STRUCTURE OF MINIMAL ZERO-SUM SEQUENCES OF MAXIMAL LENGTH IN $\mathbf{Z}_n \oplus \mathbf{Z}_n$

A Thesis

Presented to the

Faculty of

San Diego State University

In Partial Fulfillment

of the Requirements for the Degree

Master of Arts

in

Mathematics

---

by

Donald Gene Adams, Jr

Spring 2010

SAN DIEGO STATE UNIVERSITY

The Undersigned Faculty Committee Approves the

Thesis of Donald Gene Adams, Jr:

Structure of Minimal Zero-Sum Sequences

of Maximal Length in

$\mathbb{Z}_n \oplus \mathbb{Z}_n$

Vadim Ponomarenko, Chair
Department of Mathematics and Statistics

Robert Grone
Department of Mathematics and Statistics

Carl Eckberg
Department of Computer Science

Approval Date

DEDICATION

I dedicate this to my parents who set aside their differences to give me the oppurtunity for success.

Pure mathematics is, in its way, the poetry of logical ideas.

– Albert Einstein

ABSTRACT OF THE THESIS

Structure of Minimal Zero-Sum Sequences
of Maximal Length in
$\mathbb{Z}_n \oplus \mathbb{Z}_n$
by
Donald Gene Adams, Jr
Master of Arts in Mathematics
San Diego State University, 2010

Zero-sum problems over finite abelian groups have been studied extensively over the last decade for their application to factorization theory. As stated in [11], in order to understand the factorization properties of an algebraic number field, one must completely understand the structure of all minimal zero-sum sequences of maximal length. The maximal length for a minimal zero-sum sequence in a group, G, is defined by the Davenport constant, which is known only for specific types of groups such as cyclic groups, groups of rank 2, and all p-groups[2]. The minimal zero-sum sequences of maximal length over $G = \mathbb{Z}_n$ have been completely determined [3]. Much progress has been made in the case when $G = \mathbb{Z}_n \oplus \mathbb{Z}_n$, however there is one small gap to be filled. The goal of this paper is to to fill the gap slightly by showing which multiplicities occur in minimal zero-sum sequences over $G = \mathbb{Z}_p \oplus \mathbb{Z}_p$ for p an odd prime. In the search for a proof of the main result, we come across an extension of a well know result from [16] and [5].

TABLE OF CONTENTS

PAGE

ACKNOWLEDGEMENTS

I would like to thank all of my professors at San Diego State for their guidance and support, especially Vadim Ponomarenko. This project was his idea and was lead by his close guidance. He constantly challenged me and motivated me to prove theorems, and, once they were proved, he pushed me to extend them. Mathematical progress was made until the final day of this project solely do to the fact that Dr. Ponomarenko continued to ask questions and push for more results. He also helped to extend a few of the results. I am very happy in my choice for my advisor, and am very thankful for all of his support and insight.

CHAPTER 1
INTRODUCTION AND APPLICATION

Let G be a finite abelian group. By the Fundamental Theorem of Finite Abelian Groups, we have

$$G = \mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2} \oplus \cdots \mathbb{Z}_{n_d},$$

where d is the rank of G and n_d is the maximum possible order of an element of G, also called the exponent of G. We call a sequence $S = g_1 g_2 \cdots g_k$, with $g_i \in G$ for $i = 1, 2, \ldots, k$ and repetitions allowed, a *zero-sum sequence* in G if

$$\sum_{i=1}^{k} g_i \equiv (0, 0, \ldots, 0) \in G.$$

Note here that the order of the elements in S does not matter. Thus if we permute the elements of S, we have not changed the sequence at all. We say that R is a subsequence of S if $R|S$, and by convention we say that the empty sequence is a zero-sum sequence. Therefore, every sequence contains the trivial zero-sum sequence. However, if a sequence S contains no proper non-trivial zero-sum subsequence then we call S a *minimal zero-sum sequence* over G.

1.1 DAVENPORT CONSTANT

The Davenport Constant of G, denoted $D(G)$, is the smallest positive integer l such that every sequence S over G of length $|S| \geq l$ contains a non-trivial zero-sum subsequence. Let us also define

$$M(G) = 1 + \sum_{i=1}^{d} (n_i - 1),$$

where n_i are the invariant factors of G. We defined $M(G)$ in this way because

$$S = (1, 0, 0, \ldots, 0)^{n_1 - 1} (0, 1, 0, \ldots, 0)^{n_2 - 1} \cdots (0, 0, 0, \ldots, 1)^{n_d - 1} (1, 1, 1, \ldots, 1)$$

is a minimal zero-sum sequence over G. Therefore, we know that $M(G) \leq D(G)$. In two consecutive papers, John Olson proved that $D(G) = M(G)$ for all finite abelian groups of rank 2 and for all finite abelian p-groups [14],[15]. For a few specific abelian groups, the Davenport Constant is known. For example, if

$$G = \mathbb{Z}_{2p^{n_1}} \oplus \mathbb{Z}_{2p^{n_2}} \oplus \mathbb{Z}_{2p^{n_3}},$$

then $D(G) = M(G)$[18]. Most other cases are still unknown although it is still conjectured that $D(G) = M(G)$ for all groups of the form $\mathbb{Z}_n^r$ for $n, r \in \mathbb{N}$ and for all groups of rank 3. There are finite abelian groups where $D(G) > M(G)$. The first such group identified was

$$G = \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_6$$

by P. C. Baayen, who also made the conjecture that $D(G) = M(G)$ for all finite abelian groups, G[18]. The following theorem from [9] shows that there are actually infinitely many abelian groups where $D(G) > M(G)$:

Theorem 1.1. *If*

$$G = \mathbb{Z}_m \oplus \mathbb{Z}_n^2 \oplus \mathbb{Z}_{2n}, \text{ where } n, m \in \mathbb{N}_{\geq 3} \text{ are odd and } m|n,$$

or

$$G = \mathbb{Z}_2^i \oplus \mathbb{Z}_{2n}^{5-i}, \text{ where } n \in \mathbb{N}_{\geq 3} \text{ is odd and } i \in [2, 4]$$

then $D(G) > M(G)$.

There is no conjecture for the general case, however, the best known upper bound for the Davenport Constant comes from [13]. The authors prove that

$$D(G) \leq n + \left\lfloor n \log\left(\frac{|G|}{n}\right)\right\rfloor,$$

where n is the exponent of G (see [2]).

Other than defining the minimal zero-sum sequence of maximal length over a finite abelian group, the Davenport Constant also played a very important role in the proof that there are infinitely many Carmichael numbers [2].

1.2 NON-UNIQUE FACTORIZATION

One of the most important applications of minimal zero-sum sequences is non-unique factorization theory. To discuss this we must define the following:

Definition 1.2.

