section 2.3 we show that, for small values of ϵ, Alon's two-fifths result improves Filaseta and Richman's result. Alon was undoubtedly aware of this improvement, but there is nothing in the literature indicating this.

Alon[2] went on to show in 1987 that, for any fixed integer $k > 1$, if $|A| > (\frac{1}{k} + \epsilon)n$, where $\epsilon > 0$ and $n > n_0(k,\epsilon)$, then there is a zero-sum subset $S \subseteq A$ such that $0 < |S| \leq k$. This is a very deep result, and we will refer to it from now on as Alon's theorem. Stalley conjectured the case $k = 3$ in 1983 before Alon proved his

results[1,2] and, since $\frac{1}{3} < \frac{2}{5}$, this case improves Alon's two-fifths result.

Alon[2] actually proved a stronger result than his theorem. He calls this result a proposition and we refer to it from now on as Alon's proposition. Alon's proposition specifies a smaller lower bound for |A| than his theorem yet still has the same conclusion. We refer to this conclusion from now on as Alon's conclusion.

2.2 Alon's Two-Fifths Result

In this section we show that Alon's result[1], Theorem A.12 in the appendix, implies the following corollary which was alluded to in Section 2.1.

COROLLARY 1. For every fixed $\epsilon > 0$, if $n > n_0(\epsilon)$ and $A \subseteq Z_n$ satisfies $|A| > (\frac{2}{5} + \epsilon)n$, then there is a subset $S \subseteq A$ such that $0 < |S| \leq 3$ and $\sum_{s \in S} s = 0$.

Proof. Theorem A.12 is stated in terms of G, an arbitrary finite abelian group. We use the contrapositive of Theorem A.12 restricted to $G = Z_n$, which reads as follows:

THEOREM A.12′ Let $A \subseteq Z_n$. Define

$$A^{(k)} = \{a_1+\cdots+a_k : a_1,\ldots,a_k \text{ are distinct elements of } A\}$$

and r_2 to be the number of elements $g\in Z_n$ such that $g+g = 0$. If

$$n + 2r_2 + 3 < 2|A| + \frac{(|A|-r_2)|A|}{2|A|-r_2},$$

then $0\in A^{(2)}$ or $A^{(2)}\cup A^{(3)} = Z_n$.

We first show that the hypotheses of Corollary 1 imply the hypothesis of Theorem A.12′. Thus, we show for every $\epsilon > 0$, that if $n > n_0(\epsilon)$ and $A \subseteq Z_n$ satisfies $|A| > (\frac{2}{5}+\epsilon)n$, then

$$(1) \qquad n + 2r_2 + 3 < 2|A| + \frac{(|A|-r_2)|A|}{2|A|-r_2}.$$

Let $\epsilon > 0$ be given and choose $n_0(\epsilon) > \frac{4}{\epsilon}$. Also, let $\mu = (\frac{2}{5}+\epsilon)n$. Since

$$r_2 = \begin{cases} 2, & n \text{ even} \\ 1, & n \text{ odd} \end{cases}$$

it follows that

$$n + 2r_2 + 3 = \begin{cases} n+7, & n \text{ even} \\ n+5, & n \text{ odd} \end{cases}$$

To establish (1) we begin by showing that

$$(2) \qquad n + 2r_2 + 3 < 2\mu + \frac{(\mu - r_2)\mu}{2\mu - r_2}.$$

Case 1 (n even). Since $n > \frac{4}{\epsilon} > \frac{6}{2+5\epsilon}$, then

$$\mu > (\tfrac{2}{5} + \epsilon)(\frac{6}{2+5\epsilon}) = \frac{6}{5}.$$

Since also $r_2 = 2$, then we have

$$\begin{aligned} 2\mu + \frac{(\mu - r_2)\mu}{2\mu - r_2} &= 2\mu + \frac{(\mu-2)\mu}{2\mu-2} \\ &= \frac{5\mu^2 - 6\mu}{2\mu - 2} \\ &= \frac{\mu(5\mu-6)}{2\mu-2} \\ &> \frac{\mu(5\mu-6)}{2\mu} \\ &= \tfrac{1}{2}(5\mu - 6) \\ &= \tfrac{5}{2}(\tfrac{2}{5} + \epsilon)n - 3 \\ &= n + \tfrac{5}{2}\epsilon n - 3 \\ &> n + \tfrac{5\epsilon}{2}(\tfrac{4}{\epsilon}) - 3 \\ &= n + 7 \end{aligned}$$

$$= \quad n + 2r_2 + 3,$$

and inequality (2) is proved.

Case 2 (n odd). From our work at the beginning of Case 1 we have that $\mu > \frac{6}{5} > \frac{3}{5}$. Also, since $n > \frac{4}{\epsilon} > \frac{13}{5\epsilon}$ and $r_2 = 1$, then

$$\begin{aligned}
2\mu + \frac{(\mu - r_2)\mu}{2\mu - r_2} &= 2\mu + \frac{(\mu-1)\mu}{2\mu-1} \\
&= \frac{5\mu^2 - 3\mu}{2\mu - 1} \\
&= \frac{\mu(5\mu-3)}{2\mu-1} \\
&> \frac{\mu(5\mu-3)}{2\mu} \\
&= \tfrac{1}{2}(5\mu - 3) \\
&= \tfrac{5}{2}(\tfrac{2}{5} + \epsilon)n - \tfrac{3}{2} \\
&= n + \tfrac{5}{2}\epsilon n - \tfrac{3}{2} \\
&> n + \tfrac{5\epsilon}{2}(\tfrac{13}{5\epsilon}) - \tfrac{3}{2} \\
&= n + 5
\end{aligned}$$

$$= \quad n + 2r_2 + 3 \ ,$$

and inequality (2) is proved again.

Next we show that

$$(3) \qquad 2\mu + \frac{(\mu - r_2)\mu}{2\mu - r_2} \quad < \quad 2|A| + \frac{(|A| - r_2)|A|}{2|A| - r_2} \ .$$

Since $n > \frac{4}{\epsilon} > \frac{5}{2+5\epsilon}$ and $|A| > \mu$, we have that

$$\begin{aligned} 2|A| - r_2 \quad &> \quad 2\mu - r_2 \\ &> \quad 2(\tfrac{2}{5} + \epsilon)(\tfrac{5}{2+5\epsilon}) \ - \ r_2 \\ &= \quad 2 - r_2 \\ &\geq \quad 0 \ ; \end{aligned}$$

and, hence, if

$$(4) \qquad \mu(\mu - r_2)(2|A| - r_2) \quad < \quad |A|(|A| - r_2)(2\mu - r_2) \ ,$$

then

$$(5) \qquad \frac{\mu(\mu - r_2)}{2\mu - r_2} \quad < \quad \frac{|A|(|A| - r_2)}{2|A| - r_2} \ .$$

Inequality (3) follows readily from inequality (5), so we show that ineqaulity (4) holds. Since $|A| > \mu$, then

$$2|A| + \mu \quad > \quad 2\mu + |A| \ .$$

From this inequality we have that

$$\begin{aligned} -2|A|r_2 - \mu r_2 &= -(2|A| + \mu)r_2 \\ &< -(2\mu + |A|)r_2 \\ &= -2\mu r_2 - |A|r_2 \ , \end{aligned}$$

and hence

$$\begin{aligned} (\mu - r_2)(2|A| - r_2) &= 2|A|\mu + r_2^2 - 2|A|r_2 - \mu r_2 \\ &< 2|A|\mu + r_2^2 - 2\mu r_2 - |A|r_2 \\ &= (|A| - r_2)(2\mu - r_2) \ . \end{aligned}$$

Inequality (4) now follows, and so inequality (3) is proved.

Inequality (1) follows from inequality (2) and inequality (3). Hence the conclusion of Theorem A.12′ holds; that is, $0 \in A^{(2)}$ or $A^{(2)} \cup A^{(3)} = Z_n$.

We now show that the conclusion of Corollary 1 follows. If $0 \in A^{(2)}$, then there exist distinct residues $a_1, a_2 \in A$ such that $a_1 + a_2 = 0$ and we let $S = \{a_1, a_2\}$. If $0 \notin A^{(2)}$, then $A^{(2)} \cup A^{(3)} = Z_n$. Hence, $0 \in A^{(2)} \cup A^{(3)}$ and so $0 \in A^{(3)}$. Thus there exist distinct residues $a_1, a_2, a_3 \in A$ such that $a_1 + a_2 + a_3 = 0$ and we let $S = \{a_1, a_2, a_3\}$. This completes the proof of Corollary 1. □

2.3 A Comparison

In this section we show that Alon's two-fifths result; that is, Corollary 1, improves Filaseta and Richman's result[4]; that is, Theorem A.11 in the appendix. We will show that, for sufficiently large n, Theorem A.11 follows from Corollary 1 but that the converse is not always true. For convenience we restate both results.

THEOREM A.11 For every positive integer h, if $n > n_0(h)$ and $A \subseteq Z_n$ satisfies $|A| > \frac{n}{2} - h$, then there exists a subset $S \subseteq A$ such that $0 < |S| \leq 3$ and $\sum_{s \in S} s = 0$.

COROLLARY 1. For every fixed $\epsilon > 0$, if $n > n_0(\epsilon)$ and $A \subseteq Z_n$ satisfies $|A| > (\frac{2}{5} + \epsilon)n$, then there is a subset $S \subseteq A$ such that $0 < |S| \leq 3$ and $\sum_{s \in S} s = 0$.

