The Perplexing Davenport Constant and Its Equally Elusive Cousin the Cross Number

Scott Chapman

Department of Mathematics and Statistics
Sam Houston State University

March 4, 2021

Background

This talk is based on the following paper.

Chapman, S. T. "On the Davenport constant, the cross number, and their application in factorization theory." in *Zero-Dimensional Commutative Rings*, *Lecture Notes in Pure and Applied Mathematics* **171**(1995): 167-167.

Introduction

$$120, 156, 232, 333, 386, \ 458, \ 568$$

Question: Can I choose a subset of these integers whose sum is divisible by 7?

Answer: Yes! In fact, there are many ways and here are just a few:

$$\begin{aligned} 333 + 458 &= 791 &= 113 \cdot 7 \\ 156 + 232 + 458 + 568 &= 1414 &= 202 \cdot 7 \\ 120 + 232 + 333 + 386 &= 1071 &= 153 \cdot 7 \end{aligned}$$

$$\mathbf{120}, \mathbf{156}, \mathbf{232}, \mathbf{333}, \mathbf{386},\ \mathbf{458},\ \mathbf{568}$$

Question: Can I choose a subset of these integers whose sum is divisible by 7?

Answer: Yes! In fact, there are many ways and here are just a few:

$$\begin{aligned} 333 + 458 &= 791 &= 113 \cdot 7 \\ 156 + 232 + 458 + 568 &= 1414 &= 202 \cdot 7 \\ 120 + 232 + 333 + 386 &= 1071 &= 153 \cdot 7 \end{aligned}$$

Introduction

$$\mathbf{120}, \mathbf{156}, \mathbf{232}, \mathbf{333}, \mathbf{386}, \ \mathbf{458}, \ \mathbf{568}$$

Question: Can I choose a subset of these integers whose sum is divisible by 7?

Answer: Yes! In fact, there are many ways and here are just a few:

$$\begin{aligned} 333 + 458 &= 791 &= 113 \cdot 7 \\ 156 + 232 + 458 + 568 &= 1414 &= 202 \cdot 7 \\ 120 + 232 + 333 + 386 &= 1071 &= 153 \cdot 7 \end{aligned}$$

120, **232**, **386**, **458**

Question: How about now?

Answer: No! Why? Reduce the list modulo 7.

120 $\equiv 1 \pmod 7$, **232** $\equiv 1 \pmod 7$, **386** $\equiv 1 \pmod 7$, **458** $\equiv 3 \pmod 7$

In fact, I really only need these numbers.

1, 1, 1, 3

Introduction

120, **232**, **386**, **458**

Question: How about now?

Answer: No! Why? Reduce the list modulo 7.

120 $\equiv 1 \pmod 7$, **232** $\equiv 1 \pmod 7$, **386** $\equiv 1 \pmod 7$, **458** $\equiv 3 \pmod 7$

In fact, I really only need these numbers.

1, 1, 1, 3

Introduction

120, 232, 386, 458

Question: How about now?

Answer: No! **Why? Reduce the list modulo 7.**

$\mathbf{120} \equiv 1 \pmod 7$, $\mathbf{232} \equiv 1 \pmod 7$, $\mathbf{386} \equiv 1 \pmod 7$, $\mathbf{458} \equiv 3 \pmod 7$

In fact, I really only need these numbers.

1, 1, 1, 3

120, **232**, **386**, **458**

Question: How about now?

Answer: No! Why? Reduce the list modulo 7.

120 $\equiv 1 \pmod 7$, **232** $\equiv 1 \pmod 7$, **386** $\equiv 1 \pmod 7$, **458** $\equiv 3 \pmod 7$

In fact, I really only need these numbers.

1, 1, 1, 3

120, **232**, **386**, **458**

Question: How about now?

Answer: No! Why? Reduce the list modulo 7.

120 $\equiv 1 \pmod 7$, **232** $\equiv 1 \pmod 7$, **386** $\equiv 1 \pmod 7$, **458** $\equiv 3 \pmod 7$

In fact, I really only need these numbers.

1, 1, 1, 3

Moral

Moral: This is really a problem in $\mathbb{Z}_7 \cong \mathbb{Z}/7\mathbb{Z}$. Hence, it is really a Group Theory problem!

How many elements must be in a sequence of elements from $\mathbb{Z}_7$ in order to guarantee it contains a subsum that sums to 0?

Observations:

1. 4 is not enough!
2. Is 7 enough?

Moral

Moral: This is really a problem in $\mathbb{Z}_7 \cong \mathbb{Z}/7\mathbb{Z}$. Hence, it is really a Group Theory problem!

How many elements must be in a sequence of elements from $\mathbb{Z}_7$ in order to guarantee it contains a subsum that sums to 0?

Observations:

1. 4 is not enough!
2. Is 7 enough?

Moral

Moral: This is really a problem in $\mathbb{Z}_7 \cong \mathbb{Z}/7\mathbb{Z}$. Hence, it is really a Group Theory problem!

How many elements must be in a sequence of elements from $\mathbb{Z}_7$ in order to guarantee it contains a subsum that sums to 0?

Observations:

1. 4 is not enough!
2. Is 7 enough?

Moral

Moral: This is really a problem in $\mathbb{Z}_7 \cong \mathbb{Z}/7\mathbb{Z}$. Hence, it is really a Group Theory problem!