- *H is called a* monoid *if H is a multiplicative commutative semigroup with unit element and cancellation law.*
- *An element $a \in H$ is called* invertible *if there exists $\hat{a} \in H$ such that $a\hat{a} = 1 \in H$. The set of invertible elements of H is denoted by $H^\times$.*
- *An element $a \in H$ is called an* atom*, or irreducible element, if $a = bc$ implies that either b or c is invertible. The set of atoms of H is denoted by $\mathcal{A}(H)$.*
- *Let $z = a_1 a_2 \cdots a_k$ be a factorization of $a \in H$ such that $a_i \in \mathcal{A}(H)$ for $i = 1, 2, \ldots, k$ counting multiplicity. We denote $|z|$ as the* length *of the factorization.*
- *For each $a \in H$ define $L(a) = \{|z| : z$ is a factorization of a into atoms in $H\}$. Thus $L(a)$ is the set of* factorization lengths *of a.*
- *A monoid, H, is said to be* reduced *if $H^\times = \{1\}$. For any monoid, H, $H_{red} = \{aH^\times : a \in H\}$ is the associated reduced monoid.*
- *Let G be a finite abelian group and H a subset of G. Then the* free abelian monoid over *H, denoted $\mathcal{F}(H)$, is the set of all sequences in H.*
- *Let G be a finite abelian group and H a subset of G. Then the* block monoid over *H, denoted $\mathcal{B}(H)$, is the set of zero-sum sequences over H.*

If we would like to study the factorization of $\mathcal{B}(G)$ for some abelian group G, then we would first need to identify the atoms. In $\mathcal{B}(G)$, the atoms are the zero-sum sequences that cannot be factored, or "broken up," into two zero-sum sequences. These are the minimal zero-sum sequences since for every $R \in \mathcal{F}(G)$ such that $R|S$, R is not a zero-sum sequence. Now that we have identified the atoms of $\mathcal{B}(G)$, we would like to characterize the structure of $\mathcal{A}(\mathcal{B}(G))$; this would help us to study the factorization of this monoid. In [11], the authors state that in order to investigate the factorization properties of $\mathcal{B}(G)$, it is necessary to know the structure of the minimal zero-sum sequences of maximal length, $D(G)$. For $G = \mathbb{Z}_n$, the

characterization of the minimal zero-sum sequences of maximal length is completely determined since all minimal zero sum sequences of maximal length are of the form x^n for any $x \in G \setminus \{0\}$[3]. Much progress has been made in the case where $G = \mathbb{Z}_n \oplus \mathbb{Z}_n$, and the goal of this research is to narrow the gap in completing the characterization of all minimal zero-sum sequences of maximal length, $2n - 1$.

1.3 Class Groups and Class Numbers

The desire for studying free monoids and block monoids sprouted from their applications to structures like Krull monoids. Krull domains and Krull monoids are important and have applications in areas like module theory as [7] and [6] show. A Krull monoid is defined as follows:

Definition 1.3. *Let H be a monoid. H is called a Krull monoid if there exists a free monoid, D, where H_{red} can be embedded in D such that for all $a, b \in H_{red}$ we have a divides b in H_{red} if and only if a divides b in D.*

If we compare H and H_{red}, we see that $H_{red}^{\times} = 1$. This is because if $a \in H^{\times}$, then $aH = H$. Thus, in terms of the multiplication in the monoid, we have removed all of the invertible elements in the monoid. This simplifies the factorization in the monoid because of the definition of an atom. Recall $a \in H_{red}$ is an atom if $a = bc$ implies that a or b is invertible. However, the only invertible element in H_{red} is the identity element. Thus the embedding mentioned in the above definition is thought of as embedding the non-invertible elements in a free monoid D. According to [11], every reduced Krull monoid is isomorphic to a block monoid of a suitable subset of an abelian group. The group that one should choose is defined as the *class group* and the *class number* is the order of the class group. The importance of the class group is that the arithmetic of the Krull monoid is uniquely determined by its by the class group. Class groups are also defined for algebraic number fields, where they are more widely researched. Let F be an algebraic number field and $\mathcal{O}_F$ be the ring of algebraic integers of F. Let $I(F)$ denoted the group of fractional ideals of $\mathcal{O}_F$ and $P(F)$ denote the

principle ideals of $I(F)$. Then the class group of F is $I(F)/P(F)$. The class number is the order of the class group ([1], Definition 12.1.1 and 12.1.2). The factorization properties of an algebraic number field is also determined by its class group. For example, let G be the class group of an algebraic number field F (or a Krull monoid H). Then, from [4] we have,

- $|G| = 1$ if and only if F (or H) is *factorial*, which means the factorization into atoms of every element of H is unique up to commutativity.
- $|G| = 2$ if and only if F (or H) is *half-factorial*, which means each element has a unique factorization length, or $|L(a)| = 1$ for all $a \in F$ (or H).
- $|G| \geq 3$ if and only if for every $N \in \mathbb{N}$ there exists $a \in F$ (or $a \in H$) such that $|L(a)| \geq N$.

Finding the class group of an algebraic number field is very difficult, however, there exists formulas for the class numbers for very specific number fields. For example, [12] gives class number formulas for an algebraic number field, F, if

$$F = \mathbb{Q}(\sqrt{-n}) \text{ if } n \text{ is square-free and } n \equiv 1, 2 \mod 4$$

using sums of Jacobi symbols. Let $h(-n)$ denote the class number of $\mathbb{Q}(\sqrt{-n})$, then we have the following theorem.

Theorem 1.4. *Let n be a positive, square-free integer with either $n \equiv 1 \mod 4$ or $n \equiv 2 \mod 4$, and let j be a positive integer with $\gcd(j, 2n) = 1$ and $1 \leq j \leq n$. Then if $\left(\frac{-4n}{j}\right) = 1$, we have*

$$h(-n) = \frac{1}{2} \sum_{i=0}^{\frac{j-1}{2}} \sum_{a=\lfloor \frac{4in}{j} \rfloor + 1}^{\lfloor \frac{(4i+2)n}{j} \rfloor} \left(\frac{-4n}{a}\right),$$

and if $\left(\frac{-4n}{j}\right) = -1$, then we have

$$h(-n) = \frac{1}{2} \sum_{i=1}^{\frac{j-1}{2}} \sum_{a=\lfloor \frac{(4i-2)n}{j} \rfloor + 1}^{\lfloor \frac{4in}{j} \rfloor} \left(\frac{-4n}{a}\right).$$

For example, if $n = 2$ and $j = 1$, then $\left(\frac{-8}{1}\right) = 1$. Therefore, we have the first case of the theorem and the double sum simplifies nicely and we have

$$h(-2) = \frac{1}{2}\sum_{a=1}^{4}\left(\frac{-8}{a}\right) = 1.$$

Thus, the class group for $\mathbb{Q}(\sqrt{-2})$ is the trivial group and the number field is factorial by the result from [4]. This means that the factorization in this number field is unique up to commutativity. For a slightly more interesting example, consider $n = 5$ and $j = 3$. Then $\left(\frac{-20}{3}\right) = 1$. Thus,

$$h(-5) = \frac{1}{2}\sum_{i=0}^{1}\sum_{a=\lfloor\frac{20i}{3}\rfloor+1}^{\lfloor\frac{(4i+2)5}{3}\rfloor}\left(\frac{-20}{a}\right) = 2.$$