First we notice that for any fixed positive integer h, $|A| > \frac{n}{2} - h$ is equivalent to $|A| > (\frac{1}{2} - \hat{\epsilon})n$, where $\hat{\epsilon} = \frac{h}{n}$.

Next, let a positive integer h and a real number ϵ be given, where $0 < \epsilon < \frac{1}{10}$. Since $\frac{1}{2} > \frac{2}{5}$ we have $(\frac{1}{2} - \hat{\epsilon}) \geq (\frac{2}{5} + \epsilon)$ provided that n is large enough so that $\hat{\epsilon} = \frac{h}{n}$ is sufficiently small; that is, provided that $n > n_1(\epsilon)$. Hence, if $n > \max\{n_0(h), n_0(\epsilon), n_1(\epsilon)\}$, then Corollary 1 implies Theorem A.11.

Finally we give an example in which Theorem A.11 does not imply Corollary 1. Let a real number ϵ be given, where $0 < \epsilon < \frac{1}{20}$. Let h be any positive integer. Choose $n = 20s$, where s is a positive integer large enough so that $n > \max\{n_0(h), n_0(\epsilon)\}$ and $(\frac{1}{2} - \hat{\epsilon}) > \frac{9}{20}$. Finally, let $A \subseteq Z_n$ be any subset such that $|A| = \frac{9}{20}n$. We conclude our example by noticing that

$$(\tfrac{1}{2} - \hat{\epsilon})n \quad > \quad |A| \quad > \quad (\tfrac{2}{5} + \epsilon)n.$$

It follows that Corollary 1 is the stronger result.

CHAPTER 3

ALON'S THEOREM

Alon[2] actually proved a stronger result than his theorem and leaves it to the reader to show that his theorem follows. We call this stronger result Alon's proposition and show in the first section of this chapter that his theorem does, in fact, follow. His theorem and proposition appear as Theorem A.13 and Proposition A.14, respectively, in the appendix.

Alon's proposition decreases the lower bound inequality on $|A|$ from $(\frac{1}{k}+\epsilon)n$ to $\frac{n}{k} + \left(1+\sqrt{3(k-2)}\right)r_3(n)$ and has the same conclusion as his theorem. We call this conclusion Alon's conclusion. The factor $r_3(n)$ denotes the maximum cardinality of a subset $B \subseteq \{1,2,\ldots,n\}$ that contains no arithmetic progression of three terms. In the second section of this chapter we determine a specific limitation as to how much the lower bound on $|A|$ can be decreased without compromising Alon's conclusion.

We now restate both these results of Alon[2] for the reader's convenience.

THEOREM A.13 For every fixed $\epsilon > 0$ and $k > 1$, if $n > n_0(k,\epsilon)$ and $A \subseteq Z_n$ satisfies $|A| > (\frac{1}{k}+\epsilon)n$, then there

is a subset $S \subseteq A$ such that $0 < |S| \leq k$ and $\sum_{s \in S} s = 0$.

PROPOSITION A.14 Let A be a subset of Z_n of cardinality $|A| \geq \frac{n}{k} + \left(1 + \sqrt{3(k-2)}\right) r_3(n)$. Then there is a subset $S \subseteq A$ of cardinality $1 \leq |S| \leq k$ such that $\sum_{s \in S} s = 0 (\text{in } Z_n)$.

3.1 A Note on the Proof of Alon's Theorem

To show that Alon's proposition implies his theorem and is the stronger result, we need only show, for fixed $\epsilon > 0$ and $k > 1$, that $\left(1 + \sqrt{3(k-2)}\right) r_3(n) < \epsilon n$ for sufficiently large n. Notice that Alon's proposition makes no reference to a lower bound restriction on the size of n. However, even if such a restriction did appear, it would not affect what we do here. We show this inequality by using a result that K. F. Roth[2] proved more than 30 years ago and which Alon[2] cites: $r_3(n) \leq O\left(\frac{n}{\log \log n}\right)$. Letting $\epsilon > 0$ and $k > 1$ be given, we have that

$$\left(1 + \sqrt{3(k-2)}\right) r_3(n) \leq \left(1 + \sqrt{3(k-2)}\right) \frac{Kn}{\log \log n} < \epsilon n ,$$

for K some positive constant and n sufficiently large.

3.2 A Lower Bound Limitation

A natural question to ask is whether the term $\left(1+\sqrt{3(k-2)}\right)r_3(n)$ can be replaced by another non-decreasing function $f(n,k) < \left(1+\sqrt{3(k-2)}\right)r_3(n)$ in the statement of Alon's proposition without compromising his conclusion for any $k > 1$. In particular, we ask if this term can be replaced by some fixed real number $c \geq 0$ such that, once this replacement is made, his conclusion holds for all $k > 1$. In Theorem 2 below we show that for any such constant $c \geq 0$, no matter how large, this replacement cannot be made in the sense that if $k > 2c+3$ and $n \geq k(k-c-1)$ then Alon's conclusion fails to hold for at least one set $A \subseteq Z_n$ such that $|A| > \frac{n}{k}+c$. In Theorem 3 we show that this replacement cannot be made if $k = 3$ and $0 \leq c < \frac{2}{3}$. Following Theorem 4 and Theorem 5 we conjecture a best possible replacement if $k \geq 3$. In Theorem 7 we show that if $k = 2$, then the replacement $c = 0$ can be made.

THEOREM 2. For every fixed real number $c \geq 0$, integer $k > 2c+3$, and integer $n \geq k(k-c-1)$ there is a set $A \subseteq Z_n$ such that $|A| > \frac{n}{k}+c$ and such that there is no subset $S \subseteq A$ where $0 < |S| \leq k$ and $\sum_{s\in S} s = 0$.

Proof. Let $c \geq 0$, $k > 2c+3$, and $n \geq k(k-c-1)$ be

given and consider the set $A \subseteq Z_n$ defined by $A = \{i \mid 1 \leq i \leq x\}$, where $x \geq 1$. Note that $|A| = x$ and that the subsets S of A, such that $0 < |S| \leq k$, whose elements form the smallest possible sum and largest possible sum are $S = \{1\}$ and $S = \{x, x-1, \ldots, \max\{1, x-k+1\}\}$, respectively. Thus, the theorem is proved if we can show the existence of at least one integer solution x to the following system of inequalities:

$$(1) \qquad \begin{cases} x \geq 1 \\ x > \frac{n}{k} + c \\ n > x + (x-1) + \cdots + \max\{1, x-k+1\} . \end{cases}$$

First, we notice that for all $n \geq 1$, the first two inequalities in (1) are satisfied simultaneously if $x > \frac{n}{k} + c$; so (1) reduces to

$$(2) \qquad \begin{cases} x > \frac{n}{k} + c \\ n > x + (x-1) + \cdots + \max\{1, x-k+1\} . \end{cases}$$

Furthermore, $n \geq k(k-c-1)$ implies that $\frac{n}{k} + c \geq k-1$. Therefore, $x > \frac{n}{k} + c$ implies that $x \geq k$ and from this it follows that $x-k+1 \geq 1$. Thus,

$$\max\{1, x-k+1\} = x-k+1 ,$$

and the system (2) reduces to

$$(3) \qquad \begin{cases} x > \frac{n}{k} + c \\ n > x + (x-1) + \cdots + (x-k+1) \ . \end{cases}$$

Since

$$n > x + (x-1) + \cdots + (x-k+1) = \frac{k}{2}[(x-k+1) + x]$$

$$= kx + \frac{k-k^2}{2} \ ,$$

then $kx < n + \frac{k^2-k}{2}$, and (3) reduces to

$$(4) \qquad \begin{cases} x > \frac{n}{k} + c \\ x < \frac{n}{k} + \frac{k-1}{2} \ . \end{cases}$$

Since $k > 2c+3$, then

$$(\frac{n}{k} + \frac{k-1}{2}) - (\frac{n}{k} + c) = \frac{k-1}{2} - c$$

$$> \frac{(2c+3)-1}{2} - c$$

$$= 1 \ ,$$

and so (4) has at least one integer solution x. This completes the proof of the theorem. □

We remark that we state Theorem 2 for $n \geq k(k-c-1)$ because this is sufficient to insure $x \geq k$ which greatly simplifies the task of showing that (1) has an integer solution. However, by imposing this requirement we lose integer solutions x for smaller values of n. There are two cases; namely, (i) $n < k(k-c-1)$ and $x \geq k$, and (ii) $n < k(k-c-1)$ and $1 \leq x < k$. We give an example of an integer solution to (1) for each case.

Example 1. Let $c = 0$ and $k = 4$. Then we require $n < k(k-c-1) = 12$. Let $n = 11$. Choose $x = 4$ so that $x \geq k = 4$ and $x > \frac{n}{k} + c = \frac{11}{4}$. So $\max\{x-3, 1\} = 1$ and we have that $n = 11 > 4+3+2+1 = 10$. Hence, $x = 4$ is a solution.

Example 2. Let $c = 0$ and $k = 4$. Then we require $n < 12$ as we did in example 1 above. Let $n = 7$. Choose $x = 2$ so that $x < k = 4$ and $x > \frac{n}{k} + c = \frac{7}{4}$. So $\max\{x-3, 1\} = 1$ and we have that $n = 7 > 2+1 = 3$. Hence $x = 2$ is a solution.