How many elements must be in a sequence of elements from $\mathbb{Z}_7$ in order to guarantee it contains a subsum that sums to 0?

Observations:

1. 4 is not enough!
2. Is 7 enough?

Needed Machinery

Today's discussion will force us to view finite abelian groups in two ways.

The Fundamental Theorem of Finite Abelian Groups: Let G be a finite Abelian group.

1. There exists a unique set of positive integers $n_1, n_2, \ldots, n_k$ with $n_i \mid n_{i+1}$ for $1 \le i \le k-1$ such that

$$G \cong \mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2} \oplus \cdots \oplus \mathbb{Z}_{n_k}. \tag{1}$$

   The integers $n_1, \ldots, n_k$ are known as the invariant factors of G.

2. There exists a unique set of integers $p_1^{s_1}, p_2^{s_2}, \ldots, p_t^{s_t}$ where the p_i's are not necessarily distinct primes, and the s_i's not necessarily distinct positive integers such that

$$G \cong \mathbb{Z}_{p_1^{s_1}} \oplus \mathbb{Z}_{p_2^{s_2}} \oplus \cdots \oplus \mathbb{Z}_{p_k^{s_k}}. \tag{2}$$

   The integers $p_1^{s_1}, p_2^{s_2}, \ldots, p_t^{s_t}$ are known as the elementary divisors of G.

Needed Machinery

Today's discussion will force us to view finite abelian groups in two ways.

The Fundamental Theorem of Finite Abelian Groups: Let G be a finite Abelian group.

1. There exists a unique set of positive integers $n_1, n_2, \ldots, n_k$ with $n_i \mid n_{i+1}$ for $1 \leq i \leq k-1$ such that

$$G \cong \mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2} \oplus \cdots \oplus \mathbb{Z}_{n_k}. \qquad (1)$$

   The integers $n_1, \ldots, n_k$ are known as the invariant factors of G.

2. There exists a unique set of integers $p_1^{s_1}, p_2^{s_2}, \ldots, p_t^{s_t}$ where the p_i's are not necessarily distinct primes, and the s_i's not necessarily distinct positive integers such that

$$G \cong \mathbb{Z}_{p_1^{s_1}} \oplus \mathbb{Z}_{p_2^{s_2}} \oplus \cdots \oplus \mathbb{Z}_{p_k^{s_k}}. \qquad (2)$$

   The integers $p_1^{s_1}, p_2^{s_2}, \ldots, p_t^{s_t}$ are known as the elementary divisors of G.

Needed Machinery

Today's discussion will force us to view finite abelian groups in two ways.

The Fundamental Theorem of Finite Abelian Groups: Let G be a finite Abelian group.

1. There exists a unique set of positive integers $n_1, n_2, \ldots, n_k$ with $n_i \mid n_{i+1}$ for $1 \leq i \leq k-1$ such that

$$G \cong \mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2} \oplus \cdots \oplus \mathbb{Z}_{n_k}. \quad (1)$$

   The integers $n_1, \ldots, n_k$ are known as the invariant factors of G.

2. There exists a unique set of integers $p_1^{s_1}, p_2^{s_2}, \ldots, p_t^{s_t}$ where the p_i's are not necessarily distinct primes, and the s_i's not necessarily distinct positive integers such that

$$G \cong \mathbb{Z}_{p_1^{s_1}} \oplus \mathbb{Z}_{p_2^{s_2}} \oplus \cdots \oplus \mathbb{Z}_{p_k^{s_k}}. \quad (2)$$

   The integers $p_1^{s_1}, p_2^{s_2}, \ldots, p_t^{s_t}$ are known as the elementary divisors of G.

Needed Machinery

Definition: Given a finite abelian group G, the value of k from representation (1) is known as the **rank** of G and denoted by $\mathrm{rank}(G)$.

I will refer to G as written in form (1) as the *invariant factor form of* G.

I will refer to G as written in form (2) as the *elementary divisor form of* G.

Note: These forms seldom match. For instance they do not if G is cyclic NOT of prime power order. So if p and q are distinct primes, then

$$\mathbb{Z}_{pq} \cong \mathbb{Z}_p \oplus \mathbb{Z}_q.$$

Needed Machinery

Definition: Given a finite abelian group G, the value of k from representation (1) is known as the **rank** of G and denoted by $\mathrm{rank}(G)$.

I will refer to G as written in form (1) as the *invariant factor form of* G.

I will refer to G as written in form (2) as the *elementary divisor form of* G.

Note: These forms seldom match. For instance they do not if G is cyclic NOT of prime power order. So if p and q are distinct primes, then

$$\mathbb{Z}_{pq} \cong \mathbb{Z}_p \oplus \mathbb{Z}_q.$$

Needed Machinery

Definition: Given a finite abelian group G, the value of k from representation (1) is known as the **rank** of G and denoted by $\mathrm{rank}(G)$.

I will refer to G as written in form (1) as the *invariant factor form of* G.

I will refer to G as written in form (2) as the *elementary divisor form of* G.

Note: These forms seldom match. For instance they do not if G is cyclic NOT of prime power order. So if p and q are distinct primes, then

$$\mathbb{Z}_{pq} \cong \mathbb{Z}_p \oplus \mathbb{Z}_q.$$

Needed Machinery

Definition: Given a finite abelian group G, the value of k from representation (1) is known as the **rank** of G and denoted by $\mathrm{rank}(G)$.