Therefore, the class group of $\mathbb{Q}(\sqrt{-5})$ is $\mathbb{Z}_2$, and by [4], the number field is half-factorial. This means that the factorization into atoms in $\mathbb{Q}(\sqrt{-5})$ may not be unique, however each element has a unique factorization length. As a last example, let $n = 21$ and $j = 5$. Then $\left(\frac{-84}{5}\right) = 1$ and

$$h(-21) = \frac{1}{2}\sum_{i=0}^{2}\sum_{\lfloor\frac{84i}{5}\rfloor+1}^{\lfloor\frac{(4i+2)21}{5}\rfloor}\left(\frac{-404}{a}\right) = 4.$$

Hence, there are two possibilities for the class group: either $\mathbb{Z}_4$ or $\mathbb{Z}_2 \oplus \mathbb{Z}_2$. Determining the actual class group is outside the scope of this project, however, the search has been narrowed down significantly. Also, by [4], the factorization is neither factorial nor half-factorial. Thus, characterizing the minimal zero-sum sequences in these two possible class groups is imperative to determining the factorization properties in $\mathbb{Q}(\sqrt{-21})$.

CHAPTER 2
BACKGROUND AND DEFINITIONS

Much advancement has been made in the area of minimal zero-sum sequences. Of course, it only makes sense to study these sequences in the groups for which the Davenport constant is known: for groups like $\mathbb{Z}_n$ or $\mathbb{Z}_n \oplus \mathbb{Z}_m$ for $n, m \in \mathbb{N}$ to name a few focused on in this paper. Since this researched is highly related to that of Weidong Gao, Alfred Geroldinger, and David J. Grynkiewicz, we will use the following definitions from their paper:[10]

Definition 2.1. *For each $S \in \mathcal{F}(G)$,*

- *we can write $S = \prod_{g \in G} g^{v_g(S)}$, where $v_g(S) \in \mathbb{N}_0$ for all $g \in G$. We call $v_g(S)$ the* multiplicity *of g in S.*
- *$Supp(S) = \{g \in G : v_g(S) > 0\}$ is called the* support *of S.*
- *$|S| = l = \sum_{g \in G} v_g(S)$ is called the* length *of S.*

2.1 $\mathbb{Z}_n$

If we consider $G = \mathbb{Z}_n$ for $n \in \mathbb{N}$, then the minimal zero-sum sequences are almost completely characterized. From [3], we have the following result:

Theorem 2.2. *Let $k > \dfrac{n+3}{2}$, and S be a minimal zero-sum sequences over $\mathbb{Z}_n$ with length k. Then there is some $a \in \mathbb{Z}_n$ such that $v_a(S) = 2k - n$.*

In terms of the minimal zero-sum sequences of maximal length, $D(G) = n$, this theorem characterizes them completely. They are all a single element, $a \in \mathbb{Z}_n$ with multiplicity n. Another consequence of the theorem is determining number of minimal zero-sum sequences of length n in $\mathbb{Z}_n$. Since, in the maximal length case, $\gcd(a, n) = 1$, the number of minimal zero-sum sequences is given by $\phi(n)$, where ϕ is the Euler-phi function.

2.2 $\mathbb{Z}_n \oplus \mathbb{Z}_n$ AND PROPERTY B

The research for this project will be based when $G = \mathbb{Z}_n \oplus \mathbb{Z}_n$ where $n \in \mathbb{N}$. Some of the results hold when n is composite and others, in particular, the main result, hold only when n is prime. If G is of this form, we have the following definition from [8].

Definition 2.3. *Let $n \geq 2$. We say n has* Property B *if every minimal zero-sum sequence $S \in \mathcal{F}(G)$ with length $|S| = 2n - 1$ contains some element with multiplicity $n - 1$.*

It was first conjectured by Gao that every n has Property B. In a paper[8], Gao and Geroldinger proved that $2, 3, 4, 5, 6$ all have Property B and in a separate paper[17], Sury and Thangadurai proved 7 has Property B as well. In the same paper, Gao and Geroldinger proved the following theorem, which turned out to be an important step towards the proof that every n has Property B.

Theorem 2.4. *If n has Property B, then $2n$ has Property B.*

This was an important step because it eludes to the fact that Property B may be multiplicative. That is, if n and m both have Property B, then nm does as well. If it was proven that Property B was multiplicative, then it was left to prove that all primes have this property. All composites would fall as a corollary. That was exactly the progression taken. In a more recent paper[10], Gao, Geroldinger, and Grynkiewicz proved that Property B was indeed multiplicative. This left the problem to just primes, which is slightly simpler because of the existence of inverses. Before [10] could finished being reviewed for publishing, a proof for all primes was announced and filled the gap for Gao's conjecture that all $n \in \mathbb{N}_{\geq 2}$ has Property B. A citation was included in [10], although the paper which contains the proof for primes has not yet been published.

Now that it is known that $n - 1$ of the $2n - 1$ elements of a minimal zero-sum sequence of maximal length are exactly the same, we would like to study the other elements in the sequence. Can they be anything else? Obviously they can't be $(0, 0)$ because that is a minimal zero-sum sequence itself. Nor can they be the element with multiplicity $n - 1$

because that would give us n copies of one element. This would contradict the minimality of the sequence because $na \equiv 0 \mod n$ for any $a \in \mathbb{Z}_n \oplus \mathbb{Z}_n$. Another question raised is what are the multiplicities of the other elements? Is there certain multiplicities that cannot happen? These last two questions are the focus of this project.

Some progress has been made in studying the structure of the other elements of a minimal zero-sum sequence of maximal length, but none of that progress answers the question of which multiplicities can occur. For example, in [8] the authors prove the following:

Theorem 2.5. *If (e_1, e_2) is a basis of G and $a_1, \ldots, a_n \in \mathbb{Z}$ with $\sum_{j=1}^{n} a_j \equiv 1 \mod n$, then*

$$S = e_1^{n-1} \prod_{j=1}^{n} (a_j e_1 + e_2)$$

is a minimal zero-sum sequence with $|S| = D(G)$.

This theorem states a possible structure of the leftover elements, but says nothing about how many different elements will be in this sequence. The authors of [10] take this classification to the next step by giving explicit forms for the minimal zero-sum sequences.

Theorem 2.6. *Let $G = \mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2}$ with $1 < n_1 | n_2$. Then a sequence S over G of length $D(G) = n_1 + n_2 - 1$ is a minimal zero-sum sequence if and only if it has one of the following two forms:*

- $S = e_1^{ord(e_1)-1} \prod_{\nu=1}^{ord(e_2)} (x_\nu e_1 + e_2)$, *where*

(e_1, e_2) *is a basis of G with ord$(e_i) = n_i$ for $i \in \{1, 2\}$,*
$x_1, x_2, \ldots, x_{ord(e_2)} \in [0, ord(e_2) - 1]$, *and* $x_2 + x_2 + \cdots + x_{ord(e_2)} \equiv 1 \mod ord(e_1)$.

