Proof of Kemnitz' Conjecture and a generalization to higher dimensions

Panwei Hu

Introduction

We define a d-dimensional affine space V and consider the set of points which lie in the set

$$V_d := \left\{ \sum_{i=1}^{d} \alpha_i v_i \;\middle|\; \alpha_i \in \mathbb{Z}, \quad 1 \le i \le d \right\},$$

where $\left\{ v_i \;\middle|\; 1 \le i \le d \right\}$ are linear independent vectors in V. We also call the points in V_d as *lattice* points.

Problem 1

Find out the minimum of the number f s.t. given f sequences in V_d, we can guarantee to find out a subsequence of length n, s.t. the centroid of this subsequence is also a lattice point. We define such minimum number as $f(n, d)$.

Goal

Goal

Find the exact value of $f(n, d)$, if not possible, study the upper and lower bound of $f(n, d)$

Goal

Goal

Find the exact value of $f(n, d)$, if not possible, study the upper and lower bound of $f(n, d)$

Consider the additive group $G := \mathbb{Z}_n^d$. We call a subsequence of length n, which sums to a 0 in $\mathbb{Z}_n^d$ as 0-sum n-subsequence, where 0 denotes the zero vector in G.

Goal

Goal

Find the exact value of $f(n, d)$, if not possible, study the upper and lower bound of $f(n, d)$

Consider the additive group $G := \mathbb{Z}_n^d$. We call a subsequence of length n, which sums to a 0 in $\mathbb{Z}_n^d$ as 0-sum n-subsequence, where 0 denotes the zero vector in G.

Problem 2

Find the number $f(n, d)$, s.t. for any sequences of elements in G, with length $l \geq f(n, d)$, there exists a 0-sum n-subsequence.

Goal

Goal

Find the exact value of $f(n, d)$, if not possible, study the upper and lower bound of $f(n, d)$

Consider the additive group $G := \mathbb{Z}_n^d$. We call a subsequence of length n, which sums to a 0 in $\mathbb{Z}_n^d$ as 0-sum n-subsequence, where 0 denotes the zero vector in G.

Problem 2

Find the number $f(n, d)$, s.t. for any sequences of elements in G, with length $l \geq f(n, d)$, there exists a 0-sum n-subsequence.

Observation

Problem 1 and Problem 2 are equivalent

A natural bound on $f(n, d)$

Lemma 2.2

$$(n-1)2^d + 1 \leq f(n, d) \leq (n-1)n^d + 1 \tag{1}$$

A natural bound on $f(n, d)$

Lemma 2.2

$$(n-1)2^d + 1 \leq f(n, d) \leq (n-1)n^d + 1 \tag{1}$$

Proof.

Left inequality: Construct $(n-1)2^d$ vectors, which include all the vectors in $\mathbb{Z}_n^d$, which has 0 or 1 in their entry, so there are in all 2^d different vectors. Each vector appear exactly $n-1$ times. It is impossible to find a 0-sum n-subsequence among these vectors.

A natural bound on $f(n, d)$

Lemma 2.2

$$(n-1)2^d + 1 \leq f(n, d) \leq (n-1)n^d + 1 \tag{1}$$

Proof.

Left inequality: Construct $(n-1)2^d$ vectors, which include all the vectors in $\mathbb{Z}_n^d$, which has 0 or 1 in their entry, so there are in all 2^d different vectors. Each vector appear exactly $n-1$ times. It is impossible to find a 0-sum n-subsequence among these vectors.
Right inequality: pigeon hole principle
Since $\left|G\right| = n^d$, given $(n-1)n^d + 1$ elements, there are at least one vector v which has multiplicity

$$\lceil\frac{(n-1)n^d + 1}{n^d}\rceil = n.$$

□

Decomposition of $f(n, d)$ (1)

Lemma 2.3

$$f(pq, d) \leq f(p, d) + p(f(q, d) - 1) \tag{2.3.1}$$

Proof.

For the convenience of notation, we define

$$f_1 := f(p, d), f_2 := f(q, d), f := f_1 + p(f_2 - 1).$$

since

$$f = f_1 + p(f_2 - 1),$$

we would obtain f_2 0-sum p-subsequences. Among all these f_2 vectors, there exists a 0-sum q-subsequence, which means they sum to a vector z, with each component divisible by q. Since each summand has components all divisible by p, the resultant vectors will be divisible by $pq = n$, thus we obtain a 0-sum n-subsequence. $\square$

Decomposition of $f(n, d)$ (2)

Due to the symmetry we would obtain similarly:

$$f(pq, d) \leq f(q, d) + q(f(p, d) - 1) \tag{2.3.1'}$$

Decomposition of $f(n,d)$ (2)

Due to the symmetry we would obtain similarly:

$$f(pq,d) \leq f(q,d) + q(f(p,d) - 1) \tag{2.3.1'}$$

Combining (2.3.1) and (2.3.1'), we obtain the following upper bound.