I will refer to G as written in form (1) as the *invariant factor form of* G.

I will refer to G as written in form (2) as the *elementary divisor form of* G.

Note: These forms seldom match. For instance they do not if G is cyclic NOT of prime power order. So if p and q are distinct primes, then

$$\mathbb{Z}_{pq} \cong \mathbb{Z}_p \oplus \mathbb{Z}_q.$$

Finite Abelian Groups

Some of our favorite finite abelian groups.

1. $\mathrm{rank}(G) = 1 \Rightarrow G$ is cyclic.
2. $\mathrm{rank}(G) = 2$, so $G \cong \mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2}$ with $n_1 \mid n_2$. The Klein-4-group, $\mathbb{Z}_2 \oplus \mathbb{Z}_2$ is a good example.
3. Each n_i is a power of a fixed prime p. Such a group is known as a **p-group**. Hence in this case

$$G \cong \mathbb{Z}_{p^{m_1}} \oplus \mathbb{Z}_{p^{m_2}} \oplus \cdots \oplus \mathbb{Z}_{p^{m_k}}.$$

Finite Abelian Groups

Some of our favorite finite abelian groups.

1. $\mathrm{rank}(G) = 1 \Rightarrow G$ is cyclic.
2. $\mathrm{rank}(G) = 2$, so $G \cong \mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2}$ with $n_1 \mid n_2$. The Klein-4-group, $\mathbb{Z}_2 \oplus \mathbb{Z}_2$ is a good example.
3. Each n_i is a power of a fixed prime p. Such a group is known as a **p-group**. Hence in this case

$$G \cong \mathbb{Z}_{p^{m_1}} \oplus \mathbb{Z}_{p^{m_2}} \oplus \cdots \oplus \mathbb{Z}_{p^{m_k}}.$$

Finite Abelian Groups

Some of our favorite finite abelian groups.

1. $\text{rank}(G) = 1 \Rightarrow G$ is cyclic.
2. $\text{rank}(G) = 2$, so $G \cong \mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2}$ with $n_1 \mid n_2$. The Klein-4-group, $\mathbb{Z}_2 \oplus \mathbb{Z}_2$ is a good example.
3. Each n_i is a power of a fixed prime p. Such a group is known as a **p-group**. Hence in this case

$$G \cong \mathbb{Z}_{p^{m_1}} \oplus \mathbb{Z}_{p^{m_2}} \oplus \cdots \oplus \mathbb{Z}_{p^{m_k}}.$$

Minimal Zero-Sequences

Definition: Let G be a finite abelian group and $S = \{g_1, \ldots, g_t\}$ be a sequence of not necessarily distinct nonzero elements from G.

1. S is called a *zero-sequence* if $\sum_{i=1}^{t} g_i = 0$.
2. S called a *minimal zero-sequence* (or *mzs*) if it contains no proper subzero-sequence.

Comment: In general, there is no reason that G must be Abelian. If it is not, then this discussion becomes much different and will be left to another time (and another speaker!).

Notation: For S an mzs as above, we set $\mid S \mid = t$. We also let $\mathcal{B}(G)$ represent the set of zero-sequencs of G and $\mathcal{U}(G)$ represent the set of minimal zero-sequences in G. We count these irregardless of order.

Minimal Zero-Sequences

Definition: Let G be a finite abelian group and $S = \{g_1, \ldots, g_t\}$ be a sequence of not necessarily distinct nonzero elements from G.

1. S is called a *zero-sequence* if $\sum_{i=1}^{t} g_i = 0$.
2. S called a *minimal zero-sequence* (or *mzs*) if it contains no proper subzero-sequence.

Comment: In general, there is no reason that G must be Abelian. If it is not, then this discussion becomes much different and will be left to another time (and another speaker!).

Notation: For S an mzs as above, we set $|S| = t$. We also let $\mathcal{B}(G)$ represent the set of zero-sequencs of G and $\mathcal{U}(G)$ represent the set of minimal zero-sequences in G. We count these irregardless of order.

Minimal Zero-Sequences

Definition: Let G be a finite abelian group and $S = \{g_1, \ldots, g_t\}$ be a sequence of not necessarily distinct nonzero elements from G.

1. S is called a *zero-sequence* if $\sum_{i=1}^{t} g_i = 0$.
2. S called a *minimal zero-sequence* (or *mzs*) if it contains no proper subzero-sequence.

Comment: In general, there is no reason that G must be Abelian. If it is not, then this discussion becomes much different and will be left to another time (and another speaker!).

Notation: For S an mzs as above, we set $\mid S \mid = t$. We also let $\mathcal{B}(G)$ represent the set of zero-sequencs of G and $\mathcal{U}(G)$ represent the set of minimal zero-sequences in G. We count these irregardless of order.

Examples

- Let $g \neq 0$ in G with $\mid g \mid = n$. Then

$$S = \underbrace{\{g, \ldots, g\}}_{kn \text{ times}}$$

is a zero-sequence and is minimal if and only if $k = 1$.
In particular, if $G \cong \mathbb{Z}_n = \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}$, then one popular minimal zero-sequence is

$$S = \underbrace{\{\overline{1}, \ldots, \overline{1}\}}_{n \text{ times}}.$$

Examples

- Let $g \neq 0$ in G. Then
$$S = \{g, g^{-1}\}$$
is a minimal zero-sequence.