We remark further that we state Theorem 2 for $k > 2c+3$ because in our proof of the theorem this is a

sufficient condition for the system (4) to have an integer solution. However, it may not be necessary. Therefore, in addition to losing integer solutions x to (1) for smaller values of n, we may also be losing such solutions for smaller values of k.

The loss of such solutions to (1) does not affect our purpose, however, which is to show that for any real constant $c \geq 0$, no matter how large, Alon's conclusion sometimes fails to hold for sufficiently large k and n; that is, for $k > k_0(c)$ and $n > n_0(k,c)$, if we only require $|A| > \frac{n}{k} + c$. Furthermore, we have shown that Alon's conclusion sometimes fails to hold for any $k > 3$ and $n \geq k(k-1)$ if we only require $|A| > \frac{n}{k}$.

In Theorem 3 below we show, but only for certain arbitrarily large values of n, that Alon's conclusion sometimes fails to hold when $k = 3$ under the restriction $|A| > \frac{n}{k} + c$ if $0 \leq c < \frac{2}{3}$. When we write that a result is true for arbitrarily large values of n, we mean that for any modulus n_0 a modulus n larger than n_0 can be found for which the result is true.

THEOREM 3. If $k = 3$ and $0 \leq c < \frac{2}{3}$, then there exist arbitrarily large integers n and a set $A \subseteq Z_n$ for each such n, so that $|A| > \frac{n}{3} + c$ and so that there is no

subset $S \subseteq A$ where $0 < |S| \leq 3$ and $\sum_{s \in S} s = 0$.

Proof. Let c be given such that $0 \leq c < \frac{2}{3}$ and let $n = 3q+1$, where $q \geq 2$. Let $A = \{1, \ldots, q+1\}$. Then $|A| = q+1 = \frac{n-1}{3} + 1 = \frac{n}{3} + \frac{2}{3} > \frac{n}{3} + c$. The subsets S of A, where $0 < |S| \leq 3$, whose elements form the smallest possible sum and largest possible sum are $S = \{1\}$ and $S = \{q+1, q, q-1\}$, respectively. Since

$$(q+1) + q + (q-1) = 3q < n ,$$

the theorem is proved. □

We remark here that the condition $c \geq 0$ is not used in the proofs of Theorem 2 and Theorem 3, but these theorems are stated for $c \geq 0$ so that it is clear that Alon's conclusion does not always hold for $k \geq 3$ if we only require $|A| > \frac{n}{k}$.

The hypotheses of Theorem 2 include three restrictions; namely, $c \geq 0$ a fixed real number, $k > 2c+3$ an integer, and $n \geq k(k-c-1)$ an integer. An alternative form for the first two of these restrictions is $k > 3$ a fixed integer and c a real number such that $0 \leq c < \frac{k-3}{2}$. Thus, if we choose k first we have an upperbound restriction on c which is a function of k. In Theorem 4

and Theorem 5, which follow, we increase this upperbound on c for $k = 4$ and $k = 5$, but only for certain arbitrarily large values of n dependent on k that are specified in the proofs of these theorems. These theorems suggest that, in a similar way, the upperbound restriction on c can be increased for each $k > 5$.

THEOREM 4. If $k = 4$ and $\frac{1}{2} \leq c < \frac{5}{4}$, then there exist arbitrarily large integers n and a set $A \subseteq Z_n$ for each such n, so that $|A| > \frac{n}{4} + c$ and so that there is no subset $S \subseteq A$ where $0 < |S| \leq 4$ and $\sum_{s \in S} s = 0$.

Proof. Let c be given such that $\frac{1}{2} \leq c < \frac{5}{4}$ and let $n = 4q+3$, where $q \geq 2$. Let $A = \{1, \ldots, q+2\}$. Then $|A| = q+2 = \frac{n-3}{4} + 2 = \frac{n}{4} + \frac{5}{4} > \frac{n}{4} + c$. The subsets S of A, where $0 < |S| \leq 4$, whose elements form the smallest possible sum and largest possible sum are $S = \{1\}$ and $S = \{q+2, q+1, q, q-1\}$, respectively. Since

$$(q+2) + (q+1) + q + (q-1) = 4q + 2 < n ,$$

the theorem is proved. □

THEOREM 5. If $k = 5$ and $1 \leq c < \frac{9}{5}$, then there exist arbitrarily large integers n and a set $A \subseteq Z_n$ for

each such n, so that $|A| > \frac{n}{5} + c$ and so that there is no subset $S \subseteq A$ where $0 < |S| \leq 5$ and $\sum_{s \in S} s = 0$.

Proof. Let c be given such that $1 \leq c < \frac{9}{5}$ and let $n = 5q+1$, where $q \geq 3$. Let $A = \{1, \ldots, q+2\}$. Then $|A| = q+2 = \frac{n-1}{5} + 2 = \frac{n}{5} + \frac{9}{5} > \frac{n}{5} + c$. The subsets S of A, where $0 < |S| \leq 5$, whose elements form the smallest possible sum and largest possible sum are $S = \{1\}$ and $S = \{q+2, q+1, q, q-1, q-2\}$, respectively. Since

$$(q+2) + (q+1) + q + (q-1) + (q-2) = 5q < n ,$$

the theorem is proved. □

We remark that had we stated Theorem 3 for c such that $0 \leq c < \frac{1}{3}$, we could also have shown that Alon's conclusion sometimes fails to hold when $k = 3$ if $n = 3q+2$, where $q \geq 2$. However, we wanted to maximize the upperbound on c, not the number of specific forms of the arbitrarily large values of n. Likewise, in Theorem 4 and Theorem 5 we maximize the upperbound on c at the expense of showing for fewer specific forms of the arbitrarily large values of n that Alon's conclusion sometimes fails to hold. The observation of this trade-off between maximizing c and maximizing the number of specific forms of the arbitrarily large moduli n leads us to a conjecture.

CONJECTURE 6. Let $A \subseteq Z_n$. For each integer $k \geq 3$ there exists a real number $c_0(k) > 0$ such that

(1) for all $c > c_0(k)$ Alon's conclusion holds if we only require $|A| > \frac{n}{k} + c$, where $n > n_0(k,c)$, and

(2) for all $c < c_0(k)$ Alon's conclusion sometimes fails to hold for arbitrarily large n under the same restriction on $|A|$.

Finally, we show that Alon's conclusion does hold when $k = 2$ if we only require $|A| > \frac{n}{k}$.

THEOREM 7. If $n > 0$, and $A \subseteq Z_n$ satisfies $|A| > \frac{n}{2}$, then there is a subset $S \subseteq A$ such that $0 < |S| \leq 2$ and $\sum_{s \in S} s = 0$.

Proof. If $n = 1$, then zero is the only residue and we are done.

If $n \geq 2$, let $n = 2q+r$, where $r = 0$ or $r = 1$. Then $|A| > \frac{n}{2}$ implies that $|A| \geq q+1$.

First suppose that $r = 0$. We have $A \subseteq (B \cup C)$ where $B = \{\pm i \mid 1 \leq i \leq q-1\}$ and $C = \{0,q\}$ are sets of residue classes mod n. We may assume $0 \notin A$ since otherwise the conclusion of the theorem is true. Hence, we have that

$$q+1 \leq |A| = |A \cap (B \cup C)|$$

$$= |(A \cap B) \cup (A \cap C)|$$

$$= |A \cap B| + |A \cap C| .$$

Since $|A \cap C| = 0$ or 1, it follows that $|A \cap B| \geq q$ and so $\{i, -i\} \subseteq A$ for some i. Hence, we let $S = \{i, -i\}$.

In a similar way we prove the theorem for $r = 1$. In this case we have $A \subseteq (B \cup C)$, where $B = \{\pm i \mid 1 \leq i \leq q\}$ and $C = \{0\}$ are sets of residue classes mod n. Once again we may assume that $0 \notin A$. Hence, we have that

$$q+1 \leq |A| = |A \cap (B \cup C)|$$

$$= |(A \cap B) \cup (A \cap C)|$$

$$= |A \cap B| + |A \cap C|$$

$$= |A \cap B| .$$

Once again we have that $\{i, -i\} \subseteq A$ for some i and we let $S = \{i, -i\}$. This completes the proof. □

For sets A of smaller cardinality; that is, sets A

such that $|A| \leq \frac{n}{2}$, the conclusion of Theorem 7 does not always follow according to the example $A = \{1, 2, \ldots, q\}$. In this sense, Theorem 7 is the best possible result for $k = 2$.

CHAPTER 4

SETS OF q RESIDUE CLASSES MOD(2q+1)

The work of N. Alon[2] shows that if $A \subseteq Z_n$ and $|A| > (\frac{1}{3}+\epsilon)n$, for some fixed $\epsilon > 0$, then there exists a subset $S \subseteq A$ such that $0 < |S| \leq 3$ and $\sum_{s\in S} s = 0$ provided that $n > n_0(\epsilon)$. In this chapter we deterimine exactly how large n must be for odd moduli given a certain more severe constraint on the size of A. In particular, we set $n = 2q+1$, where $q \geq 1$, and restrict the sets A to those that satisfy $|A| = q$. We then determine the smallest integer $q_0(0)$ such that for all $q \geq q_0(0)$ any such A contains a zero-sum subset S of at most three residue classes modn. Notice that given this constraint on A, there does exist a sufficiently small fixed $\epsilon > 0$ such that $|A| > (\frac{1}{3}+\epsilon)n$ for all sufficiently large odd n since $\lim_{q\to\infty} \frac{|A|}{n} = \frac{1}{2}$. Therefore, Alon's theorem assures us that such a $q_0(0)$ exists. We then state and prove two theorems for smaller values of q. Specifically, for each $q < q_0(0)$ we determine whether every set A of q residue classes mod(2q+1) contains at least one zero-sum subset S and, if so, the smallest integer $t_0(q)$ so that every set A contains at least one zero-sum subset S such that $0 < |S| \leq t_0(q) \leq q$. All of our proofs are constructive.