Corollary 2.5

$$f(pq,d) \leq \min\{f(p,d) + p(f(q,d) - 1), f(q,d) + q(f(p,d) - 1)\} \tag{2}$$

Decomposition of $f(n,d)$ (2)

Due to the symmetry we would obtain similarly:

$$f(pq,d) \leq f(q,d) + q(f(p,d)-1) \tag{2.3.1'}$$

Combining (2.3.1) and (2.3.1'), we obtain the following upper bound.

Corollary 2.5

$$f(pq,d) \leq \min\{f(p,d)+p(f(q,d)-1), f(q,d)+q(f(p,d)-1)\} \tag{2}$$

Theorem 2.5 (Cauchy-Davenport)

Let p be a prime number. If $A, B \subset \mathbb{Z}_p$ are nonempty, then

$$\left|A+B\right| \geq \min\{p, \left|A\right| + \left|B\right| - 1\},$$

where $A+B := \left\{ a+b \,\middle|\, a \in A, b \in B \right\}$

Examples

Theorem 2.7 (Erdös-Ginsburg-Ziv)

$$f(n,1) = 2n - 1$$

Proof sketches.

From (1):

$$f(n,1) \geq 2n - 1 \tag{3}$$

Only need to show

$$f(n,1) \leq 2n - 1. \tag{4}$$

Examples

Theorem 2.7 (Erdös-Ginsburg-Ziv)

$$f(n,1) = 2n - 1$$

Proof sketches.

From (1):

$$f(n,1) \geq 2n - 1 \tag{3}$$

Only need to show

$$f(n,1) \leq 2n - 1. \tag{4}$$

Recall $\qquad f(pq,d) \leq f(p,d) + p(f(q,d) - 1)$

Examples

Theorem 2.7 (Erdös-Ginsburg-Ziv)

$$f(n,1) = 2n - 1$$

Proof sketches.

From (1):

$$f(n,1) \geq 2n - 1 \tag{3}$$

Only need to show

$$f(n,1) \leq 2n - 1. \tag{4}$$

Recall $\quad f(pq,d) \leq f(p,d) + p(f(q,d) - 1)$

1. restrict to prime number $(f(pq,1) \leq 2pq - 1)$
2. application of Theorem 1 to prove

$$f(p,1) \leq 2p - 1$$

$\square$

Proof of (4)(1)

Proof of (4)(2)

Further examples

Lemma 2.8

$$f(2^n, d) = (2^n - 1)2^d + 1$$

Further examples

Lemma 2.8

$$f(2^n, d) = (2^n - 1)2^d + 1$$

Lemma 2.9

$$f(3^n, 2) = 4 \cdot 3^n - 3$$

Further examples

Lemma 2.8

$$f(2^n, d) = (2^n - 1)2^d + 1$$

Lemma 2.9

$$f(3^n, 2) = 4 \cdot 3^n - 3$$

Problem

Is it true for all $n \in \mathbb{Z}$,

$$f(n, 2) = 4n - 3$$

This is the well-known *Kemnitz' Conjecture*

Remark

Notation: $\equiv$ means modulo in $\mathbb{Z}_p$.
The 0 denotes the usual neutral element of addition in the corresponding abelian group. In particular, 0 denotes the standard 0 in the abelian group $\mathbb{Z}_p$ and $(0,0)$ in the case of $\mathbb{Z}_p \times \mathbb{Z}_p$.

Remark

Notation: $\equiv$ means modulo in $\mathbb{Z}_p$.
The 0 denotes the usual neutral element of addition in the corresponding abelian group. In particular, 0 denotes the standard 0 in the abelian group $\mathbb{Z}_p$ and $(0,0)$ in the case of $\mathbb{Z}_p \times \mathbb{Z}_p$.