- If $m_1 + m_2 + \cdots + m_k = n$ is a partition of n, then
$$S = \{\overline{m_1}, \overline{m_2}, \ldots, \overline{m_k}\}$$
is a minimal zero-sequence in $\mathbb{Z}_n$. Since the number of partitions of n is asymptotic to
$$\frac{1}{4n\sqrt{3}} \exp\left(\pi\sqrt{\frac{2n}{3}}\right)$$
the number of minimal zero-sequences in $\mathbb{Z}_n$ grows extremely quickly.

Examples

- Let $g \neq 0$ in G. Then
$$S = \{g, g^{-1}\}$$
is a minimal zero-sequence.

- If $m_1 + m_2 + \cdots + m_k = n$ is a partition of n, then
$$S = \{\overline{m_1}, \overline{m_2}, \ldots, \overline{m_k}\}$$
is a minimal zero-sequence in $\mathbb{Z}_n$. Since the number of partitions of n is asymptotic to
$$\frac{1}{4n\sqrt{3}} \exp\left(\pi\sqrt{\frac{2n}{3}}\right)$$
the number of minimal zero-sequences in $\mathbb{Z}_n$ grows extremely quickly.

Examples

- Let G have invariant form

$$G \cong \mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2} \oplus \cdots \oplus \mathbb{Z}_{n_k}$$

and e_i be the element of G consisting of 1 in the ith coordinate and 0 elsewhere. Then

$$S_G = \{\underbrace{e_1, \ldots, e_1}_{n_1 - 1 \text{ times}}, \underbrace{e_2, \ldots, e_2}_{n_2 - 1 \text{ times}}, \ldots, \underbrace{e_k, \ldots, e_k}_{n_k - 1 \text{ times}}, e_1 + e_2 + \cdots + e_k\}$$

is a minimal zero-sequence of G. So if $G = \mathbb{Z}_3 \oplus \mathbb{Z}_6$, then

$$S_G = \{(1,0),(1,0),(0,1),(0,1),(0,1),(0,1),(0,1),(1,1)\}.$$

We note in particular that

$$| S_G | = \left[\sum_{i=1}^{k}(n_i - 1)\right] + 1 = 1 - k + \left[\sum_{i=1}^{k} n_i\right].$$

Examples

- Let G have invariant form

$$G \cong \mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2} \oplus \cdots \oplus \mathbb{Z}_{n_k}$$

and e_i be the element of G consisting of 1 in the ith coordinate and 0 elsewhere. Then

$$S_G = \{\underbrace{e_1, \ldots, e_1}_{n_1 - 1 \text{ times}}, \underbrace{e_2, \ldots, e_2}_{n_2 - 1 \text{ times}}, \ldots, \underbrace{e_k, \ldots, e_k}_{n_k - 1 \text{ times}}, e_1 + e_2 + \cdots + e_k\}$$

is a minimal zero-sequence of G. So if $G = \mathbb{Z}_3 \oplus \mathbb{Z}_6$, then

$$S_G = \{(1,0),(1,0),(0,1),(0,1),(0,1),(0,1),(0,1),(1,1)\}.$$

We note in particular that

$$\mid S_G \mid = \left[\sum_{i=1}^{k}(n_i - 1)\right] + 1 = 1 - k + \left[\sum_{i=1}^{k} n_i\right].$$

The Definition

Taking one small liberty (which we will later justify), we make the following definition.

Definition: Let G be a finite abelian group. The *Davenport Constant* of G is

$$\mathsf{D}(G) = \max\{|\, S \,| \mid S \in \mathcal{U}(G)\}.$$

Basic Results

Theorem

If G is a finite Abelian group, then

$$\mathsf{D}(G) \leq \mid G \mid .$$

Proof

Proof.

Let $S = \{g_1, \ldots, g_k\}$ be a minimal zero-sequence with $k > G$. Thus $g_i \neq 0$ for all i. Let

$$\begin{aligned} \gamma_1 &= g_1 \\ \gamma_2 &= g_1 + g_2 \\ \vdots \quad & \vdots \quad \vdots \\ \gamma_k &= g_1 + g_2 + \cdots + g_k \end{aligned}$$

Since none of the γ_i's are 0, $\gamma_i = \gamma_j$ for some $i > j$. Thus

$$g_{j+1} + g_{j+2} + \cdots + g_k = 0,$$

which contradicts the minimality of S. □

Basic Results

Proposition

If $G \cong \mathbb{Z}_n$ for $n > 0$, then $\mathsf{D}(G) = n$.

Proof.

$S = \underbrace{\{\overline{1}, \ldots, \overline{1}\}}_{n \text{ times}}$ is a minimal zero-sequence of length n. □

Moral: The computation of the Davenport constant on a cyclic group is trivial.

Basic Results

Proposition

If $G \cong \mathbb{Z}_n$ for $n > 0$, then $\mathsf{D}(G) = n$.

Proof.

$S = \underbrace{\{\overline{1}, \ldots, \overline{1}\}}_{n \text{ times}}$ is a minimal zero-sequence of length n. □

Moral: The computation of the Davenport constant on a cyclic group is trivial.