- $S = g_1^{sn_1-1} \prod_{\nu=1}^{n_2+(1-s)n_1} (-x_\nu g_1 + g_2)$, *where*

$\{g_1, g_2\}$ *is a generating set of G with ord$(g_2) = n_2$,* $x_1, x_2, \ldots, x_{n_2+(1-s)n_1} \in [0, n_1 - 1]$,
$x_1 + x_2 + \cdots + x_{n_2+(1-s)n_1} = n_1 - 1$, $s \in [1, n_2/n_1]$, *and either $s = 1$ or $n_1 g_1 = n_2 g_2$.*

In our case, $n_1 = n_2$ so the two cases are the same. Thus, we know most of the structure of the minimal zero-sum sequences of maximal length, but still no nothing about the

possible multiplicities. This theorem gives us a construction of minimal zero-sum sequences, but nothing about the exact multiplicities that occur. If we would like to construct a minimal zero-sum sequence of maximal length over $\mathbb{Z}_n \oplus \mathbb{Z}_n$ using the previous theorem, we would have to use the following method. Suppose we wanted to find $a_0, a_1, a_2, a_3 \in \mathbb{Z}_9 \oplus \mathbb{Z}_9$ such that

$$S = a_0^8 a_1^3 a_2^3 a_3^3$$

is a minimal zero-sum sequence. By Theorem 2.6, we define $e_1 = (1, 1)$, $e_2 = (0, 1)$, $x_1 = x_2 = x_3 = 1$, and $x_4 = x_5 = x_6 = 2$. Since we want

$$x_7 = x_8 = x_9 \text{ and we know } \sum_{i=1}^{9} x_i \equiv 1 \mod 9,$$

we solve the equation $9 + 3x_7 \equiv 1 \mod 9$. Thus $3x_7 \equiv 1 \mod 9$, which cannot be solved since 3 is a zero-divisor $\mod 9$. Therefore, we cannot find a minimal zero-sum sequence with the properties we want. In order to get something "close," let $x_7 = x_8 = 3$. Then we must solve the equation $15 + x_9 \equiv 1 \mod 9$. Thus $x_9 = 4$. By substituting our values into the construction of Theorem 2.6, we get

$$S = (1, 1)^8 (1, 2)^3 (2, 3)^3 (3, 4)^2 (4, 5).$$

We found a minimal zero-sum sequence of with a bigger support than we desired. Instead, if we let $x_7 + x_8 = 4$, we must solve the equation $17 + x_9 \equiv 1 \mod 9$. Therefore, $x_9 \equiv 2 \mod 9$, and we have found the minimal zero-sum sequence

$$S = (1, 1)^8 (1, 2)^3 (2, 3)^4 (3, 4)^2$$

with the same size support, but still with a slightly different multiplicities. Thus the main result has some significance.

Before stating the main result we must define multiplicity pattern. That is $(n_0, n_1, n_2, \ldots, n_k)$ is *multiplicity pattern* of a sequence $S \in \mathcal{F}(G)$ if

$$S = a_0^{n_0} a_1^{a_1} \cdots a_k^{n_k}.$$

Then the main theorem of this research is

Theorem 2.7. *Let n be an odd prime. Then $(n-1, n_1, n_2, \ldots, n_k)$ is a multiplicity pattern of an minimal zero-sum sequence of maximal length over $\mathbb{Z}_n \oplus \mathbb{Z}_n$ if and only if $n_1 + n_2 + \cdots + n_k$ is a partition of n with $2 \leq k \leq n-1$.*

which determines which multiplicity patterns occur for minimal zero-sum sequences of maximal length in $\mathbb{Z}_n \oplus \mathbb{Z}_n$, where n is a prime.

CHAPTER 3
A LINEAR DIOPHANTINE EQUATION

As we moved closer to the main result, we came across the following linear Diophantine equation:

$$n_1y_1 + n_2y_2 + \cdots + n_ky_k \equiv 1 \mod n \text{ with } n \in \mathbb{N}_{\geq 2},\ n_i, y_i \in \mathbb{Z}_n \text{ for } i = 1, 2, \ldots, k, \text{ and } 2 \leq k \leq n-1.$$

The problem faced was given $n_1, n_2, \ldots, n_k$, we needed to find $y_1, y_2, \ldots, y_k$ such that they solved the above equation and $y_i \not\equiv y_j \mod n$ for $i \neq j$. Note that we do not required the n_i's to be distinct $\mod n$. It is worth noting that Proposition 6.2.2 on page 340 of [5] guarantees the exists of a solution to

$$\sum_{i=1}^{k} n_iy_i \equiv 1 \mod n$$

as a corollary. We state that corollary here as a theorem.

Theorem 3.1. *For* $n, n_1, n_2, \ldots, n_k \in \mathbb{Z}$

$$\sum_{i=1}^{k} n_iy_i \equiv 1 \mod n$$

has a solution if and only if $\gcd(n, n_1, n_2, \ldots, n_k) = 1$.

This result has been known for many years. The earliest paper we found this result in was published in 1940 [16]. However, this result was not sufficient because we require the elements of the solution to be distinct. Therefore we have our new theorem.

Theorem 3.2. *Let* $n, n_1, n_2, \ldots, n_k \in \mathbb{Z}$ *where* n *is prime and* $1 \leq k \leq n-1$. *Then*

$$\sum_{i=1}^{k} n_iy_i \equiv 1 \mod n$$

has a solution with $y_i \not\equiv y_j \mod n$ *for* $i \neq j$ *if and only if* $\gcd(n, n_1, n_2, \ldots, n_k) = 1$.

Here we limit n to be prime only because the proof breaks down if n is a general composite number.

Proof. ($\Longrightarrow$) This is a direct consequence of Theorem 3.1.

($\Longleftarrow$) Let $\gcd(n, n_1, n_2, \ldots, n_k) = 1$. Note that at least one of the n_i's is not a multiple of n since the greatest common divisor is 1.

We will use induction on k.

Let $k = 1$. We must solve the equation

$$n_1 y_1 \equiv 1 \mod n.$$

By inspection we see that if $y_1 \equiv n_1^{-1} \mod n$ the equation is solved and the distinctness requirement is vacuously satisfied.

