Contents

1. Combinatorial methods

Definition. Let G be an abelian group and $A, B \subseteq G$. The **sumset** of A and B is

$$A + B \coloneqq \{a + b : a \in A, b \in B\}.$$

The **difference set** of A and B is

$$A - B \coloneqq \{a - b : a \in A, b \in B\}.$$

Proposition. $\max\{|A|, |B|\} \leq |A + B| \leq |A| \cdot |B|$.

Proof. Trivial. □

Example. Let $A = [n] = \{1, ..., n\}$. Then $A + A = \{2, ..., 2n\}$ so $|A + A| = 2|A| - 1$.

Lemma. Let $A \subseteq \mathbb{Z}$ be finite. Then $|A + A| \geq 2|A| - 1$ with equality iff A is an arithmetic progression.

Proof.

- Let $A = \{a_1, ..., a_n\}$ with $a_i < a_{i+1}$. Then $a_1 + a_1 < a_1 + a_2 < \cdots < a_1 + a_n < a_2 + a_n < \cdots < a_n + a_n$.
- Note this is not the only choice of increasing sequence that works, in particular, so does $a_1 + a_1 < a_1 + a_2 < a_2 + a_2 < a_2 + a_3 < a_2 + a_4 < \cdots < a_2 + a_n < a_3 + a_n < \cdots < a_n + a_n$.
- So when equality holds, all these sequences must be the same. In particular, $a_2 + a_i = a_1 + a_{i+1}$ for all i.

□

Exercise. If $A, B \subseteq \mathbb{Z}$, then $|A + B| \geq |A| + |B| - 1$ with equality iff A and B are arithmetic progressions with the same common difference.

Example. Let $A, B \subseteq \mathbb{Z}/p$ for p prime. If $|A| + |B| \geq p + 1$, then $A + B = \mathbb{Z}/p$.

Proof.

- $g \in A + B$ iff $A \cap (g - B) \neq \emptyset$ where $(g - B = \{g\} - B)$.
- Let $g \in \mathbb{Z}/p$, then use inclusion-exclusion on $|A \cap (g - B)|$ to conclude result.

□

Theorem (Cauchy-Davenport). Let p be prime, $A, B \subseteq \mathbb{Z}/p$ be non-empty. Then

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

Proof.

- Assume $|A| + |B| \leq p + 1$, and WLOG that $1 \leq |A| \leq |B|$ and $0 \in A$ (by translation).
- Use induction on $|A|$. $|A| = 1$ is trivial.
- Let $|A| \geq 2$ and let $0 \neq a \in A$. Then since p is prime, $\{a, 2a, ..., pa\} = \mathbb{Z}/p$.
- There exists $m \geq 0$ such that $ma \in B$ but $(m + 1)a \notin B$. Let $B' = B - ma$, so $0 \in B'$, $a \notin B'$ and $|B'| = |B|$.
- $1 \leq |A \cap B'| < |A|$ (why?) so the inductive hypothesis applies to $A \cap B'$ and $A \cup B'$.

- Since $(A \cap B') + (A \cup B') \subseteq A + B'$ (why?), we have $|A+B| = |A+B'| \geq |(A \cap B') + (A \cup B')| \geq |A \cap B'| + |A \cup B'| - 1 = |A| + |B| - 1$.

$\square$

Exercise. Find a counterexample for Cauchy-Davenport for general abelian groups (e.g. $\mathbb{Z}/n$ for n composite).

Example. Fix a small prime p and let $V \subseteq \mathbb{F}_p^n$ be a subspace. Then $V + V = V$, so $|V + V| = |V|$. In fact, if $A \subseteq \mathbb{F}_p^n$ satisfies $|A + A| = |A|$, then A is an affine subspace (a coset of a subspace).

Proof. If $0 \in A$, then $A \subseteq A + A$, so $A = A + A$. General result follows by considering translation of A. $\square$

Example. Let $A \subseteq \mathbb{F}_p^n$ satisfy $|A + A| \leq \frac{3}{2} |A|$. Then there exists a subspace $V \subseteq \mathbb{F}_p^n$ such that $|V| \leq \frac{3}{2} |A|$ and A is contained in a coset of V.

Proof. Exercise (sheet 1). $\square$

Definition. Let $A, B \subseteq G$ be finite subsets of an abelian group G. The **Ruzsa distance** between A and B is

$$d(A, B) := \log \frac{|A - B|}{\sqrt{|A| \cdot |B|}}.$$

2. Fourier-analytic techniques

3. Probabilistic tools

4. Further topics