Basic Results

Proposition

If $G \cong \mathbb{Z}_n$ for $n > 0$, then $\mathrm{D}(G) = n$.

Proof.

$S = \underbrace{\{\bar{1}, \ldots, \bar{1}\}}_{n \text{ times}}$ is a minimal zero-sequence of length n. □

Moral: The computation of the Davenport constant on a cyclic group is trivial.

Non-Cyclic Groups

Example

If G is not cyclic, then the fun begins! For instance,

$$\mathbb{Z}_2 \oplus \mathbb{Z}_2 = 3 <| \mathbb{Z}_2 \oplus \mathbb{Z}_2 |= 4$$

as

$$S_{\mathbb{Z}_2 \oplus \mathbb{Z}_2} = \{(1,0), (0,1), (1,1)\}$$

is the longest minimal zero-sequence of $\mathbb{Z}_2 \oplus \mathbb{Z}_2$.

Let's return to S_G for $G \cong \mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2} \oplus \cdots \oplus \mathbb{Z}_{n_k}$ written in invariant form. We set

$$\mathrm{D}^*(G) =| S_G |= \left[\sum_{i=1}^{k}(n_i - 1)\right] + 1.$$

Non-Cyclic Groups

Example

If G is not cyclic, then the fun begins! For instance,

$$\mathbb{Z}_2 \oplus \mathbb{Z}_2 = 3 <| \mathbb{Z}_2 \oplus \mathbb{Z}_2 |= 4$$

as

$$S_{\mathbb{Z}_2 \oplus \mathbb{Z}_2} = \{(1,0),(0,1),(1,1)\}$$

is the longest minimal zero-sequence of $\mathbb{Z}_2 \oplus \mathbb{Z}_2$.

Let's return to S_G for $G \cong \mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2} \oplus \cdots \oplus \mathbb{Z}_{n_k}$ written in invariant form. We set

$$\mathrm{D}^*(G) =| S_G |= \left[\sum_{i=1}^{k}(n_i - 1)\right] + 1.$$

The Erdős Conjecture

Theorem

If G is a finite abelian group, then

$$\mathrm{D}^*(G) \leq \mathrm{D}(G) \leq |G| .$$

Conjecture (Erdős (mid 1960's))

If G is a finite abelian group, then

$$\mathrm{D}(G) = \mathrm{D}^*(G).$$

The Erdős Conjecture

Theorem

If G is a finite abelian group, then

$$\mathsf{D}^*(G) \le \mathsf{D}(G) \le | G | .$$

Conjecture (Erdős (mid 1960's))

If G is a finite abelian group, then

$$\mathsf{D}(G) = \mathsf{D}^*(G).$$

The Erdős Conjecture is False!

van Emde Boas finally disproved this conjecture in 1969.

Example: Let

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

(here $\mathsf{D}^*(G) = 10$) and set $e_1 = (0,1,1,1,1)$, $e_2 = (1,0,1,1,1)$, $e_3 = (1,1,0,1,1)$, $e_4 = (1,1,1,0,1)$, $e_5 = (0,0,0,0,1)$, $e_6 = (1,0,0,0,4)$, $e_7 = (0,1,0,0,4)$, $e_8 = (0,0,1,0,4)$, $e_9 = (0,0,0,1,4)$ and $e_{10} = (1,1,1,1,4)$. Then T=

$$\{e_1, e_2, e_3, e_4, e_4, e_5, e_6, e_7, e_8, e_9, e_{10}\}$$

is a sequence of length 10 which is not a zero sequence and does not contain a mzs. Thus $\mathsf{D}(G) > \mathsf{D}^* = 10$.

This is the group of smallest known order (96) for which $\mathsf{D}(G) > \mathsf{D}^*$**.**

Is There An Easy Explanation?

Set $G = \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_6 = \mathbb{Z}_2^5 \oplus \mathbb{Z}_3$. Moreover, for $k \geq 5$, set

$$G_k = \mathbb{Z}_2^k \oplus \mathbb{Z}_3.$$

k	$\mathsf{D}(G_k)$	$\mathsf{D}^*(G_k)$
5	11	10
6	12	11
7	13	12
8	15	13

$k = 9 \Rightarrow$ **THE COMPUTER EXPLODES!**

Is There An Easy Explanation?

Set $G = \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_6 = \mathbb{Z}_2^5 \oplus \mathbb{Z}_3$. Moreover, for $k \geq 5$, set

$$G_k = \mathbb{Z}_2^k \oplus \mathbb{Z}_3.$$

k	$\mathsf{D}(G_k)$	$\mathsf{D}^*(G_k)$
5	11	10
6	12	11
7	13	12
8	15	13

$k = 9 \Rightarrow$ **THE COMPUTER EXPLODES!**

Is There An Easy Explanation?

Set $G = \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_6 = \mathbb{Z}_2^5 \oplus \mathbb{Z}_3$. Moreover, for $k \geq 5$, set

$$G_k = \mathbb{Z}_2^k \oplus \mathbb{Z}_3.$$

k	$\mathsf{D}(G_k)$	$\mathsf{D}^*(G_k)$
5	11	10
6	12	11
7	13	12
8	15	13

$k = 9 \Rightarrow$ **THE COMPUTER EXPLODES!**

Open Problem

In a similar manner one can show that

$$G \cong \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_6$$

has $\mathsf{D}(G) > \mathsf{D}^*(G) = 12$.