Theorem 3.1 (*Chevalley-Warning Theorem*)

Let p be a prime number and $q = p^t, t \in \mathbb{N}$. We use $\mathbb{F}_q$ to denote the finite field of q elements. Let $p_1, \ldots, p_m$ be m polynomials in $\mathbb{F}_q[x_1, x_2, \ldots, x_n]$, with degree d_i. Denote the number of common zeros of the m polynomials as N. If

$$\sum_{i=1}^{m} d_i < n,$$

then

$$N \equiv 0 \pmod{p}$$

Main Theorem (*Kemnitz' Conjecture*)

Any choice of $4p - 3$ *lattice points in the plane* $\mathbb{Z} \times \mathbb{Z}$ *contains a subset of cardinality* p *whose centroid is a lattice point. In other words:*

$$f(n, 2) = 4n - 3$$

First reduction

Main Theorem (*Kemnitz' Conjecture*)

$$f(n, 2) = 4n - 3$$

Proposition

It suffices to consider the case for n is an odd prime number.

First reduction

Main Theorem (*Kemnitz' Conjecture*)

$$f(n, 2) = 4n - 3$$

Proposition

It suffices to consider the case for n is an odd prime number.

Notation

Denote J, X and other capital alphabets as a multiset of $\mathbb{Z}_p \times \mathbb{Z}_p$.

$(p|J) \quad \widehat{=} \quad$ number of 0-sum p-subsequence in J.

Corollary 3.2

If $\left|J\right| = 3p - 3$, *then* $1 - (p-1|J) - (p|J) + (2p-1|J) + (2p|J) \equiv 0$

Corollary 3.2

If $\left|J\right| = 3p - 3$, *then* $1 - (p-1|J) - (p|J) + (2p-1|J) + (2p|J) \equiv 0$

We consider three polynomials

$$p_1 := \sum_{n=1}^{3p-3} x_n^{p-1} + x_{3p-2}^{p-1}, \quad p_2 := \sum_{n=1}^{3p-3} a_n x_n^{p-1}, \quad p_3 := \sum_{n=1}^{3p-3} b_n x_n^{p-1}$$

Corollary 3.2

If $\left|J\right| = 3p-3$*, then* $1 - (p-1|J) - (p|J) + (2p-1|J) + (2p|J) \equiv 0$

We consider three polynomials

$$p_1 := \sum_{n=1}^{3p-3} x_n^{p-1} + x_{3p-2}^{p-1}, \quad p_2 := \sum_{n=1}^{3p-3} a_n x_n^{p-1}, \quad p_3 := \sum_{n=1}^{3p-3} b_n x_n^{p-1}$$

Since the total sum of degress are $3(p-1) = 3p-3 < 3p-2$, we can apply the *Chevalley-Warning Theorem*.

Corollary 3.2

If $\left|J\right| = 3p-3$, *then* $1-(p-1|J)-(p|J)+(2p-1|J)+(2p|J) \equiv 0$

We consider three polynomials

$$p_1 := \sum_{n=1}^{3p-3} x_n^{p-1} + x_{3p-2}^{p-1}, \quad p_2 := \sum_{n=1}^{3p-3} a_n x_n^{p-1}, \quad p_3 := \sum_{n=1}^{3p-3} b_n x_n^{p-1}$$

Since the total sum of degress are $3(p-1) = 3p-3 < 3p-2$, we can apply the *Chevalley-Warning Theorem*.
Since three polynomials have 0 as a common zero, the *Chevalley-Warning Theorem* states that there are non-trivial common zeros. We consider the common zeros depending on the term x_{3p-2} in p_1.

Proof of Corollary 3.2(1) $x_{3n-2} = 0$

$x_{3n-2} = 0$

Proof of Corollary 3.2(1) $x_{3n-2} = 0$

$x_{3n-2} = 0$

$$p_1 := \sum_{n=1}^{3p-3} x_n^{p-1} + x_{3p-2}^{p-1}$$

$$p_2 := \sum_{n=1}^{3p-3} a_n x_n^{p-1}$$

$$p_3 := \sum_{n=1}^{3p-3} b_n x_n^{p-1}$$

Proof of Corollary 3.2(1) $x_{3n-2} = 0$

$x_{3n-2} = 0$

$$p_1 := \sum_{n=1}^{3p-3} x_n^{p-1} + x_{3p-2}^{p-1}$$

$$p_2 := \sum_{n=1}^{3p-3} a_n x_n^{p-1}$$

$$p_3 := \sum_{n=1}^{3p-3} b_n x_n^{p-1}$$

In this case for the zero of p_1, it needs to satisfy

$$\sum_{n=1}^{3p-3} x_n^{p-1} \equiv 0$$

We know that

$$x^{p-1} \equiv \begin{cases} 1, & \text{if } x \not\equiv 0; \\ 0, & \text{if } x \equiv 0. \end{cases}$$