Suppose for $k = m - 1$ a solution to can be found with the restriction that $y_i \not\equiv y_j \mod n$ for $i \neq j$. Let $k = m$. So we have

$$\sum_{i=1}^{m} n_i y_i = n_m y_m + \sum_{i=1}^{m-1} n_i y_i.$$

By the induction hypothesis, a solution to

$$\sum_{i=1}^{m-1} n_i y_i \equiv 1 \mod n \text{ such that the } y_i\text{'s are distinct mod } n.$$

If $y_i \not\equiv 0 \mod n$ for all $i = 1, 2, \ldots, m-1$, then let $y_m = 0$ and a solution is found. If not, without the loss of generality, let $y_1 \equiv 0$. If $n_m \equiv 0 \mod n$, then we can pick y_m to be anything not equivalent to the others and a solution is found. If not, then multiply both sides of the equation above by $1 - n_m y_m$ to get

$$1 - n_m y_m \sum_{i=1}^{m-1} n_i y_i \equiv \sum_{i=1}^{m-1} n_i (1 - n_m y_m) y_i \equiv 1 - y_m n_m \mod n.$$

Thus, by adding $y_m n_m$ to both sides of the equivalence, we have a solution where, as long as $y_m \not\equiv n_m^{-1}$, the first $m - 1$ y_i's are distinct mod n. We must check now if we can define y_m such that

$$(1 - y_m n_m) y_i \not\equiv y_m \mod n \text{ for } i = 1, 2, \ldots, m-1.$$

Since we know that $y_m \not\equiv 0$ and $y_1 \equiv 0$, we need only to check the above equation for $i = 2, 3, \ldots, m-1$. Also, we may use the fact that y_i^{-1} exists for $i = 2, 3, \ldots, m$. Hence, we multiply both sides of the equation above by $y_i^{-1} y_m - 1$ to get

$$y_m^{-1} - n_m \not\equiv y_i^{-1} \mod n \text{ for } i = 2, 3, \ldots, m-1.$$

Note that there are $n-2$ choices for y_m^{-1} and $m - 2 \leq n - 3$ exclusions from the equations above. Hence, we can find y_m^{-1} such that

$$(1 - y_m n_m) y_i \not\equiv y_m \text{ for } i = 1, 2, \ldots, m-1,$$

and the solution exists.

□

In the statement of the theorem, we require $1 \leq k \leq n-1$. If $k = n$, then a solution cannot be guaranteed. In the proof of the theorem we use a counting argument where we show there is at least one extra element we can choose. In the case where $k = n$, there may or may not be that extra element. The following theorem shows when a solution with distinct elements exists.

Theorem 3.3. *Let $n_1, n_2, \ldots, n_n \in \mathbb{Z}$ where n is an odd prime and $\gcd(n, n_1, n_2, \ldots, n_n) = 1$. Then*

$$\sum_{i=1}^{n} n_i y_i \equiv 1 \mod n$$

has a solution with $y_i \not\equiv y_j \mod n$ for $i \neq j$ if and only if the n_i's are not all equivalent $\mod n$.

Proof. ($\Longrightarrow$) Let $n_1, n_2, \ldots, n_n \in \mathbb{Z}$ with $\gcd(n, n_1, n_2, \ldots, n_n) = 1$ and let

$$\sum_{i=1}^{n} n_i y_i \equiv 1 \mod n$$

have a solution with $y_i \not\equiv y_j \mod n$ for $i \neq j$. Suppose the n_i's are all equivalent $\mod n$. Without the loss of generality we may assume the n_i's are all equal and

$$\{y_1, y_2, \ldots, y_n\} = \{1, 2, \ldots, n\}.$$

Thus,

$$\sum_{i=1}^{n} n_i y_i \equiv n_1 \sum_{i=1}^{n} y_i \equiv n_1 \frac{n(n+1)}{2} \equiv 1 \mod n.$$

This implies that $\gcd(\frac{n(n+1)}{2}, n) = 1$. However, if $n \geq 3$, $\gcd(\frac{n(n+1)}{2}, n) > 1$. Therefore, a solution with distinct elements cannot exist. Hence, the n_i's are not all equivalent $\mod n$.

($\Longleftarrow$)

Let $n_1, n_2, \ldots, n_n \in \mathbb{Z}$ with $\gcd(n, n_1, n_2, \ldots, n_n) = 1$ such that not all the n_i's are equivalent $\mod n$. The proof relies on the fact that

$$1 + 2 + \cdots + n = \frac{n(n+1)}{2} \equiv 0 \mod n \text{ since } n \text{ is an odd prime,}$$

and the observation that

$$n_1 + 2n_2 + \cdots + nn_n \equiv 1 \mod n$$

if and only if

$$n_1 + 2n_2 + \cdots + nn_n - (1 + 2 + \cdots + n)$$
$$\equiv (n_1 - 1) + 2(n_2 - 1) + \cdots + n(n_n - 1) \equiv 1 \mod n.$$

Thus, we can subtract from the n_i's until at least one of them is zero $\mod n$. Note, not all of them will be zero since they are not all equivalent. Without the loss of generality, suppose

$$n_{k+1} \equiv n_{k+2} \equiv \cdots \equiv n_n \equiv 0 \mod n.$$

Then we have $n_1, n_2, \ldots, n_k$ with $\gcd(n, n_1, n_2, \ldots, n_k) = 1$ and $1 \leq k \leq n-1$. By Theorem 3.2 there exists $\{y_1, y_2, \ldots, y_k\} \subsetneq \{1, 2, \ldots, n\}$ such that

$$\sum_{i=1}^{k} n_i y_i \equiv 1 \mod n.$$

Then we can choose $\{y_{k+1}, y_{k+2}, \ldots, y_n\} = \{1, 2, \ldots, n\} \setminus \{y_1, y_2, \ldots, y_k\}$, and we have found a solution with distinct elements. □

If $k \geq n+1$, then there is no way to find a solution with distinct elements modulo n to

$$\sum_{i=1}^{k} n_i y_i \equiv 1 \mod n$$

by the pigeon-hole principle. Not only was this a major step in the proof of the main theorem of this project, but it is a significant advancement of an old result.

CHAPTER 4
MAIN RESULT

Before we move into the main result, there are a couple of observations and facts that need to be stated. First, if

$$S = a_0^{n_0} a_1^{n_1} \cdots a_k^{n_k}$$

is a minimal zero-sum sequence over any finite abelian group, G, and θ is an automorphism of G, then

$$\theta(S) = \theta(a_0)^{n_0} \theta(a_1)^{n_1} \cdots \theta(a_k)^{n_k}$$

is also a minimal zero-sum sequence over G [9, 10, 8, 3]. Note that this does not change the multiplicity pattern of the sequence, but only the elements in the sequence. Thus, for our application, we can choose the appropriate automorphism of $\mathbb{Z}_n \oplus \mathbb{Z}_n$ such that

$$\theta(S) = (0,1)^{n-1} a_1^{n_1} \cdots a_k^{n_k}.$$

Then, once we do our calculations with the given multiplicity pattern, we can apply θ^{-1} to get back to the original sequence. Or if we find a minimal zero-sum sequence where $(0,1)$ is the element with multiplicity $n-1$, we can apply any automorphism to find a minimal zero-sum sequence with any other non-zero element of $\mathbb{Z}_n \oplus \mathbb{Z}_n$ as the element of high multiplicity. Secondly, since we are limiting our research to minimal zero-sum sequences of maximal length over $G = \mathbb{Z}_n \oplus \mathbb{Z}_n$, when we consider the multiplicity pattern $(n-1, n_1, n_2, \ldots, n_k)$ we see that

$$\sum_{i=1}^{k} n_i = n, \text{ since}$$
$$n - 1 + \sum_{i=1}^{k} n_i = 2n - 1.$$

Therefore, we can make our first worthwhile observation and say that the multiplicity pattern of the leftover elements must be a partition of the integer n. This leads us to the first lemma in proving the main result.

