

# Three proofs of the Cauchy-Davenport Inequality

Following Tao and Vu *Additive Combinatorics*

Trevor Karn

University of Minnesota Student Number Theory Seminar

April 27, 2020

Algebraic proof

Combinatorial proof

Fourier Analytic Proof

# Additive sets

## Definition

- ▶ An *additive set* is a pair  $(A, Z)$  where  $Z$  is a group and  $A \subseteq Z$  is a finite, nonempty subset of  $Z$
- ▶ Given two additive sets  $A, B$  we can define the *sum set*  
 $A + B := \{a + b : a \in A, b \in B\}$

## Example

$A = \{2, 3\}$ ,  $B = \{4\}$ , then  $A + B = \{6, 7\}$

## Nonexample

$A = \{2, 3\}$ ,  $B = 2\mathbb{Z}$ , then  $A + B = \mathbb{Z}$ , but  $B$  not finite.

# Cauchy-Davenport theorem

Theorem (Cauchy, 1813 and Davenport, 1935)

Let  $p$  be a prime, and  $A, B$  are two additive sets in  $\mathbb{Z}/p\mathbb{Z}$ , then

$$|A + B| \geq \min(|A| + |B| - 1, p)$$

# Cauchy-Davenport theorem

## Example 1

Let  $A = \{1, 3, 5, 9\}$ ,  $B = \{2, 3, 4\}$  be additive sets with ambient group  $\mathbb{Z}/11\mathbb{Z}$ .

Then  $A + B = \{3, 4, 5, 6, 7, 8, 9, 0, 1, 2\}$  so

$$|A + B| = 10 \geq \min(6, 11) \quad \checkmark$$

# Cauchy-Davenport theorem

## Example 2

Let  $A = \{1, 3, 5, 7\}$ ,  $B = \{2, 4, 6, 8, 10\}$  in  $\mathbb{Z}/11\mathbb{Z}$ .

Then  $A + B = \{3, 5, 7, 9, 0, 2, 4, 6\}$  so

$$|A + B| = 8 \geq \min(8, 11) \quad \checkmark$$

There are a few things to notice here:

- ▶ Compare to last example:  $|A|$  is the same,  $|B|$  is bigger, but  $|A + B|$  is smaller
- ▶ “Consecutive” numbers in  $A, B$  have common difference of 2.
- ▶ Equality is achieved!

## Arithmetic progression

- ▶ In  $\mathbb{Z}$ , we call sequence with a common difference of consecutive terms an arithmetic progression.
- ▶ In the language of additive sets, if we can write

$$A = a + [0, n) \cdot r = \{a, a + r, a + 2r, \dots, a + nr\}$$

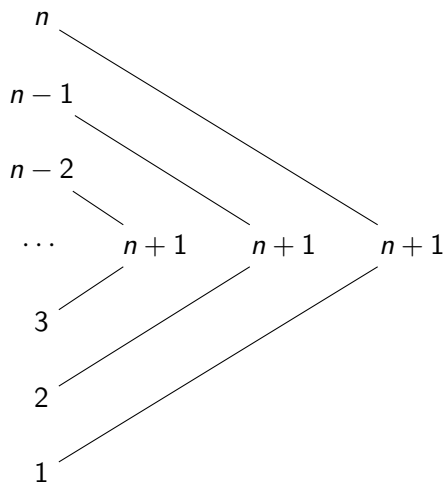
then we call  $A$  an *arithmetic progression*.

- ▶ From last example:  $A = 1 + [0, 4) \cdot 2$
- ▶ A well known formula which makes me smile is

$$\sum_{i=1}^n i = \frac{n(n+1)}{2}$$

because of this proof:

## Arithmetic progression



Each line has a value of  $n+1$ .

When  $n$  is even, add up for each of  $1, 2, \dots, n$ , but that has overcounted by double, so  $\frac{n(n+1)}{2}$ .

When  $n$  is odd, same idea but add up  $n+1$   $(n-1)$ -many times (omitting  $\frac{n+1}{2}$ ) so we get  $\frac{(n+1)(n-1)}{2} + \frac{n+1}{2}$ .



## Arithmetic progression

- ▶ It turns out that there is a similar formula for arithmetic progressions. If  $s_n$  is the  $n$ th partial sum for an arithmetic progression,

$$s_n = \frac{n(a_1 + a_n)}{2}$$

- ▶ Same proof
- ▶  $\{1, 2, \dots, n\} = 1 + [0, n] \cdot 1$  is a special case

# Vosper's theorem

## Theorem

If  $|A|, |B| \geq 2$ ,  $|A + B| \leq p - 2$ , the Cauchy-Davenport theorem achieves equality if and only if  $A, B$  are both arithmetic progressions with a common difference.

## Proof $\emptyset$ of Cauchy-Davenport

- ▶ Augustin Louis Cauchy, 1813
- ▶ As far as I can tell, *Oeuvres complete d'Augustin Cauchy* starts in 1815.