Since there are in all $3p-3$ variables left, there could only be three cases:

Proof of Corollary 3.2(2)

$$p_1 := \sum_{n=1}^{3p-3} x_n^{p-1} + x_{3p-2}^{p-1}$$

$$p_2 := \sum_{n=1}^{3p-3} a_n x_n^{p-1}$$

$$p_3 := \sum_{n=1}^{3p-3} b_n x_n^{p-1}$$

Proof of Corollary 3.2(2)

$$p_1 := \sum_{n=1}^{3p-3} x_n^{p-1} + x_{3p-2}^{p-1}$$

$$p_2 := \sum_{n=1}^{3p-3} a_n x_n^{p-1}$$

$$p_3 := \sum_{n=1}^{3p-3} b_n x_n^{p-1}$$

- 0 of them are 1: # 1

Proof of Corollary 3.2(2)

$$p_1 := \sum_{n=1}^{3p-3} x_n^{p-1} + x_{3p-2}^{p-1}$$

$$p_2 := \sum_{n=1}^{3p-3} a_n x_n^{p-1}$$

$$p_3 := \sum_{n=1}^{3p-3} b_n x_n^{p-1}$$

- 0 of them are 1: # 1
- p of them are 1: $x_{i_1}, \ldots, x_{i_p}$.

Proof of Corollary 3.2(2)

$$p_1 := \sum_{n=1}^{3p-3} x_n^{p-1} + x_{3p-2}^{p-1}$$

$$p_2 := \sum_{n=1}^{3p-3} a_n x_n^{p-1}$$

$$p_3 := \sum_{n=1}^{3p-3} b_n x_n^{p-1}$$

- 0 of them are 1: # 1
- p of them are 1: $x_{i_1}, \ldots, x_{i_p}$.

  $$\sum_{j=1}^{p} a_{i_j} \equiv 0, \quad \sum_{j=1}^{p} b_{i_j} \equiv 0.$$

  $\# \ (p-1)^p (p|J)$.
- $2p$ of them are 1:
  $\# \ (p-1)^{2p} (2p|J)$.

Proof of Corollary 3.2(3)

$$p_1 := \sum_{n=1}^{3p-3} x_n^{p-1} + x_{3p-2}^{p-1}$$

$$p_2 := \sum_{n=1}^{3p-3} a_n x_n^{p-1}$$

$$p_3 := \sum_{n=1}^{3p-3} b_n x_n^{p-1}$$

Proof of Corollary 3.2(3)

$$p_1 := \sum_{n=1}^{3p-3} x_n^{p-1} + x_{3p-2}^{p-1}$$

$$p_2 := \sum_{n=1}^{3p-3} a_n x_n^{p-1}$$

$$p_3 := \sum_{n=1}^{3p-3} b_n x_n^{p-1}$$

- $p-1$ of them are 1.
  $\# \ (p-1)^p (p-1|J)$

Proof of Corollary 3.2(3)

$$p_1 := \sum_{n=1}^{3p-3} x_n^{p-1} + x_{3p-2}^{p-1}$$

$$p_2 := \sum_{n=1}^{3p-3} a_n x_n^{p-1}$$

$$p_3 := \sum_{n=1}^{3p-3} b_n x_n^{p-1}$$

- $p-1$ of them are 1.
  $\# \ (p-1)^p (p-1|J)$
- $2p-1$ of them are 1.
  $\# \ (p-1)^{2p} (2p-1|J)$

Proof of Corollary 3.2(3)

$$p_1 := \sum_{n=1}^{3p-3} x_n^{p-1} + x_{3p-2}^{p-1}$$

$$p_2 := \sum_{n=1}^{3p-3} a_n x_n^{p-1}$$

$$p_3 := \sum_{n=1}^{3p-3} b_n x_n^{p-1}$$

- $p-1$ of them are 1.
  $\#\ (p-1)^p(p-1|J)$
- $2p-1$ of them are 1.
  $\#\ (p-1)^{2p}(2p-1|J)$

Collecting all the number of common zeros considered in different cases

$$1+(p-1)^p(p|J)+(p-1)^{2p}(2p|J)+(p-1)^p(p-1|J)+(p-1)^{2p}(2p-1|J) \equiv 0$$

Simplifying the equation above we obtain

$$1-(p-1|J)-(p|J)+(2p-1|J)+(2p|J) \equiv 0$$

Corollary 3.3

If $|J| = 3p - 2$, *or* $|J| = 3p - 1$, *then* $1 - (p|J) + (2p|J) \equiv 0$

Corollary 3.3

If $|J| = 3p - 2$, *or* $|J| = 3p - 1$, *then* $1 - (p|J) + (2p|J) \equiv 0$

Corollary 3.5

If $\left|J\right| = 3p - 2$ *or* $\left|J\right| = 3p - 1$, *then* $(p|J) = 0$ *implies* $(2p|J) \equiv -1$.