Lemma 4.1. *Let $n \in \mathbb{Z}$ with $n \geq 3$ and let $S = (0,1)^{n-1} a_1^{v_{a_1}(S)} \cdots a_k^{v_{a_k}(S)}$ be a minimal zero-sum sequence of maximal length in $\mathbb{Z}_n \oplus \mathbb{Z}_n$ where $a_i = (x_i, y_i)$ for $i = 1, 2, \ldots, k$. Then $x_1 = x_2 = \cdots = x_k$.*

Proof. First note that

$$\sum_{i=1}^{k} v_{a_i}(S) x_i \equiv 0 \mod n$$

in order for S to be a zero-sum sequence. Thus

$$T = x_1^{v_{a_1}(S)} x_2^{v_{a_1}(S)} \cdots x_k^{v_{a_k}(S)}$$

is a zero-sum sequence in $\mathbb{Z}_n$. Note that since $v_{a_1}(S) + v_{a_2}(S) + \cdots + v_{a_k}(S)$ is a partition of n, then $|T| = n$.

Suppose that T is not an minimal zero-sum sequence in $\mathbb{Z}_n$. That is to say,

$$\sum_{i \in I} v_{a_i}(S) x_i \equiv 0 \mod n \text{ for some } I \subsetneq \{1, 2, 3, \ldots, k\}$$

$$\text{Then, let } \sum_{i \in I} v_{a_i}(S) a_i \equiv (0, m) \mod n.$$

If $m \equiv 0 \mod n$, then we have found a subsequence of S that sums to zero which contradicts the fact that S is minimal. Thus, $m \not\equiv 0 \mod n$, however, by utilizing the $n-1$ copies of $(0,1)$, we have

$$\sum_{i=1}^{n-m} (0,1) + \sum_{i \in I} v_{a_i}(S) a_i \equiv (0, n-m) + (0, m) \equiv (0,0) \mod n,$$

which is a contradiction since S is minimal. Therefore, T is an minimal zero-sum sequence in $\mathbb{Z}_n$ of length n, which is maximal length. By [3], there is an element that repeats n times. In other words, $x_1 = x_2 = \cdots = x_k$.

□

This is a technical result that tells us more about the structure of minimal zero-sum sequences of this type. Since we now know that the first coordinates of the leftover elements are all equal, then our problem will simplify from two dimensions to just one dimension. One may also notice that Theorem 2.6 would give this result as well, by letting $e_1 = (0, 1)$ and e_1 be any other element in $\mathbb{Z}_n \oplus \mathbb{Z}_n$ such that (e_1, e_2) is a basis. However, the above proof is very different than that of Theorem 2.6, and the two were proved concurrently.

As a reminder, the goal is to determine which multiplicity patterns can or cannot occur. The following lemma tells us more about structure of minimal zero-sum sequences, but more importantly, tells us two multiplicity patterns that cannot occur: $(n-1, n)$ and $(n-1, 1, 1, 1, \ldots, 1)$. The lemma does so by giving bounds on the support of a minimal zero-sum sequence. The support was defined in Definition 2.1 as

$$Supp(S) = \{g \in G : v_g(S) > 0\}.$$

Lemma 4.2. *Let S be an minimal zero-sum sequence in $G = \mathbb{Z}_n \oplus \mathbb{Z}_n$ of maximal length with $n \geq 3$. Then $3 \leq |Supp(S)| \leq n$.*

Proof. Suppose $Supp(S) = \{a_0, a_1, \ldots, a_k\}$ where $v_{a_0}(S) = n - 1$. First we must note that $2 \leq |Supp(S)| \leq n + 1$. This is true because $|S| = 2n - 1$ and n has Property B. Thus, it suffices to show a contradiction when $|Supp(S)| = 2$ and $|Supp(S)| = n + 1$. First assume, $|Supp(S)| = 2$. Since n has Property B, there is an element with multiplicity $n - 1$. Since there are only 2 distinct elements in S, the other element must have multiplicity n. This is a contradiction since a^n is a zero-sum sequence for every $a \in \mathbb{Z}_n \oplus \mathbb{Z}_n$ and S was supposed to be minimal.

Then assume $|Supp(S)| = n + 1$. Then, without the loss of generality,
$S = (0, 1)^{n-1} a_1^{v_{a_1}(S)} \cdots a_n^{v_{a_n}(S)}$. Let $a_i = (x_i, y_i)$, for each $i = 0, 1, \ldots, n$. Then

$$\sum_{i=0}^{n} v_{a_i}(S) x_i \equiv \sum_{i=1}^{n} v_{a_i}(S) x_i \equiv 0 \mod n$$

Also, since $v_{a_0}(S) = n - 1$, we have

$$\sum_{i=1}^{n} v_{a_i}(S) = n.$$

It follows that $v_{a_1}(S) = v_{a_2}(S) = \cdots = v_{a_n}(S) = 1$. Also, by Lemma 4.1, $x_1 = x_2 = \cdots = x_n$. Without loss of generality,

$$\{y_1, y_2, \ldots, y_n\} = \{0, 1, \ldots, n-1\}.$$

since if $y_i = y_l$ for $i \neq l$ then $(x_i, y_i) = (x_l, y_l)$ which contradicts the fact that both elements are in $Supp(S)$.

Now, in order for the elements of S to sum to $(0, 0)$, we need

$$\sum_{i=1}^{n} y_i \equiv 1 \mod n.$$

If this were not true, then the second coordinates would not sum to 0. It follows that

$$\sum_{i=1}^{n} y_i = \sum_{i=1}^{n-1} i = \frac{(n-1)n}{2} \equiv 1 \mod n.$$

Case 1: n is odd. Then $\frac{n-1}{2} \in \mathbb{N}$ and

$$\frac{(n-1)n}{2} \equiv 0 \not\equiv 1 \mod n.$$

This contradicts the fact that S is a zero-sum sequence.

Case 2: n is even. Then

$$\frac{(n-1)n}{2} = \frac{n^2}{2} - \frac{n}{2} \equiv -\frac{n}{2} \mod n.$$

Therefore, it is necessary that $-\frac{n}{2} \equiv 1 \mod n$. Or, in other words, we need

$$\frac{n}{2} + 1 = \frac{n+2}{2} = kn \text{ for } n \in \mathbb{Z}.$$

However, this implies that

$$2 \equiv 0 \mod n,$$

which only occurs if $n = 1, 2$. Thus, we have contradicted the fact that S is a zero-sum sequence. Therefore, it is impossible to have a minimal zero-sum sequence in $\mathbb{Z}_n \oplus \mathbb{Z}_n$ ($n \geq 3$) of maximal length containing $n + 1$ distinct elements and we have the result. □

This eliminates $(n-1, n)$ as a possible multiplicity pattern for an minimal zero-sum sequence of maximal length because $|Supp(S)|$ must be greater than 2. The same can be said for $(n-1, 1, 1, 1, \ldots, 1)$ because $|Supp(S)|$ must be less than n.