4.1 The General Theorem ($q \geq 6$)

THEOREM 8. Any set A of q residue classes mod(2q+1), where $q \geq 6$, has a nonempty subset S of at most three residue classes that sum to zero mod(2q+1), with three residue classes necessary for some sets A.

Proof. First we notice that at least three residue classes are necessary for some sets A because of the sets $A = \{i \mid 1 \leq i \leq q\}$ since no two residue classes from 1 to q can sum to zero mod(2q+1).

Next we show that no more than three residue classes are necessary for any set A. Let $B = \{\pm i \mid 1 \leq i \leq q\}$ and $C = \{0\}$. Then $B \cup C = Z_{2q+1}$. We may assume $0 \notin A$, for otherwise we let $S = \{0\}$. Therefore, we may assume $A \subseteq B$. Also, for any i such that $1 \leq i \leq q$, we may assume $\{i,-i\} \not\subseteq A$ since otherwise we let $S = \{i,-i\}$. Hence,

$$
\begin{aligned}
q = |A| &= |A \cap B| \\
&= |A \cap \left(\bigcup_{i=1}^{q} \{i,-i\} \right)| \\
&= |\bigcup_{i=1}^{q} (A \cap \{i,-i\})| \\
&= \sum_{i=1}^{q} |A \cap \{i,-i\}| \ .
\end{aligned}
$$

Since $|A \cap \{i,-i\}| = 0$ or 1, then $|A \cap \{i,-i\}| = 1$ for each i. In otherwords, for each i such that $1 \leq i \leq q$ either $i \in A$ or $-i \in A$. Next, we may assume $1 \in A$ since if $-1 \in A$, then the residue classes of A may be replaced by their negatives without changing the validity of the theorem. This is because zero sums will not be affected by this change.

We give an example. Even though $q \geq 6$ in the statement of the theorem we take $q = 3$ for simplicity. If $q = 3$, then the four possibilities remaining for A after the above elimination process are $A_1 = \{1,2,3\}$, $A_2 = \{1,-2,3\}$, $A_3 = \{1,2,-3\}$, and $A_4 = \{1,-2,-3\}$. This concludes our example and we continue with our proof of the theorem.

Notice that if $i \in A$, where $2 \leq i \leq q-1$, then we may assume $(i+1) \in A$ for, otherwise, we let $S = \{1,i,-(i+1)\}$. Thus, for i and j such that $2 \leq i < j \leq q$, $i \in A$ implies $j \in A$. By the contrapositive it follows that $-j \in A$ implies $-i \in A$. Therefore, in the above example A_3 is also eliminated.

Consider the following possibilities for A: (1) $3 \in A$, (2) $-q \in A$, and (3) $-3 \in A$ and $q \in A$. Notice that these are all of the possible cases and that these cases do not overlap since $3 \in A$ implies $q \in A$ and $-q \in A$ implies

$-3 \in A$. If $3 \in A$, then $(q-2) \in A$ and $q \in A$, and we let $S = \{3, q-2, q\}$. If $-q \in A$, then $-(q-2) \in A$ and $-3 \in A$, and we let $S = \{-3, -(q-2), -q\}$. (Notice that this proof is invalid for $q = 5$ because of the two previous subsets S. As will be seen later, the theorem is not true for $1 \leq q \leq 5$.) Now suppose that $-3 \in A$ and $q \in A$. If $4 \in A$, then $5 \in A$. Since $-3 \in A$, then $-2 \in A$ and we let $S = \{-2, -3, 5\}$. If $-4 \in A$, then there is some j, with $4 \leq j \leq q-1$, such that $-j \in A$ and $(j+1) \in A$. Since $-j \in A$, it follows that $-(j-1) \in A$ and we let $S = \{-2, -(j-1), j+1\}$. This completes the proof. □

A comment regarding our choice of cases in the proof of Theorem 8 is appropriate before proceeding further. Although Theorem 8 is not true for $q = 5$, a modified version, Theorem 10 which follows, is true. In our proof of Theorem 10 we will look at those sets A for which the proof of Theorem 8 is invalid in the event $q = 5$. The number of these exceptional sets A can be reduced by choosing our cases in the proof of Theorem 8 to be (1) $2 \in A$, (2) $-q \in A$, (3) $-2 \in A$ and $q \in A$. However, this alternative choice of cases lengthens the proof of Theorem 8. Since simplicity in the proof of the general Theorem 8 is our primary goal, the inconvenience of having to deal with a greater number of exceptional sets A in our proof of Theorem 10 is judged worthwhile. This

goal of simplicity in the proof of a general theorem also guides our choice of cases in the proof of the general Theorem 11, which follows in Chapter 5.

We now continue with Theorems 9 and 10 and their proofs.

4.2 The Theorems for $1 \leq q \leq 4$ and $q = 5$

THEOREM 9. If $1 \leq q \leq 4$, then for each q there exists at least one set A of q residue classes mod$(2q+1)$ which does not have a nonempty, zero-sum subset S.

Proof. If $q = 4$ we let $A = \{1,-2,3,4\}$; if $q = 3$ we let $A = \{1,2,3\}$; if $q = 2$ we let $A = \{1,2\}$; and if $q = 1$ we let $A = \{1\}$. □

THEOREM 10. Any set A of 5 residue classes mod 11, has a nonempty subset S of at most 5 residue classes whose sum is zero mod 11, with five residue classes necessary for some sets A.

Proof. The parts of the proof of Theorem 8 which are invalid for $q = 5$ are cases (1) $3 \in A$ and (2) $-q \in A$. If $3 \in A$, then we note that either $2 \in A$ or $-2 \in A$ but not both. Thus the only two possibilities for A are the sets

$A_1 = \{1,-2,3,4,5\}$ and $A_2 = \{1,2,3,4,5\}$. With respect to A_1, the only nonempty subset whose elements sum to zero mod 11 is $S = A_1$. With respect to A_2, we let $S = \{2,4,5\}$. If $-q \in A$, then the only possibility for A is the set $A_3 = \{1,-2,-3,-4,-5\}$ and we let $S = \{-2,-4,-5\}$. This completes the proof. □

CHAPTER 5

SETS OF (q−1) RESIDUE CLASSES MOD(2q+1)

In this chapter we consider subsets $A \subseteq Z_n$, where $n = 2q+1$ and $q \geq 2$, such that $|A| = q-1$ and we determine the smallest integer $q_0(1)$ such that for all $q \geq q_0(1)$ any such A contains a zero-sum subset S of at most three residue classes modn. Once again, reasoning as we do at the beginning of Chapter 4, Alon's theorem assures us that $q_0(1)$ exists. We then state and prove three theorems for smaller values of q. All of our proofs in this chapter are constructive. As expected, the results in this chapter are somewhat deeper than those in Chapter 4.

5.1 The General Theorem ($q \geq 8$) and the Theorem for $2 \leq q \leq 5$

THEOREM 11. Any set A of (q−1) residue classes mod(2q+1), where $q \geq 8$, has a nonempty subset S of at most three residue classes that sum to zero mod(2q+1), with three residue classes necessary for some sets A.

Proof. First we notice that at least three residue classes are necessary for some sets A because of the sets $A = \{i \mid 1 \leq i \leq q-1\}$ since no two residue classes from 1 to

$(q-1)$ can sum to zero $\bmod(2q+1)$.

Next we show that no more than three residue classes are necessary for any set A. Once again let $B = \{\pm i \mid 1 \leq i \leq q\}$ and $C = \{0\}$ so that $B \cup C = Z_{2q+1}$. As in the proof of Theorem 8 we may assume that $0 \notin A$ and $\{i,-i\} \not\subseteq A$ for $1 \leq i \leq q$. Hence again, $A \subseteq B$ and

$$q-1 = |A| = |A \cap B| = \sum_{i=1}^{q} |A \cap \{i,-i\}| .$$

Since $|A \cap \{i,-i\}| = 0$ or 1, then there is exactly one d, where $1 \leq d \leq q$, such that $|A \cap \{d,-d\}| = 0$. Furthermore, for $1 \leq i \leq q$ and $i \neq d$, $|A \cap \{i,-i\}| = 1$. In other words, for each i such that $1 \leq i \leq q$ and $i \neq d$ either $i \in A$ or $-i \in A$. Next, let g be the residue class from A having the smallest absolute value. We may assume $g > 0$ since all of the residue classes of A may be replaced by their negatives without changing the validity of the theorem. This is because zero sums will not be affected by this change. Futhermore, if $d \neq 1$, then $1 \in A$ and, similarly, if $d = 1$, then $2 \in A$. The remainder of the proof will be organized by cases on d.

Consider $d > 1$. We know then that $1 \in A$. Also, if $i \in A$ and $2 \leq i \leq d-2$ or $d+1 \leq i \leq q-1$, then it follows that $(i+1) \in A$ since, otherwise, we let $S = \{1, i, -(i+1)\}$. Therefore, if $2 \leq i < j \leq d-1$ or $d+1 \leq i < j \leq q$, then

$i \in A$ implies that $j \in A$. By the contrapositive we also have that $-j \in A$ implies $-i \in A$. This result is useful in all of the cases on d that follow except for the case $d = 1$ for which there is a similar, but different, result. Accordingly, we will save the proof of the case $d = 1$ until last since we wish to begin with the most general case first, namely, the case where $4 \leq d \leq q-3$.