This is the group of smallest known rank (4) for which $\mathsf{D}(G) > \mathsf{D}^*(G)$.

Theorem (Olson, JNT 1969)

If G is a finite abelian group of rank ≤ 2, then $\mathsf{D}(G) = \mathsf{D}^*(G)$.

Open For More Than 50 Years Problem: Let G be a finite abelian group of rank 3. Is $\mathsf{D}(G) = \mathsf{D}^*(G)$?

Open Problem

In a similar manner one can show that

$$G \cong \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_6$$

has $\mathsf{D}(G) > \mathsf{D}^*(G) = 12$.

This is the group of smallest known rank (4) for which $\mathsf{D}(G) > \mathsf{D}^*(G)$.

Theorem (Olson, JNT 1969)

If G is a finite abelian group of rank ≤ 2, then $\mathsf{D}(G) = \mathsf{D}^*(G)$.

Open For More Than 50 Years Problem: Let G be a finite abelian group of rank 3. Is $\mathsf{D}(G) = \mathsf{D}^*(G)$?

Open Problem

In a similar manner one can show that

$$G \cong \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_6$$

has $\mathsf{D}(G) > \mathsf{D}^*(G) = 12$.

This is the group of smallest known rank (4) for which $\mathsf{D}(G) > \mathsf{D}^*(G)$.

Theorem (Olson, JNT 1969)

If G is a finite abelian group of rank ≤ 2, then $\mathsf{D}(G) = \mathsf{D}^*(G)$.

Open For More Than 50 Years Problem: Let G be a finite abelian group of rank 3. Is $\mathsf{D}(G) = \mathsf{D}^*(G)$?

The Cross Number

There is a large class of groups for which it is known that $\mathsf{D}(G) = \mathsf{D}^*(G)$

Theorem: *If G is any of the following finite abelian groups, then* $\mathsf{D}(G) = \mathsf{D}^*(G)$.

1. *G has rank less than or equal to 2.*
2. *G is a p-group for p prime in $\mathbb{Z}$. (Olson, JNT 1969)*
3. $G \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_{2m}$ *with m odd.*
4. $G \cong \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_{6m}$ *where* $\gcd(3, m) = 1$.
5. $G \cong \mathbb{Z}_{3\cdot 2^n} \oplus \mathbb{Z}_{3\cdot 2^m} \oplus \mathbb{Z}_{3\cdot 2^s}$ *where* $n \leq m \leq s$.

$$\vdots$$

The Cross Number

Here are two recent results of note.

Theorem

Let $G \cong \mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2} \oplus \cdots \oplus \mathbb{Z}_{n_k}$ be a finite abelian group written in invariant form.

1. *(Meshulam 1990 Discrete Math.)* $\mathsf{D}(G) \le n_k \left(1 + \log \frac{|G|}{n_k}\right)$.
2. *(Dimitrov 2007)* $\frac{\mathsf{D}(G)}{\mathsf{D}^*(G)} \le (Ck \log k)^k$ *for some absolute constant* C*.*

We close this section with an obvious problem.

Problem: Given a finite abelian group G, find a formula for $D(G)$.

The Cross Number

Here are two recent results of note.

Theorem

Let $G \cong \mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2} \oplus \cdots \oplus \mathbb{Z}_{n_k}$ be a finite abelian group written in invariant form.

1. *(Meshulam 1990 Discrete Math.)* $\mathsf{D}(G) \le n_k \left(1 + \log \frac{|G|}{n_k}\right)$.
2. *(Dimitrov 2007)* $\frac{\mathsf{D}(G)}{\mathsf{D}^*(G)} \le (Ck \log k)^k$ *for some absolute constant C.*

We close this section with an obvious problem.

Problem: Given a finite abelian group G, find a formula for $D(G)$.

The Cross Number

Here are two recent results of note.

Theorem

Let $G \cong \mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2} \oplus \cdots \oplus \mathbb{Z}_{n_k}$ *be a finite abelian group written in invariant form.*

1. *(Meshulam 1990 Discrete Math.)* $\mathrm{D}(G) \leq n_k \left(1 + \log \frac{|G|}{n_k}\right)$.
2. *(Dimitrov 2007)* $\frac{\mathrm{D}(G)}{\mathrm{D}^*(G)} \leq (Ck \log k)^k$ *for some absolute constant* C.

We close this section with an obvious problem.

Problem: Given a finite abelian group G, find a formula for $D(G)$.

The Cross Number

We shift gears and consider another invariant related to the Davenport constant. **From this point onward, we will use groups written in terms of their elementary divisors**.

Definitions: Let G be a finite abelian group and $S = \{g_1, \ldots, g_t\}$ a zero-sequence of G. The *cross number* of S is

$$\Bbbk(S) = \sum_{i=1}^{t} \frac{1}{\mid g_i \mid}$$

and the *cross number* of G is

$$\mathbb{K}(G) = \max\{\Bbbk(S) \mid S \text{ is an mzs of } G\}.$$

Where did this come from?