The next theorem clarifies the connection between linear Diophantine equations and Theorem 2.7.

Theorem 4.3. *Let $n_1 + n_2 + \cdots + n_k$ be a partition of $n \geq 3$ with $2 \leq k \leq n-1$. Then*

$$\sum_{i=1}^{k} n_i y_i \equiv 1 \mod n$$

has a solution such that $y_i \not\equiv y_j \mod n$ for $i \neq j$ if and only if there is a minimal zero-sum sequence of maximal length with multiplicity pattern $(n-1, n_1, n_2, \ldots, n_k)$.

Proof. ($\Longrightarrow$) Suppose $n_1 + n_2 + \cdots + n_k$ is a partition of n with $2 \leq k \leq n-1$ and suppose

$$\sum_{i=1}^{k} n_i y_i \equiv 1 \mod n$$

has a solution such that $y_i \not\equiv y_j \mod n$ for $i \neq j$. Let $S = a_0^{n-1} a_1^{n_1} \cdots a_k^{n_k}$. We will find a_i for $i = 0, 1, 2, \ldots, k$ such that S is a minimal zero-sum sequence of maximal length. Note that since

$$n - 1 + \sum_{i=1}^{k} n_i = n - 1 + n = 2n - 1,$$

we have the proper length. Without the loss of generality and 4.1, we assume that

$$a_0 = (0, 1) \text{ and } a_i = (x, y_i) \text{ for } i = 1, \ldots k \text{ and some } x \in \mathbb{Z}_n \setminus \{0\}.$$

All that is left is to define the y_i for $i = 1, 2, \ldots, k$. The conditions for defining the y_i's are the following:

1. $n_1 y_1 + n_2 y_2 + \cdots + n_k y_k \equiv 1 \mod n$ in order for S to be an minimal zero-sum sequence, and
2. $y_i \not\equiv y_j$ for $i \neq j$ so that we maintain the correct multiplicities.

By the hypothesis, there exists a solution with distinct elements. Therefore, there exists a sequence, S, such that S is a minimal zero-sum sequence of maximal length over $\mathbb{Z}_n \oplus \mathbb{Z}_n$ with multiplicity pattern $(n-1, n_1, n_2, \ldots, n_k)$.

($\Longleftarrow$)

Suppose $n_1 + n_2 + \cdots + n_k$ is a partition of n with $2 \leq k \leq n-1$ and suppose there is a minimal zero-sum sequence of maximal length with multiplicity pattern $(n-1, n_1, n_2, \ldots, n_k)$. Let $S = a_0^{n-1} a_1^{n_1} \cdots a_k^{n_k}$ is a minimal zero-sum sequence. By applying the proper automorphism, θ, we can transform S to

$$\theta(S) = (0,1)^{n-1}\theta(a_1)^{n_1} \cdots \theta(a_k)^{n_k} = (0,1)^{n-1}(x_1, y_1)^{n_1} \cdots (x_k, y_k)^{n_k}.$$

By Lemma 4.1, $x_1 = x_2 = \cdots = x_k$. Thus, in order to for $\theta(S)$ to be a zero-sum sequence, there must be a solution to

$$\sum_{i=1}^{k} n_i y_i \equiv 1 \mod n$$

with $y_i \not\equiv y_j \mod n$ for $i \neq j$ in order to maintain the multiplicity pattern. □

4.1 PROOF OF THEOREM 2.7

Proof. ($\Longrightarrow$) Suppose $(n-1, n_1, n_2, \ldots, n_k)$ is a multiplicity pattern of a minimal zero-sum sequence of maximal length over $\mathbb{Z}_n \oplus \mathbb{Z}_n$. That is, there exists $a_0, a_1, \ldots, a_k \in \mathbb{Z}_n \oplus \mathbb{Z}_n$ such that

$$S = a_0^{n-1} a_1^{n_1} a_2^{n_2} \cdots a_k^{n_k}$$

is a minimal zero-sum sequence of maximal length. Without the loss of generality, we may assume

$$S = (0,1)^{n-1} a_1^{n_1} a_2^{n_2} \cdots a_k^{n_k}.$$

Since

$$n - 1 + \sum_{i=1}^{k} n_i = 2n - 1, \text{ then}$$

$$\sum_{i=1}^{k} n_i = n.$$

Hence, $n_1 + n_2 + \cdots + n_k$ is a partition of n. Also, by Lemma 4.2, $3 \leq |Supp(S)| \leq n$. Since

$$Supp(S) = \{a_0, a_1, \ldots, a_k\},$$

thus $2 \leq k \leq n-1$.

($\Longleftarrow$)

Let $n_1 + n_2 + \cdots + n_k$ be a partition of n with $2 \leq k \leq n-1$. Since n is prime, $\gcd(n, n_1, n_2, \ldots, n_k) = 1$ and by Theorem 3.2, there exists a solution to

$$\sum_{i=1}^{k} n_i y_i \equiv 1 \mod n$$

such that $y_i \not\equiv y_j \mod n$ for $i \neq j$. By Theorem 4.3, there exists a minimal zero-sum sequence of maximal length over $\mathbb{Z}_n \oplus \mathbb{Z}_n$ with multiplicity pattern $(n-1, n_1, n_2, \ldots, n_k)$. □

If a result similar to that of Theorem 3.2 could be found for n composite, then all possible multiplicity patterns for minimal zero-sum sequences of maximal length over $\mathbb{Z}_n \oplus \mathbb{Z}_n$ would be determined. However, since the proof utilizes the existence of inverses, a generalized result was not found.

CHAPTER 5
FUTURE WORK

5.1 LINEAR DIOPHANTINE EQUATIONS

After coming across this application of Diophantine equations, solving them became an extreme interest. Of course, in the linear case, we know when solution exists and when they do not, however, the solution's distinctness $\mod n$ has not been investigated. Thus, we offer a conjecture for advancement, which is a generalization of Theorem 3.2 for n composite.

Conjecture 5.1. *Let $n, n_1, n_2, \ldots, n_k \in \mathbb{Z}$ where $1 \leq k \leq n-1$. Then*

$$\sum_{i=1}^{k} n_i y_i \equiv 1 \mod n$$

has a solution with $y_i \not\equiv y_j \mod n$ for $i \neq j$ if and only if $\gcd(n, n_1, n_2, \ldots, n_k) = 1$.

Again, Theorem 3.1 from [5] guarantees the existence of a solution, but says nothing about the elements of the solution being distinct.

5.2 MINIMAL ZERO-SUM SEQUENCES

Since this project does not completely characterize all minimal zero-sum sequences of maximal length of $\mathbb{Z}_n \oplus \mathbb{Z}_n$, we offer a conjecture for future work.