Case 1 ($4 \leq d \leq q-3$). First suppose that $-(q-1) \in A$. It follows that $-(q-2) \in A$ and $-(d+1) \in A$. If $2 \in A$, then $(d-1) \in A$ and we let $S = \{2, d-1, -(d+1)\}$. If $-2 \in A$ and $q \in A$, we let $S = \{-2, -(q-2), q\}$. If $-2 \in A$ and $-q \in A$, we let $S = \{-2, -(q-1), -q\}$.

Next suppose that $(q-1) \in A$. This implies that $q \in A$. If $2 \in A$, we let $S = \{2, q-1, q\}$. If $-2 \in A$, we consider the subcases $-(d+1) \in A$ and $(d+1) \in A$. If $-(d+1) \in A$, then there is some j, with $d+1 \leq j \leq q-2$, such that $-j \in A$ and $(j+2) \in A$. So we let $S = \{-2, -j, j+2\}$. Now assume that $(d+1) \in A$. If it is also true that $-(d-1) \in A$, then we let $S = \{-2, -(d-1), d+1\}$. If, however, we have that $(d-1) \in A$, then there is some j, with $2 \leq j \leq d-2$, such that $-j \in A$ and $(j+1) \in A$. If $j \geq 4$, we let $S = \{-2, -(j-1), j+1\}$. If $j = 3$, then $4 \in A$, and since $(d+1) \in A$ we have $(q-2) \in A$; so we let $S = \{4, q-2, q-1\}$. If $j = 2$, then $3 \in A$ and again $(q-2) \in A$, and hence we let $S = \{3, q-2, q\}$.

Case 2 ($d = 2$). If $3 \in A$, then $(q-2) \in A$ and $q \in A$. Hence we let $S = \{3, q-2, q\}$. If $-q \in A$, then $-(q-2) \in A$ and $-3 \in A$. Thus we let $S = \{-3, -(q-2), -q\}$. If $-3 \in A$ and $q \in A$, then there is some j, with $3 \leq j \leq q-1$, such that $-j \in A$ and $(j+1) \in A$. If $j \geq 6$, then $-(j-2) \in A$ and we let $S = \{-3, -(j-2), j+1\}$. If $j = 4$ or $j = 5$, then $-3 \in A$, $-4 \in A$, and $7 \in A$. Hence we let $S = \{-3, -4, 7\}$. If $j = 3$, then $4 \in A$, $(q-2) \in A$, and $(q-1) \in A$. So we let $S = \{4, q-2, q-1\}$.

Case 3 ($d = 3$). If $4 \in A$, then $(q-2) \in A$ and $(q-1) \in A$. Therefore we let $S = \{4, q-2, q-1\}$. If $-(q-1) \in A$, then $-(q-2) \in A$ and $-4 \in A$. Thus we let $S = \{-4, -(q-2), -(q-1)\}$. If $-4 \in A$ and $(q-1) \in A$, then $q \in A$ and there is some j, with $4 \leq j \leq q-2$, such that $-j \in A$ and $(j+2) \in A$. If $-2 \in A$, then we let $S = \{-2, -j, j+2\}$. If $2 \in A$, we let $S = \{2, q-1, q\}$.

Case 4 ($d = q-2$ and $d = q-1$). First suppose that $4 \in A$, which implies $(q-3) \in A$. If it is also true that $q \in A$, then we let $S = \{4, q-3, q\}$. (Notice that because of this set S this is the first instance of this proof being invalid for $q = 7$. As will be seen later, this theorem is false if $2 \leq q \leq 7$.) If instead we have $3 \in A$ and $-q \in A$, then we let $S = \{3, q-3, -q\}$. If, however, $-3 \in A$ and $-q \in A$, then we let $S = \{-2, -3, 5\}$ since $-3 \in A$ implies $-2 \in A$ and $4 \in A$ implies $5 \in A$.

Next suppose that $-(q-3)\in A$. This implies $-4\in A$ and $-3\in A$. If we also have $q\in A$, then we let $S = \{-3,-(q-3),q\}$. If instead we have $-q\in A$, then we let $S = \{-4,-(q-3),-q\}$.

Finally, suppose that $-4\in A$ and $(q-3)\in A$. In this case there is some j, with $4 \leq j \leq q-4$, such that $-j\in A$ and $(j+1)\in A$. Hence we let $S = \{-2,-(j-1),j+1\}$.

Case 5 $(d = q)$. If $3\in A$, then $4\in A$, $(q-2)\in A$, and $(q-1)\in A$. Therefore we let $S = \{4,q-2,q-1\}$. If $-(q-1)\in A$, then $-(q-2)\in A$ and $-4\in A$. So we let $S = \{-4,-(q-2),-(q-1)\}$. If $-3\in A$ and $(q-1)\in A$, then $-2\in A$ and there is some j, with $3 \leq j \leq q-3$, such that $-j\in A$ and $(j+2)\in A$. Thus we let $S = \{-2,-j,j+2\}$.

Case 6 $(d = 1)$. Since $1\notin A$ it follows that $2\in A$. Therefore, we may assume further that if $i\in A$, where $3 \leq i \leq q-2$, then $(i+2)\in A$ since, otherwise, $-(i+2)\in A$ and we let $S = \{2,i,-(i+2)\}$. Thus, if $3 \leq i < j \leq q$ and $(j-i)$ is even, then $i\in A$ implies $j\in A$ and, by the contrapositive, $-j\in A$ implies $-i\in A$.

If $(q-1)\in A$ and $q\in A$, then we let $S = \{2,q-1,q\}$.

If $-(q-1)\in A$ and $-q\in A$, then $-3\in A$ and $-(q-2)\in A$. Hence we let $S = \{-3,-(q-2),-q\}$.

If $-(q-1)\in A$ and $q\in A$, then $-(q-3)\in A$. If we also have

that $-3 \in A$, then we let $S = \{-3,-(q-3),q\}$. If instead we have that $3 \in A$, then $(q-2) \in A$ since, otherwise, $-(q-2) \in A$ and $-(q-1) \in A$ would imply $-3 \in A$. Thus we let $S = \{3,q-2,q\}$.

If $(q-1) \in A$ and $-q \in A$, then $-(q-2) \in A$. If we also have that $-3 \in A$, then we let $S = \{-3,-(q-2),-q\}$. If instead we have that $3 \in A$, then $(q-3) \in A$ since, otherwise, $-(q-3) \in A$ and $-(q-2) \in A$ would imply $-3 \in A$. Therefore we let $S = \{3,q-3,-q\}$. This completes case 6 and the proof of the theorem. □

THEOREM 12. If $2 \leq q \leq 5$, then for each q there exists at least one set A of $(q-1)$ residue classes $\bmod(2q+1)$ which does not have a nonempty, zero-sum subset S.

Proof. If $q = 5$ let $A = \{1,2,3,4\}$; if $q = 4$ let $A = \{1,2,3\}$; if $q = 3$ let $A = \{1,2\}$; and if $q = 2$ let $A = \{1\}$. □

5.2 Methods of Proof for q = 6 and q = 7

A few preliminary comments are in order before we begin the proofs of the theorems for $q = 6$ and $q = 7$. Parts of our proof of Theorem 11 are invalid for $q = 6$ and for $q = 7$. However, this does not mean that the theorem is false for these values. In the remainder of

this chapter we determine those sets A for which the proof of Theorem 11 is invalid when $q = 6$ or $q = 7$, then determine for which of these sets Theorem 11 is false, and finally proceed to examine these latest sets to complete the proofs of the theorems for $q = 6$ and for $q = 7$.

We consider six methods for finding the sets A, if any exist, of $(q-1)$ residue classes, when $q = 6$ or $q = 7$, which have no nonempty zero-sum subsets S or which have only zero-sum subsets S of four or more residue classes. These six methods correspond to the steps, which we describe in detail below, of a six step screening process. The steps are numbered 0 through 5. The methods are correspondingly numbered 0 through 5. A method consists of applying a certain number of steps of the screening process, starting from step 0, followed by analyzing the remaining sets A for nonempty zero-sum subsets S of minimal cardinality. For example, method 2 consists of applying step 0, step 1, and step 2 of the screening process followed by the aforementioned analysis. Methods 4 and 5 will soon appear to be the best. We now describe each step of the screening process while keeping in mind that any set A of $(q-1)$ residue classes $\mathrm{mod}(2q+1)$ is a subset of $B \cup C$, where B and C are defined in the proof of Theorem 11. Step 1, step 2,

step 4, and step 5 of the screening process filter out sets A for which the proof of Theorem 11 is valid. In step 0 we consider all sets A of $(q-1)$ residue classes $\bmod(2q+1)$. Step 3 of the process filters out sets A which when paired with certain retained sets form pairs of sets for which the proof of Theorem 11 is valid for either both members or neither member of the pair.

Step 0. Consider all sets A of $(q-1)$ residue classes $\bmod(2q+1)$.

Step 1. Retain only those sets A such that $0 \notin A$.

Step 2. Retain only those sets A such that $\{i,-i\} \not\subseteq A$ for $1 \leq i \leq q$.

Step 3. Retain only those sets A such that the (nonzero) residue class g from A having smallest absolute value is positive.