Where did this come from? The cross number is a key tool in studying the factorization properties of rings of algebraic integers (like $\mathbb{Z}[\sqrt{-5}]$) and more general objects known as Krull monoids. The details of this will have to be left to another talk.

Notice that

$$\Bbbk : \mathcal{B}(G) \to \mathbb{Q}^+$$

which acts like a homomorphism (i.e. $\Bbbk(S_1S_2) = \Bbbk(S_1) + \Bbbk(S_2)$).

Where did this come from?

Where did this come from? The cross number is a key tool in studying the factorization properties of rings of algebraic integers (like $\mathbb{Z}[\sqrt{-5}]$) and more general objects known as Krull monoids. The details of this will have to be left to another talk.

Notice that

$$\Bbbk : \mathcal{B}(G) \to \mathbb{Q}^+$$

which acts like a homomorphism (i.e. $\Bbbk(S_1S_2) = \Bbbk(S_1) + \Bbbk(S_2)$).

Examples

Examples: Let $G \cong \mathbb{Z}_4$. The minimal zero-sequences and associated cross numbers of $\mathbb{Z}_4$ are:

$$\begin{array}{ll} S_1 = (1,1,1,1) & \Bbbk(S_1) = 1 \\ S_2 = (2,2) & \Bbbk(S_2) = 1 \\ S_3 = (3,3,3,3) & \Bbbk(S_3) = 1 \\ S_4 = (3,1) & \Bbbk(S_4) = 1/2 \\ S_5 = (2,1,1) & \Bbbk(S_5) = 1 \\ S_6 = (2,3,3) & \Bbbk(S_6) = 1 \end{array}$$

Hence, $\mathbb{K}(\mathbb{Z}_4) = 1$.

Examples

Now, let $G \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2$. The minimal zero-sequences and associated cross numbers for $\mathbb{Z}_2 \oplus \mathbb{Z}_2$ are:

$$\begin{array}{ll} S_1 = ((0,1),(0,1)) & \Bbbk(S_1) = 1 \\ S_2 = ((1,1),(1,1)) & \Bbbk(S_2) = 1 \\ S_3 = ((1,0),(1,0)) & \Bbbk(S_3) = 1 \\ S_4 = ((1,0),(0,1),(1,1)) & \Bbbk(S_4) = 3/2 \end{array}$$

Hence, $\mathbb{K}(\mathbb{Z}_2 \oplus \mathbb{Z}_2) = 3/2$.

Basic Facts

Some Elementary Facts: Let $G \cong \mathbb{Z}_{p_1^{s_1}} \oplus \mathbb{Z}_{p_2^{s_2}} \oplus \cdots \oplus \mathbb{Z}_{p_k^{s_k}}$ in elementary divisor form. Recall that $\exp(G) = \mathrm{lcm}\{|\, x \,| \mid x \in G\}$.

1) $\mathbb{K}(G) \geq 1$. (WHY?)

2) Let T_G be the parallel mzs construction for groups in elementary divisor form as that previously called S_G. We have

$$\Bbbk(T_G) = \frac{1}{\exp(G)} + \sum_{i=1}^{k} \frac{p_i^{s_i} - 1}{p_i^{s_i}} = \mathbb{K}^*(G).$$

Hence, $\mathbb{K}(G) \geq \mathbb{K}^*(G)$.

Example

Example

Let $G = \mathbb{Z}_6 \cong \mathbb{Z}_2 \oplus \mathbb{Z}_3$. Here

$$T_{\mathbb{Z}_6} = \{(1,0),(0,1),(0,1),(1,1)\}.$$

So,

$$\Bbbk(T_{\mathbb{Z}_6}) = \frac{1}{2} + \frac{1}{3} + \frac{1}{3} + \frac{1}{6} = \frac{4}{3}.$$

Open for 35 Years Problem: Is $\mathbb{K}(G) = \mathbb{K}^*(G)$ for all finite abelian groups G?

Example

Example

Let $G = \mathbb{Z}_6 \cong \mathbb{Z}_2 \oplus \mathbb{Z}_3$. Here

$$T_{\mathbb{Z}_6} = \{(1,0),(0,1),(0,1),(1,1)\}.$$

So,

$$\Bbbk(T_{\mathbb{Z}_6}) = \frac{1}{2} + \frac{1}{3} + \frac{1}{3} + \frac{1}{6} = \frac{4}{3}.$$

Open for 35 Years Problem: Is $\mathbb{K}(G) = \mathbb{K}^*(G)$ for all finite abelian groups G?

Some Facts

Some Not So Elementary Facts:

1) (Krause, *Math. Zeit.* 1984) $\mathbb{K}(G) = 1$ if and only if $G \cong \mathbb{Z}_{p^n}$ for some prime number p.

2) (Geroldinger, *JNT* 1994) If G is a p-group (for p a prime) then $\mathbb{K}(G) = \mathbb{K}^*(G)$.

3) If G is any of the following abelian groups, then $\mathbb{K}(G) = \mathbb{K}^*(G)$.

- **a)** G is a p-group.
- **b)** $G \cong \mathbb{Z}_{p^n q}$ where p and q are distinct primes and $n \geq 1$.
- **c)** $G \cong \mathbb{Z}_{pqr}$ where p, q and r are distinct primes.
- **d)** $G \cong \mathbb{Z}_{p^2 q^2}$ where p and q are distinct primes.