Conjecture 5.2. *Let $n_1 + n_2 + \cdots + n_k$ be a partition of the integer $n \geq 3$ with $2 \leq k \leq n-1$. Then $(n-1, n_1, n_2, \ldots, n_k)$ is a multiplicity pattern of a minimal zero-sum sequence in $\mathbb{Z}_n \oplus \mathbb{Z}_n$ of maximal length if and only if $\gcd(n, n_1, n_2, \ldots, n_k) = 1$.*

Although we do not have a proof for Conjecture 5.2, we have the following lemma, which is half of the proof of Conjecture 5.2.

Lemma 5.3. *Let $n_1 + n_2 + \cdots + n_k$ be a partition of the integer $n \geq 3$ with $2 \leq k \leq n-1$. If $(n-1, n_1, n_2, \ldots, n_k)$ is a multiplicity pattern of an minimal zero-sum sequence in $\mathbb{Z}_n \oplus \mathbb{Z}_n$ of maximal length, then $\gcd(n, n_1, n_2, \ldots, n_k) = 1$.*

Proof. Let $n_1 + n_2 + \cdots + n_k$ be a partition of the integer $n \geq 3$ with $2 \leq k \leq n-1$. Thus, we are attempting to find a minimal zero-sum sequence of the form

$S = a_0^{n-1} a_1^{n_1} a_2^{n_2} \cdots a_k^{n_k}$ for $a_i \in \mathbb{Z}_n \oplus \mathbb{Z}_n$ for each $i = 0, 1, \ldots, k$. Without the loss of generality and Lemma 4.1, we may assume $S = (0,1)^{n-1}(x, y_1)^{n_1}(x, y_2)^{n_2} \cdots (x, y_k)^{n_k}$.

Thus,

$$\sum_{i=1}^{k} n_i y_i \equiv 1 \mod n$$

in order for S to be a zero-sum sequence. Suppose

$$\gcd(n_1, n_2, \ldots, n_k, n) > 1.$$

By Theorem 3.1 from [5],

$$\sum_{i=1}^{k} n_i y_i \equiv 1 \mod n$$

does not have a solution at all. Therefore, if $(n-1, n_1, n_2, \ldots, n_k)$ is a multiplicity pattern of an minimal zero-sum sequence of maximal length over $\mathbb{Z}_n \oplus \mathbb{Z}_n$, then $\gcd(n, n_1, n_2, \ldots, n_k) = 1$. □

If Conjecture 5.1 was proved, then Conjecture 5.2 would fall immediately by Lemma 5.3 and Theorem 4.3. Thus all possible multiplicity patterns would be found and all minimal zero-sum sequences of maximal length over $\mathbb{Z}_n \oplus \mathbb{Z}_n$ would be completely characterized.

BIBLIOGRAPHY

[1] Şaban Alaca and Kenneth S. Williams. *Introductory algebraic number theory*. Cambridge University Press, Cambridge, 2004.

[2] Emre Alkan. Davenport constant for finite abelian groups. *Indag. Math. (N.S.)*, 19(1):1–21, 2008.

[3] J. D. Bovey, Paul Erdős, and Ivan Niven. Conditions for a zero sum modulo n. *Canad. Math. Bull.*, 18(1):27–29, 1975.

[4] L. Carlitz. A characterization of algebraic number fields with class number two. *Proc. Amer. Math. Soc.*, 11:391–392, 1960.

[5] Henri Cohen. *Number theory. Vol. I. Tools and Diophantine equations*, volume 239 of *Graduate Texts in Mathematics*. Springer, New York, 2007.

[6] Alberto Facchini. Direct sum decompositions of modules, semilocal endomorphism rings, and Krull monoids. *J. Algebra*, 256(1):280–307, 2002.

[7] Alberto Facchini. Krull monoids and their application in module theory. In *Algebras, rings and their representations*, pages 53–71. World Sci. Publ., Hackensack, NJ, 2006.

[8] Weidong Gao and Alfred Geroldinger. On zero-sum sequences in $\mathbb{Z}/n\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z}$. *Integers*, 3:A8, 45 pp. (electronic), 2003.

[9] Weidong Gao and Alfred Geroldinger. Zero-sum problems in finite abelian groups: a survey. *Expo. Math.*, 24(4):337–369, 2006.

[10] Weidong Gao, Alfred Geroldinger, and David J. Grnkiewicz. Inverse zero-sum problems iii. *Acta Arithmetica*, 141.2:103–152, 2010.

[11] Alfred Geroldinger and Franz Halter-Koch. Non-unique factorizations: a survey. In *Multiplicative ideal theory in commutative algebra*, pages 207–226. Springer, New York, 2006.

[12] Richard H. Hudson, Charles J. Judge, and Turker Teker. Class number formulae for imaginary quadratic number fields $\mathbf{Q}(\sqrt{-n})$ with n squarefree and $n \equiv 1 \pmod 4$ or $n \equiv 2 \pmod 4$. *Enseign. Math. (2)*, 45(3-4):349–355, 1999.

[13] Roy Meshulam. An uncertainty inequality and zero subsums. *Discrete Math.*, 84(2):197–200, 1990.

[14] John E. Olson. A combinatorial problem on finite Abelian groups. I. *J. Number Theory*, 1:8–10, 1969.

[15] John E. Olson. A combinatorial problem on finite Abelian groups. II. *J. Number Theory*, 1:195–199, 1969.

[16] S. S. Pillai. On a linear Diophantine equation. *Proc. Indian Acad. Sci., Sect. A.*, 12:199–201, 1940.

[17] B. Sury and R. Thangadurai. Gao's conjecture on zero-sum sequences. *Proc. Indian Acad. Sci.*, 112(3):399–414, 2002.

[18] P. van Emde Boas. A combinatorial problem on finite abelian groups. II. *Math. Centrum Amsterdam Afd. Zuivere Wisk.*, 1969(ZW-007):60, 1969.

ABSTRACT OF THE THESIS

Structure of Minimal Zero-Sum Sequences
of Maximal Length in
$\mathbb{Z}_n \oplus \mathbb{Z}_n$
by
Donald Gene Adams, Jr
Master of Arts in Mathematics
San Diego State University, 2010

Zero-sum problems over finite abelian groups have been studied extensively over the last decade for their application to factorization theory. As stated in [11], in order to understand the factorization properties of an algebraic number field, one must completely understand the structure of all minimal zero-sum sequences of maximal length. The maximal length for a minimal zero-sum sequence in a group, G, is defined by the Davenport constant, which is known only for specific types of groups such as cyclic groups, groups of rank 2, and all p-groups[2]. The minimal zero-sum sequences of maximal length over $G = \mathbb{Z}_n$ have been completely determined [3]. Much progress has been made in the case when $G = \mathbb{Z}_n \oplus \mathbb{Z}_n$, however there is one small gap to be filled. The goal of this paper is to to fill the gap slightly by showing which multiplicities occur in minimal zero-sum sequences over $G = \mathbb{Z}_p \oplus \mathbb{Z}_p$ for p an odd prime. In the search for a proof of the main result, we come across an extension of a well know result from [16] and [5].