Step 4. Retain only those sets A such that one of the following holds:

a. If $d \neq 1$, then $i \in A$ implies $j \in A$ provided that $2 \leq i < j \leq d-1$

or $d+1 \leq i < j \leq q$.

b. If $d = 1$, then $i \in A$ implies $j \in A$ provided that $3 \leq i < j \leq q$ and $(j-i)$ is even.

Step 5. Of the sets A which remain after step 4, screen out those for which the proof of Theorem 11 is valid according to the following procedure:

First, examine the separate cases on d in the proof of the theorem and determine exactly where each case is invalid for $q = 6$ or for $q = 7$.

Second, list those sets A remaining after step 4 that satisfy the descriptions of sets affected by these invalid parts of the proof. Those sets A for which the proof of Theorem 11 is valid are not listed and hence are screened out.

Table 1, which follows, lists the number of sets A that remain after each successive step of the screening process. Equivalently, the table gives the number of

sets A which must be analyzed for zero-sum subsets S of minimal cardinality under the corresponding method. The number of sets remaining after steps 0 through 3 is determined by using elementary counting methods. The number of sets remaining after steps 4 and 5 is determined by enumerating them.

TABLE 1. Sets Remaining After Each Step of the Screening Process

After Step	Number of Sets Remaining		
	q = 6	q = 7	Total
0	$\binom{13}{5} = 1287$	$\binom{15}{6} = 5005$	6292
1	$\binom{12}{5} = 792$	$\binom{14}{6} = 3003$	3795
2	$\binom{6}{5}\cdot 2^5 = 192$	$\binom{7}{6}\cdot 2^6 = 448$	640
3	$\binom{6}{5}\cdot 2^4 = 96$	$\binom{7}{6}\cdot 2^5 = 224$	320
4	44	68	112
5	32	13	45

A computer can be programmed to perform part or all of the sequence of steps from 0 through 4 of the screening process and to individually analyze the remaining sets A for zero-sum subsets of minimal cardinality. It is in step 5 where one is required to closely analyze the logic of the proof of Theorem 11 at a level where it is no longer practical to program a computer. Step 5, requiring the type of analysis that it

does, is what persuaded us to choose method 5 over the other methods. The fact that there are fewer sets A to individually analyze under method 5 is of secondary importance to us. Having made our choice, we found ourselves meticulously examining the proof of Theorem 11. During this process we acquired deeper insight into the proof and rewrote parts of it, not because they were flawed, but because we saw more efficient ways of organizing them.

5.3 The Theorems for q = 6 and q = 7

We now prove our results for q = 6 and q = 7 following the style of deferring the statements of these theorems until the end of the section. Under method 5 the 45 sets A that must be analyzed for zero-sum subsets S of minimal cardinality arise from the parts of the proof of Theorem 11 that are invalid for q = 6 or for q = 7. Table 2 on the following page indicates the validity or invalidity of the proof of Theorem 11 for these values of q with respect to cases on d.

In Table 2 invalid is written when we mean that all or part of the proof is invalid for that particular value of q and case on d. Note that Case 1 is vacuous when q = 6.

TABLE 2. Validity of the Proof of Theorem 11

Case	q=6	q=7
1 ($4 \leq d \leq q-3$)	Vacuous	Valid
2 ($d=2$)	Invalid	Valid
3 ($d=3$)	Invalid	Valid
4 ($d=q-2$)	Invalid	Invalid
4 ($d=q-1$)	Invalid	Invalid
5 ($d=q$)	Invalid	Valid
6 ($d=1$)	Invalid	Valid

Table 3 on the following page is organized by cases on d and displays the result of applying method 5 when q = 6. Thus Table 3 contains a list of the 32 sets A that remain after applying step 0 through step 5 of the screening process when q = 6. Furthermore, we list with each set A its zero-sum subsets S of minimal cardinality. Table 4 is the same as Table 3 except that q = 7.

Examination of Table 3 and Table 4 shows that Theorem 11 is false for q = 6 and q = 7. For both these values of q, although each listed set A has at least one zero-sum subset S, there is at least one of these sets A which has no zero-sum subset S satisfying $0 < |S| \leq 3$. For q = 6 there are 18 of these sets A whose zero-sum subsets S have smallest cardinality greater than three:

TABLE 3. Zero-Sum Subsets S
for $q = 6$

d	A	S
2	$A_1 = \{1, -3, -4, 5, 6, \}$	$S_1 = \{1, -3, -4, 6\}$
	$A_2 = \{1, -3, -4, -5, 6\}$	$S_2 = \{1, -3, -4, 6\}$
	$A_3 = \{1, -3, 4, 5, 6\}$	$S_3 = A_3$
3	$A_4 = \{1, 2, 4, 5, 6\}$	$S_4 = \{2, 5, 6\}$
	$A_5 = \{1, -2, 4, 5, 6\}$	$S_5 = \{-2, 4, 5, 6\}$
	$A_6 = \{1, 2, -4, -5, 6\}$	$S_6 = A_6$
	$A_7 = \{1, 2, -4, -5, -6\}$	$S_7 = \{2, -4, -5, -6\}$
	$A_8 = \{1, -2, -4, -5, 6\}$	$S_8 = \{-2, -4, 6\}$
	$A_9 = \{1, -2, -4, -5, -6\}$	$S_9 = \{-2, -5, -6\}$
q−2	$A_{10} = \{1, 2, 3, 5, 6\}$	$S_{10} = \{2, 5, 6\}$
	$A_{11} = \{1, 2, 3, -5, 6\}$	$S_{11} = \{2, 3, -5\}$
	$A_{12} = \{1, 2, 3, -5, -6\}$	$S_{12} = \{2, 3, -5\}$
	$A_{13} = \{1, -2, 3, 5, 6\}$	$S_{13} = A_{13}$
	$A_{14} = \{1, -2, 3, -5, 6\}$	$S_{14} = \{1, -2, -5, 6\}$
	$A_{15} = \{1, -2, 3, -5, -6\}$	$S_{15} = \{-2, -5, -6\}$
	$A_{16} = \{1, -2, -3, 5, 6\}$	$S_{16} = \{-2, -3, 5\}$
	$A_{17} = \{1, -2, -3, -5, 6\}$	$S_{17} = \{1, -2, -5, 6\}$
	$A_{18} = \{1, -2, -3, -5, -6\}$	$S_{18} = \{-2, -5, -6\}$

(Table 3 is continued on the next page.)

TABLE 3 (continued).

d	A	S
q−1	$A_{19}=\{1,2,3,4,6\}$	$S_{19}=\{3,4,6\}$
	$A_{20}=\{1,2,3,4,-6\}$	$S_{20}=\{2,4,-6\}$
	$A_{21}=\{1,-2,3,4,6\}$	$S_{21}=\{3,4,6\}$
	$A_{22}=\{1,-2,3,4,-6\}$	$S_{22}=A_{22}$
	$A_{23}=\{1,-2,-3,4,6\}$	$S_{23}=\{1,-2,-3,4\}$
	$A_{24}=\{1,-2,-3,4,-6\}$	$S_{24}=\{1,-2,-3,4\}$
	$A_{25}=\{1,-2,-3,-4,6\}$	$S_{25}=\{-2,-4,6\}$
	$A_{26}=\{1,-2,-3,-4,-6\}$	$S_{26}=\{-3,-4,-6\}$
q	$A_{27}=\{1,2,3,4,5\}$	$S_{27}=\{1,3,4,5\}$
	$A_{28}=\{1,-2,3,4,5\}$	$S_{28}=\{1,3,4,5\}$
	$A_{29}=\{1,-2,-3,-4,-5\}$	$S_{29}=A_{29}$
1	$A_{30}=\{2,-3,4,-5,6\}$	$S_{30}=\{2,-3,-5,6\}$
	$A_{31}=\{2,-3,-4,-5,6\}$	$S_{31}=\{2,-3,-5,6\}$
	$A_{32}=\{2,3,-4,5,-6\}$	$S_{32}=A_{32}$

TABLE 4. Zero-Sum Subsets S
for $q = 7$

d	A	S
$q-2$	$A_{33} = \{1,2,3,4,6,7\}$	$S_{33} = \{2,6,7\}$
	$A_{34} = \{1,2,3,4,-6,7\}$	$S_{34} = \{2,4,-6\}$
	$A_{35} = \{1,-2,3,4,6,7\}$	$S_{35,1} = \{1,3,4,7\}$
		$S_{35,2} = \{-2,4,6,7\}$
	$A_{36} = \{1,-2,3,4,-6,7\}$	$S_{36,1} = \{1,3,4,7\}$
		$S_{36,2} = \{1,-2,-6,7\}$
	$A_{37} = \{1,-2,-3,4,6,7\}$	$S_{37,1} = \{1,-2,-3,4\}$
		$S_{37,2} = \{-2,4,6,7\}$
	$A_{38} = \{1,-2,-3,4,-6,7\}$	$S_{38,1} = \{1,-2,-6,7\}$
		$S_{38,2} = \{1,-2,-3,4\}$
	$A_{39} = \{1,-2,-3,4,-6,-7\}$	$S_{39} = \{-2,-6,-7\}$
	$A_{40} = \{1,-2,-3,-4,-6,-7\}$	$S_{40} = \{-2,-6,-7,\}$
$q-1$	$A_{41} = \{1,2,3,4,5,7\}$	$S_{41} = \{3,5,7\}$
	$A_{42} = \{1,-2,3,4,5,7\}$	$S_{42} = \{3,5,7\}$
	$A_{43} = \{1,-2,-3,4,5,7\}$	$S_{43} = \{-2,-3,5\}$
	$A_{44} = \{1,-2,-3,-4,5,-7\}$	$S_{44} = \{-2,-3,5\}$
	$A_{45} = \{1,-2,-3,-4,-5,-7\}$	$S_{45} = \{-3,-5,-7\}$

cardinality five for six sets A, in which case S = A, and cardinality four for 12 sets A. For q = 7 there are four of these sets A whose zero-sum subsets S have smallest cardinality greater than three: cardinality four for all four sets A. These observations complete the proofs of Theorem 13 and Theorem 14.