Corollary 3.3

If $|J| = 3p - 2$, *or* $|J| = 3p - 1$, *then* $1 - (p|J) + (2p|J) \equiv 0$

Corollary 3.5

If $\Big|J\Big| = 3p - 2$ *or* $\Big|J\Big| = 3p - 1$, *then* $(p|J) = 0$ *implies* $(2p|J) \equiv -1$.

Corollary 3.6

If J *contains exactly* $3p$ *elements, and* $\sum_{x \in J} x \equiv 0$, *then* $(p|J) > 0$.

Proof of Corollary 3.6

Proof.

If $(p|J) = 0 \Rightarrow$

$$\forall x \in J, \quad (p|J - x) = 0.$$

Proof of Corollary 3.6

Proof.

If $(p|J) = 0 \Rightarrow$

$$\forall x \in J, \quad (p|J - x) = 0.$$

$\left|J - x\right| = 3p - 1 \Rightarrow$

$$(2p|J - x) \equiv -1.$$

In particular

$$(2p|J - x) > 0$$

Proof of Corollary 3.6

Proof.

If $(p|J) = 0 \Rightarrow$

$$\forall x \in J, \quad (p|J - x) = 0.$$

$\left|J - x\right| = 3p - 1 \Rightarrow$

$$(2p|J - x) \equiv -1.$$

In particular

$$(2p|J - x) > 0$$

$\forall A \subset J$, s.t. $\sum_{a \in A} a \equiv 0$,

$$\sum_{a \in A} a + \sum_{b \in J - A} b = \sum_{j \in J} j \equiv 0$$
$$\Rightarrow \sum_{b \in J - A} b \equiv 0$$

The map T

$$T : \left\{ A \subset J \,\middle|\, |A| = p, \sum_{a \in A} a \equiv 0 \right\} \to \left\{ A \subset J \,\middle|\, |A| = 2p, \sum_{a \in A} a \equiv 0 \right\}$$

$$A \mapsto J - A$$

is a bijection. It follows that:

$$(p|J) = (2p|J) \geq (2p|J - x) > 0,$$

which is a contradiction to the assumption $(p|J) = 0$ $\square$

Corollary

If $\left|X\right| = 4p-3$, *then*

1. $-1+(p|X)-(2p|X)+(3p|X) \equiv 0$
2. $(p-1|X)-(2p-1|X)+(3p-1|X) \equiv 0$

Corollary

If $\left|X\right| = 4p-3$, *then* $3-2(p-1|X)-2(p|X)+(2p-1|X)+(2p|X) \equiv 0.$

Proof.

We deduce from Corollary 3.2 that:

$$\sum_I 1 - (p-1|I) - (p|I) + (2p-1|I) + (2p|I) \equiv 0,$$

where the sum is over $I \subset X$, s.t, $\left|I\right| = 3p-3$. For a given subset $Y \subset X$,s.t $\left|Y\right| = p$ and $\sum_{y \in Y} y \equiv 0$, we want to find out the number of pairs (Y, I), s.t $Y \subset I, \left|I\right| = 3p-3$.

We could see that

$$\left|\{(Y, I) | Y \subset I, \left|I\right| = 3p-3\right|\} = \binom{3p-3}{2p-3},$$

since once we have chosen p elements Y, we need to further choose $\left|I\right| - p = 3p-3-p = 2p-3$ elements from total $\left|X\right| - p = 4p-3-p = 3p-3$ elements. Note that

$$\sum_{\substack{Y \subset X, \\ \sum y=0}} \sum_{\substack{I, s.t. \\ Y \subset I}} 1$$

We finally prove that

$$\binom{4p-3}{3p-3} \equiv 3, \binom{3p-2}{2p-2} \equiv 2, \tag{6}$$

because:

$$\begin{aligned}
\binom{4p-3}{3p-3} &\equiv \frac{(4p-3)\cdots(4p-(p-1))\cdot 3p\cdot(3p-1)\cdot(3p-2)}{p!} \\
&\equiv \frac{(4p-3)\cdots(4p-(p-1))\cdot 3\cdot(3p-1)\cdot(3p-2)}{(p-1)!} \\
&\equiv 3\cdot\frac{(-3)\cdot(-4)\cdots(-(p-1))\cdot(-1)\cdot(-2)}{(p-1)!} \\
&\equiv 3\cdot\frac{(p-1)!}{(p-1)!} \\
&\equiv 3
\end{aligned}$$