Moral: If G is cyclic, then $\mathbb{K}(G)$ is probably not easy to compute.

Some Facts

Some Not So Elementary Facts:

1) (Krause, *Math. Zeit.* 1984) $\mathbb{K}(G) = 1$ if and only if $G \cong \mathbb{Z}_{p^n}$ for some prime number p.

2) (Geroldinger, *JNT* 1994) If G is a p-group (for p a prime) then $\mathbb{K}(G) = \mathbb{K}^*(G)$.

3) If G is any of the following abelian groups, then $\mathbb{K}(G) = \mathbb{K}^*(G)$.

- **a)** G is a p-group.
- **b)** $G \cong \mathbb{Z}_{p^n q}$ where p and q are distinct primes and $n \geq 1$.
- **c)** $G \cong \mathbb{Z}_{pqr}$ where p, q and r are distinct primes.
- **d)** $G \cong \mathbb{Z}_{p^2 q^2}$ where p and q are distinct primes.

Moral: If G is cyclic, then $\mathbb{K}(G)$ is probably not easy to compute.

A Closing Example

Theorem

(Chapman-Geroldinger, ARS Comb. 1996) Let $G \cong \mathbb{Z}_{p^{n_1}} \oplus \cdots \mathbb{Z}_{p^{n_k}}$ be a p-group with p odd. Thus

$$\mathbb{K}(G) = \frac{1}{p^{n_k}} + \sum_{i=1}^{k} \frac{p^{n_i} - 1}{p^{n_i}} = \frac{X}{p^{n_k}}.$$

Then,

$$\{\Bbbk(S) \mid S \in \mathcal{U}(G)\} = \{\frac{2}{p^k}, \frac{3}{p^k}, \ldots, \frac{X-1}{p^k}, \frac{X}{p^k}\}.$$

Example

Example

Let $G = \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_9$.

$$\mathsf{k}(T_G) = \frac{1}{9} + 4 \cdot \frac{1}{3} + 8 \cdot \frac{1}{9} = \frac{21}{9} = \mathbb{K}^*(G) = \mathbb{K}(G).$$

$$\{\mathsf{k}(S) \mid S \in \mathcal{U}(\mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_9)\} = \{\frac{2}{9}, \frac{3}{9}, \ldots, \frac{20}{9}, \frac{21}{9}\}.$$

Question: What happens if G is not a p-group?

Example

Example

Let $G = \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_9$.

$$\Bbbk(T_G) = \frac{1}{9} + 4 \cdot \frac{1}{3} + 8 \cdot \frac{1}{9} = \frac{21}{9} = \mathbb{K}^*(G) = \mathbb{K}(G).$$

$$\{\Bbbk(S) \mid S \in \mathcal{U}(\mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_9)\} = \{\frac{2}{9}, \frac{3}{9}, \ldots, \frac{20}{9}, \frac{21}{9}\}.$$

Question: What happens if G is not a p-group?

Example

Example

Let $G = \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_9$.

$$\Bbbk(T_G) = \frac{1}{9} + 4 \cdot \frac{1}{3} + 8 \cdot \frac{1}{9} = \frac{21}{9} = \mathbb{K}^*(G) = \mathbb{K}(G).$$

$$\{\Bbbk(S) \mid S \in \mathcal{U}(\mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_9)\} = \{\frac{2}{9}, \frac{3}{9}, \ldots, \frac{20}{9}, \frac{21}{9}\}.$$

Question: What happens if G is not a p-group?

A Closing Example

An Example taken from Geroldinger & Schneider (ARS Comb. 1997). Let $p = 5$ and $q = 3$:

$$\{\Bbbk(S) \mid S \in \mathcal{U}(\mathbb{Z}_{15})\} = \{\frac{2}{15}, \frac{3}{15}, \frac{4}{15}, \ldots, \frac{20}{15}, \frac{21}{15}, \frac{23}{15}\}.$$

In Baginski et. al. (ARS Comb. 2004), the authors show (redacted version):

If $p >> q$, then these holes multiply! For $p = 11$ and $q = 5$, we obtain:

$$\{\Bbbk(S) \mid S \in \mathcal{U}(\mathbb{Z}_{55})\} = \{\frac{2}{55}, \frac{3}{55}, \frac{4}{55}, \ldots, \frac{87}{55}, \frac{90}{55}, \frac{91}{55}, \frac{95}{55}\}.$$

A Closing Example

An Example taken from Geroldinger & Schneider (ARS Comb. 1997). Let $p = 5$ and $q = 3$:

$$\{\Bbbk(S) \mid S \in \mathcal{U}(\mathbb{Z}_{15})\} = \{\frac{2}{15}, \frac{3}{15}, \frac{4}{15}, \ldots, \frac{20}{15}, \frac{21}{15}, \frac{23}{15}\}.$$

In Baginski et. al. (ARS Comb. 2004), the authors show (redacted version):

If $p >> q$, then these holes multiply! For $p = 11$ and $q = 5$, we obtain:

$$\{\Bbbk(S) \mid S \in \mathcal{U}(\mathbb{Z}_{55})\} = \{\frac{2}{55}, \frac{3}{55}, \frac{4}{55}, \ldots, \frac{87}{55}, \frac{90}{55}, \frac{91}{55}, \frac{95}{55}\}.$$