We now explain the precise origin of each set listed in Table 3 and Table 4.

First suppose q = 6 and d = 2. The sets A_1, A_2, and A_3 originate in that part of the proof of Case 2 where we suppose that $-3 \in A$ and $q \in A$. Then j = 3, j = 4, or j = 5. When j = 4 or j = 5, the set $S = \{-3,-4,7\}$ is not a subset of A. When j = 3, then $\{4,q-2,q-1\}$ is not a set because q−2 = 4. The sets A_1, A_2, and A_3 correspond to j = 4, j = 5, and j = 3, respectively.

Now suppose that q = 6 and d = 3. The sets A_4 and A_5 originate in that part of the proof of Case 3 where we suppose $4 \in A$. Because q−2 = 4, then $\{4,q-2,q-1\}$ is not a set. The sets A_6, A_7, A_8, and A_9 originate in that part of the proof of Case 3 where we suppose $-(q-1) \in A$. Since −(q−2) = −4, then $\{-4,-(q-2),-(q-1)\}$ is not a set.

Next suppose that q = 6 and d = q−2 = 4 or d = q−1 = 5. This is the only instance where the proof of Theorem 11 breaks down in some way other than that the

sets S are not sets or are not subsets of A. Actually, the steps in this part of the proof of Theorem 11 are all either vacuous or invalid when q = 6, and so we abandon the proof entirely in favor of an enumeration of the sets for this case. Hence, we list the sets A_{10}, A_{11}, A_{12}, A_{13}, A_{14}, A_{15}, A_{16}, A_{17}, A_{18}, A_{19}, A_{20}, A_{21}, A_{22}, A_{23}, A_{24}, A_{25}, and A_{26}.

Next suppose that q = 6 and d = q = 6. The sets A_{27} and A_{28} originate in that part of the proof of Case 5 where we suppose that $3 \in A$. Since $q-2 = 4$, then $\{4, q-2, q-1\}$ is not a set. The set A_{29} comes from that part of the proof of Case 5 where we suppose $-(q-1) \in A$. Because $-(q-2) = -4$, then $\{-4, -(q-2), -(q-1)\}$ is not a set.

Now suppose that q = 6 and d = 1. The sets A_{30} and A_{31} originate in that part of the proof of Case 6 where we suppose that $-(q-1) \in A$ and $q \in A$. Then $-3 \in A$, and since $-(q-3) = -3$, then $\{-3, -(q-3), q\}$ is not a set. The set A_{32} comes from that part of the proof of Case 6 where we assume that $(q-1) \in A$, $-q \in A$, and $3 \in A$. Since $q-3 = 3$, then $\{3, q-3, -q\}$ is not a set.

Next suppose that q = 7 and d = q−2 = 5. The sets A_{33}, A_{34}, A_{35}, A_{36}, A_{37}, and A_{38} originate in that part of the proof of Case 4 where we assume that $4 \in A$ and $q \in A$.

Since $q-3 = 4$, then $\{4,q-3,q\}$ is not a set. The set A_{39} originates in that part of the proof of Case 4 where we assume that $4 \in A$ and also that $-3 \in A$ and $-q \in A$. The set $S = \{-2,-3,5\}$ is not a subset of A since $d = 5$. The set A_{40} comes from that part of the proof of Case 4 where we suppose that $-(q-3) \in A$ and $-q \in A$. Since $-(q-3) = -4$, then $\{-4,-(q-3),-q\}$ is not a set.

Finally, suppose that $q = 7$ and $d = q-1 = 6$. The sets A_{41}, A_{42}, and A_{43} originate in the same part of the proof of Case 4 as do the sets A_{33}, A_{34}, A_{35}, A_{36}, A_{37}, and A_{38} and for the same reason. Similarly, the sets A_{44} and A_{45} originate in the same part of the proof of Case 4 as does the set A_{40} and for the same reason.

Once the sets A remaining after step 5 of the screening process are determined, they must be analyzed individually for zero-sum subsets S. For each set A we are interested only in those zero-sum subsets having minimal cardinality and we list them all. Following is a systematic procedure for locating these subsets:

1. If $q = 6$, sum the residue classes of A. If this sum is zero, then by steps 1 and 2 of the earlier screening $S = A$. If the residue classes of A sum to a non-zero residue class r, search for subsets of A

of cardinality 2 or 1 which sum to r since the complements of these subsets are all of the zero-sum subsets of A with 3 or 4 elements, respectively.

2. If q = 7, sum the residue classes of A. If this sum is zero, then again by the earlier screening S = A or S is a subset of A with 3 elements. Such a subset of 3 elements must be found by enumerating all subsets of A with 3 elements. If the residue classes of A sum to a nonzero residue class r, then search for subsets of cardinality 3, 2, or 1 which sum to r since the complements of these subsets are all of the zero-sum subsets of A with 3, 4, or 5 elements, respectively.

This concludes our explanation of Table 3 and Table 4. The following two theorems follow immediately from these tables.

THEOREM 13. Any set A of five residue classes mod 13 has a nonempty subset S of at most five residue classes that sum to zero mod 13, with five residue

classes necessary for some sets A.

THEOREM 14. Any set A of six residue classes mod 15 has a nonempty subset S of at most four residue classes that sum to zero mod 15, with four residue classes necessary for some sets A.

CHAPTER 6

FURTHER PROBLEMS

We have already listed several general problems in the introduction. In this chapter we list specific unsolved problems arising out of our work in this thesis.

In Section 6.1 we introduce some interesting unsolved problems arising from our attempts to decrease the lower bound restriction on $|A|$ in Alon's theorem. These attempts led to our results in Chapter 3. In Section 6.2 we introduce some interesting unsolved problems arising from our research with respect to odd moduli developed in Chapter 4 and Chapter 5. All of the variables used in this chapter are integers unless stated otherwise. Of course ϵ is always real.

6.1 Problems Related to Our Results in Chapter 3

(i) Immediately before the statements and proofs of Theorem 4 and Theorem 5 we mention that these theorems suggest that similar theorems can be constructed for each $k > 5$. A more interesting problem is to construct a single theorem for $k \geq 3$, which includes Theorem 3, Theorem 4 and Theorem 5 as special cases.

(ii) Prove or disprove Conjecture 6.

(iii) If Conjecture 6 cannot be proved, determine if there exists a real number $c(k) > 0$ for each $k \geq 3$ such that Alon's conclusion holds if we only require $|A| > \frac{n}{k} + c(k)$, where $A \subseteq Z_n$ and $n > n_0(k, c(k))$.

(iv) If Conjecture 6 cannot be proved and problem (iii) cannot be solved, find an increasing function $f(n,k)$ satisfying $0 < f(n,k) < \left(1 + \sqrt{3(k-2)}\right) r_3(n)$ such that Alon's conclusion can be shown to hold if we only require $|A| > \frac{n}{k} + f(n,k)$, where $k \geq 3$, $A \subseteq Z_n$, and $n > n_0(k)$.

(v) If a function $f(n,k)$ described in problem (iv) is found, determine if it is the minimum such function for which Alon's conclusion can be shown to hold.

(vi) If Conjecture 6 cannot be proved and problem (iii) cannot be solved, find an increasing function $g(n,k) > 0$ for which it can be shown that Alon's conclusion sometimes fails to hold if we only require $|A| > \frac{n}{k} + g(n,k)$, where $k \geq 3$, $A \subseteq Z_n$, and n is arbitrarily large.

(vii) If a function $g(n,k)$ described in problem (vi) is found, determine if it is the maximum such function for which it can be shown that Alon's conclusion sometimes fails to hold for arbitrarily large moduli n.

(viii) If Conjecture 6 can be proved, consider the term $c_0(k)$ in the statement of the conjecture. Determine if Alon's conclusion holds for each $k \geq 3$ if $|A| > \frac{n}{k} + c_0(k)$, where $A \subseteq Z_n$ and $n > n_0(k, c_0(k))$.

(ix) Extend Alon's theorem to finite noncyclic abelian groups and to finite nonabelian groups.

6.2 Problems Related to Our Results in Chapter 4 and Chapter 5

(x) Extend Stalley's and the author's results to sets A of (q−h) residue classes mod(2q) or mod(2q+1), where $q > h \geq 2$. Alon's theorem assures us (and also Filaseta and Richman's result[4] but for a different reason) that there is a solution to this problem for each $h \geq 2$ since $\lim_{q \to \infty} \frac{|A|}{n} = \frac{1}{2} > (\frac{1}{3} + \epsilon)$, for $\epsilon > 0$ sufficiently small. However, such solutions will probably require techniques different from those used for $h = 0$ and $h = 1$. Even with $h = 2$ these techniques become extremely cumbersome and possibly inadequate.