Note that we have used the fact that p is an odd prime, s.t. $(-1)^{p-1} \equiv 1$. Similarly, one can prove that

Lemma

If $\left|X\right| = 4p - 3$ *and* $(p|X) = 0$, *then* $(p-1|X) \equiv (3p-1|X)$.

Proof.

We consider the partition of $X = A \cup B \cup C$, where

$$\left|A\right| = p - 1, \quad \left|B\right| = p - 2, \quad \left|C\right| = 2p.$$

and

$$\sum_{a \in A} a \equiv 0, \quad \sum_{b \in B} b \equiv \sum_{x \in X} x, \quad \sum_{c \in C} c \equiv 0$$

Let χ denote the number of such partition. We use two ways to compute the number χ, the first one fixes A and find out the possible set C:

$$\chi \equiv \sum_{A} (2p|X - A) \equiv \sum_{A} -1 \equiv -(p - 1|X),$$

where we have used Corollary 4, for $J = X - A$, with $\left|J\right| = 3p - 2$ and the fact that

$$0 \leq (p|J) \leq (p|X) = 0,$$

which leads to $(p|J) = 0$.

Now by fixing B and count the possible set C, we get:

$$\chi \equiv \sum_{B} (2p|X - B) \overset{1}{\equiv} \sum_{B} -1 \overset{2}{\equiv} \sum_{X-B} -1 \overset{3}{\equiv} -(3p - 1|X)$$

For the three equivalences, we have used the following facts:

1. We use the similar argumentation as before, since $\left|X - B\right| = 3p - 1$ and apply Corollary 4 leads to $(2p|X - B) \equiv -1$.
2. The map T defined by:

$$\left\{ B \subset X \;\middle|\; |B| = p - 1, \sum_{b \in B} a \equiv \sum_{x \in X} x \right\} \to \left\{ J \subset X \;\middle|\; |J| = 3p - 1, \sum_{j \in J} j \equiv$$

$$X \mapsto X - B$$

   is a bijection, s.t.

$$\sum_{B} 1 \equiv \sum_{X-B} 1$$

3. Since $\sum_{b \in B} b \equiv \sum_{x \in X} x$, it follows that

Proof of *Kemnitz' Conjecture*

Proof.

$$-1+(p|X)-(2p|X)+(3p|X)\equiv 0 \tag{9}$$

$$(p-1|X)-(2p-1|X)+(3p-1|X)\equiv 0 \tag{10}$$

$$3-2(p-1|X)-2(p|X)+(2p-1|X)+(2p|X)\equiv 0. \tag{11}$$

Proof of *Kemnitz' Conjecture*

Proof.

$$-1 + (p|X) - (2p|X) + (3p|X) \equiv 0 \tag{9}$$

$$(p-1|X) - (2p-1|X) + (3p-1|X) \equiv 0 \tag{10}$$

$$3 - 2(p-1|X) - 2(p|X) + (2p-1|X) + (2p|X) \equiv 0. \tag{11}$$

Adding the three above equations, we obtain:

$$2 - (p-1|X) - (p|X) + (3p-1|X) + (3p|X) \equiv 0 \tag{12}$$

Assume there is a set X, with $\left|X\right| = 4p-3$ which contradicts the thm, that is $(p|X) = 0$. Using the previous Lemma 5, we obtain $(p-1|X) \equiv (3p-1|X)$ Then (12) simplifies to

$$2 - (p|X) + (3p|X) \equiv 0 \tag{13}$$

Since p is odd, we see that $(p|X)$ and $(3p|X)$ could not both be 0. Since we assume that $(p|X) = 0$, it follows that $(3p|X) > 0$, i.e., there is a subset $J \subset X$, $\left|J\right| = 3p$ and $\sum_{j \in J} j \equiv 0$. But from Corollary 5, we see that $(p|J) > 0$, in particular $(p|X) > 0$, which is a contradiction. $\square$

Theorem (*Alon-Dubiner Theorem*)

$\exists c > 0$, *s.t.* $\forall n \in \mathbb{N}$,

$$f(n, d) < (cd \log_2 d)^d n$$