(xi) Let $A \subseteq Z_n$ and $|A| = q-h$ where $n = 3q+r$, $0 \leq r < 3$, and $q > h \geq 0$. Further, let $q_0(h) = q_0(r,h)$. Determine the smallest integer $q_0(h)$ so that for all $q \geq q_0(h)$ any such A will contain a zero-sum subset S of at most four residue classes modn. Alon's theorem

assures us that there is a solution to this problem for each $h \geq 0$ since $\lim_{q\to\infty} \frac{|A|}{n} = \frac{1}{3} > (\frac{1}{4}+\epsilon)$, where $\epsilon > 0$ is sufficiently small.

(xii) More generally, let $A \subseteq Z_n$ and $|A| = q-h$ where $n = kq+r$, $k \geq 3$, $0 \leq r < k$, and $q > h \geq 0$. In addition, let $q_0(h) = q_0(k,r,h)$. Determine the smallest integer $q_0(h)$ so that for all $q \geq q_0(h)$ any such A will contain a zero-sum subset S of at most (k+1) residue classes modn. Once again, Alon's theorem assures us that solutions exist to this problem since $\lim_{q\to\infty} \frac{|A|}{n} = \frac{1}{k} > (\frac{1}{k+1}+\epsilon)$, for $\epsilon > 0$ sufficiently small.

A reasonable assumption to make is that $q_0(h) > k$ because of the sets $A = \{i \mid 1 \leq i \leq q-h\}$. For suppose that $q \leq k$. The subsets S of such a set A whose elements form the smallest possible sum and largest possible sum are $S = \{1\}$ and $S = \{1,\ldots,q-h\}$, respectively. Since

$$1 + 2 + \ldots + (q-h) \quad < \quad (q-h)^2 \quad \leq \quad kq+r \quad = \quad n \ ,$$

it follows that no such set A, when $q \leq k$, has a zero-sum subset S.

(xiii) Extend problem (xi) and, more generally, problem (xii) to smaller values of q. Specifically, for each $q < q_0(h)$ determine whether every set A of (q-h)

residue classes mod(kq+r), where $k \geq 3$, $0 \leq r < k$, and $q > h \geq 0$, contains at least one zero-sum subset S and, if so, the smallest integer $t_0(q) = t_0(q,k,r,h)$ so that every set A contains at least one zero-sum subset S such that $0 < |S| \leq t_0(q) \leq q-h$.

(xiv) Extend Stalley's and the author's results to finite noncyclic abelian groups and to finite nonabelian groups.

This completes our list.

BIBLIOGRAPHY

1. N. Alon. Private communication from M. Filaseta.

2. _____ *Subset sums*. Journal of Number Theory 27:196-205. 1987.

3. P. Erdös and H. Heilbronn. *On the addition of residue classes mod p*. Acta Arithmetica 9:149-159. 1964.

4. M. Filaseta and D. Richman. *A conjecture of Stalley*. Private communication.

5. Richard K. Guy. *Unsolved Problems in Number Theory*, Springer-Verlag, New York, 1981, p. 73-74.

6. John E. Olson. *An addition theorem modulo p*. Journal of Combinatorial Theory 5:45-52. 1968.

7. Charles Ryavec. *The addition of residue classes modulo n*. Pacific Journal of Mathematics 26:367-373. 1968.

8. Robert D. Stalley. *Some bounds related to Szemerédi's theorem*. Unpublished notes.

9. E. Szemerédi. *On a conjecture of Erdös and Heilbronn*. Acta Arithmetica 17:227-229. 1970

APPENDIX

APPENDIX 1

STATEMENTS OF THEOREMS

In this appendix we provide the reader with authors' verbatim statements of the theorems and conjectures, listed in chronological order, that are mentioned in the historical background section of Chapter 2. In some cases we use different letters to be consistent with the symbols used in this thesis. Also, minimal explanatory material provided by each author precedes these statements when necessary. We mark the end of each statement with the symbol □.

In the following theorem let p be a prime, $a_1,\dots,a_m$ distinct non-zero residue classes modp, r a residue class modp. Let

$$F(r) = F(r\,;p\,;a_1,\dots,a_m)$$

denote the number of solutions of the congruence

$$e_1a_1 + \cdots + e_ma_m \equiv r(\mathrm{mod}\,p),$$

where the $e_1,\dots,e_m$ are restricted to the values 0 and 1.

Note of clarification: Here $e_1,\ldots,e_m$ are not all zero.

THEOREM A.1 (P. Erdös and H. Heilbronn, 1964[3]).

$F(r) > 0$ if $m \geq (3\sqrt{6})\sqrt{p}$. □

CONJECTURE A.2 (Erdös and Heilbronn, 1964[3]).

It is possible to replace the constant $3\sqrt{6}$ in Theorem A.1 by the constant 2. □

CONJECTURE A.3 (Erdös and Heilbronn, 1964[3]).

$F(0) > 0$ for $m > 2\sqrt{p}$, where p is not necessarily a prime.

This conjecture may also be true for finite abelian groups of composite order p, and possibly even, *mutatis mutandis*, for nonabelian groups. □

In the following theorem let $a_1,\ldots,a_m$ be distinct non-zero residue classes modulo the prime p and let r be the number of residue classes x of the form

$$x = e_1a_1 + \cdots + e_ma_m,$$

where the e_i are restricted to the values 0 and 1 and are

not all 0.

THEOREM A.4 (John E. Olson, 1968[6]).

If $m > \sqrt{(4p-3)}$, then $r = p$. □

THEOREM A.5 (Charles Ryavec, 1968[7]).

Let $a_1,\ldots,a_m$ be m distinct, nonzero residues modulo n, where n is any natural number and where

$$m \geq 3\sqrt{6n}\exp\left\{c\frac{\sqrt{\log n}}{\log\log n}\right\},$$

where $c > 0$ is some large constant. Then the congruence

$$e_1a_1 + \cdots + e_ma_m \equiv 0(\mathrm{mod}\, n)$$

is solvable with $e_i = 0$ or 1 and not all $e_i = 0$. □

In the following theorem let G be an abelian group of n elements. Let H denote the set of elements of G and let A denote a subset of H. Put

$$A^* = \left\{\sum e_ia_i : a_i \in A,\ e_i = 0 \text{ or } 1 \text{ but not all } e_i \text{ are } 0\right\}.$$

THEOREM A.6 (E. Szemerédi, 1970[9]).

There exist a real number $K > 0$ and an integer n_0 such that for every $n > n_0$, for every G, and for every $A \subset H$, $|A| \geq K\sqrt{n}$,

$$0 \in A^*. \quad \square$$

THEOREM A.7 (Robert D. Stalley[8]).

Any set A of q distinct residues mod2q, where $q \geq 5$, has a nonempty subset S of at most three residues whose sum is zero mod2q, with three residues necessary for some sets A. $\square$

COROLLARY A.8 (Stalley[8]).

Any set A of q distinct residues mod2q, where $q = 4$, has a nonempty subset S of at most four residues whose sum is zero mod2q, with four residues necessary for some sets A. $\square$

THEOREM A.9 (Stalley[8]).

Any set A of $(q-1)$ distinct residues mod2q, where $q \geq 8$, has a nonempty subset S of at most three residues whose sum is zero mod2q, with three residues necessary

for some sets A. □

COROLLARY A.10 (Stalley[8]).

Any set A of (q−1) distinct residues mod2q, where q = 7, has a nonempty subset S of at most four residues whose sum is zero mod2q, with four residues necessary for some sets A, and where q = 6, has a nonempty subset S of at most five residues whose sum is zero mod2q, with five residues necessary for some sets A. □

THEOREM A.11 (M. Filaseta and D. Richman [4]).

For every positive integer h, if $n > n_0(h)$ and $A \subseteq Z_n$ satisfies $|A| > \frac{n}{2} - h$, then there exists a subset $S \subseteq A$ such that $0 < |S| \leq 3$ and $\sum_{s \in S} s = 0$. □

In the following theorem let G be a (finite) abelian group and let $A \subseteq G$. Define

$$A^{(k)} = \{a_1 + \cdots + a_k : a_1, \ldots, a_k \text{ are distinct elements of } A\}.$$

Define r_2 to be the number of elements $g \in G$ such that $g+g = 0$.

THEOREM A.12 (N. Alon[1]).

If $0 \notin A^{(2)}$ and if $A^{(3)} \cup A^{(2)} \neq G$, then

$$|G| + 2r_2 + 3 \geq 2|A| + \frac{(|A| - r_2)|A|}{2|A| - r_2}. \quad \square$$

THEOREM A.13 (Alon's Theorem, 1987[2]).

For every fixed $\epsilon > 0$ and $k > 1$, if $n > n_0(k,\epsilon)$ and $A \subseteq Z_n$ satisfies $|A| > (\frac{1}{k} + \epsilon)n$, then there is a subset $S \subseteq A$ such that $0 < |S| \leq k$ and $\sum_{s \in S} s = 0$. $\square$

In the following proposition let $r_3(n)$ denote the maximum cardinality of a subset $B \subseteq \{1, 2, \ldots, n\}$ that contains no arithmetic progression of three terms.

PROPOSITION A.14 (Alon's Proposition, 1987[2]).

Let A be a subset of Z_n of cardinality $|A| \geq \frac{n}{k} + \left(1 + \sqrt{3(k-2)}\right) r_3(n)$. Then there is a subset $S \subseteq A$ of cardinality $1 \leq |S| \leq k$ such that $\sum_{s \in S} s = 0$ (in Z_n). $\square$