# Proof 1 of Cauchy-Davenport [Dav35, TV10]

## Definition

Let  $A, B$  additive sets,  $e \in A - B$  define  $e$ -transform  $A_{(e)}, B_{(e)}$  as

$$A_{(e)} := A \cup (B + e) \supseteq A$$

$$B_{(e)} := B \cap (A - e) \subseteq B$$

## Example

Let  $A = \{1, 3, 5, 9\}$ ,  $B = \{2, 3, 4\}$ ,  $5 = 9 - 4 \in A - B$

$$A_{(5)} = \{1, 3, 5, 9\} \cup \{7, 8, 9\} = \{1, 3, 5, 7, 8, 9\}$$

$$B_{(5)} = \{2, 3, 4\} \cap \{7, 9, 0, 4\} = \{4\}$$

## Proof 1 of Cauchy-Davenport [Dav35, TV10]

- ▶  $A_{(5)} + B_{(5)} = \{5, 7, 9, 0, 1, 2\} \subseteq A + B$
- ▶  $|A| + |B| = |A_{(5)}| + |B_{(5)}|$ .
- ▶ These are true in general
- ▶ Upshot:  $\epsilon$ -transformation keeps the total size of the two sets the same, while making the sum set weakly smaller.

# Proof 1 of Cauchy-Davenport [Dav35, TV10]

## Lemma

If  $A, B \subseteq Z$  are additive sets,  $n, m \in \mathbb{Z}$  then:

$|A + nB - mB| = |A|$  if and only if there is a subgroup  $G \leq Z$  so that  $B \subseteq h + G$  and  $A$  is a union of cosets of  $G$ .

## Proof.

Construct such a  $G$ .



## Proof 1 of Cauchy-Davenport [Dav35, TV10]

**Idea:** fix  $A$ , see how  $B$  acts on  $A$ . Induct.

Proof.

**Base case:** If  $|B| = 1$ , then  $|A + B| = |A| = |A| + |B| - 1 \leq p$ . ✓

**Induction step:** Suppose we know the claim holds for  $|B'| < |B|$ .

Suppose  $\exists e \in A - B$  so  $|B_{(e)}| < |B|$ . Then

$$\begin{aligned} |A + B| &\geq |A_{(e)} + B_{(e)}| \\ &\geq \min(|A_{(e)}| + |B_{(e)}| - 1, p) \\ &= \min(|A| + |B| - 1, p). \end{aligned}$$

## Proof 1 of Cauchy-Davenport [Dav35, TV10]

Now suppose  $|B_{(e)}| = |B| \forall e$ .

- ▶  $B \cap (A - e) = B$
- ▶  $B \subseteq (A - e) \Leftrightarrow B + e \subseteq A$
- ▶ Adding *anything* in  $A - B$  makes  $B + e \subset A$
- ▶ So adding *everything* yields  $B + (A - B) \subseteq A$
- ▶ By lemma,  $B$  in coset of subgroup of  $\mathbb{Z}/p\mathbb{Z}$ ,  $A$  is union of cosets.
- ▶ Only subgroups of  $\mathbb{Z}/p\mathbb{Z}$  are  $\mathbf{0}$  and itself.

$G = \mathbf{0}$  case:

$|B| = 1$  so back in base case.

$G = \mathbb{Z}/p\mathbb{Z}$  case:

$|A| = p$  so  $A + B = \mathbb{Z}/p\mathbb{Z}$ , so

$|A + B| = p$ .

□



## A few comments

- ▶ This can be phrased nicely because of the  $e$ -transform.  
Davenport's proof required lots of keeping track of indices.
- ▶ This gives insight into why this is true for a cyclic group of *prime* order.

## Warmup question

- ▶ Let  $f$  be a polynomial over a field. Bound the size of the set  $A := \{\alpha : f(\alpha) = 0\}$ .

$$|A| \leq \deg f$$

- ▶ Said another way, if  $|A| > \deg f$ , then  $\exists a \in A$  with  $f(a) \neq 0$
- ▶ Question: can we phrase a set (e.g. a sum set  $A + B$ ) as the zero locus of a polynomial? This is the *polynomial method*.

### Theorem (The combinatorial Nullstellensatz)

Let  $F$  be a field,  $p \in F[t_1, t_2, \dots, t_n]$  a degree- $d$  polynomial which has nonzero coefficient of  $t_1^{d_1} t_2^{d_2} \dots t_n^{d_n}$  where  $d = d_1 + \dots + d_n$ . If  $S_i \subset F$  with  $|S_i| \geq d_i \forall i$ , then there exists a tuple  $\mathbf{x} = (x_1, x_2, \dots, x_n) \in S_1 \times S_2 \times \dots \times S_n$  for which  $p(\mathbf{x}) \neq 0$ .

## Proof 2 of Cauchy-Davenport [TV10]

### Lemma

Let  $h \in \mathbb{F}_p[x, y]$ . Let  $k \geq 0$ , and let  $A, B$  be additive sets in  $\mathbb{F}_p$  with  $|A| + |B| = k + 2 + \deg h$ . If  $(x + y)^k h(x, y)$  has a nonzero coefficient of  $x^{|A|-1}y^{|B|-1}$ , then

$$|\{\alpha + \beta : \alpha \in A, \beta \in B, h(\alpha, \beta) \neq 0\}| \geq k + 1$$

### Proof.

Contradict combinatorial Nullstellensatz. □

## Proof 2 of Cauchy-Davenport [TV10]

Proof.

If  $|A| + |B| > p$ , then  $|A + B| = \mathbb{Z}/p\mathbb{Z}$ . If  $|A| + |B| \leq p$ ,  
Consider the polynomial

$$f = (x + y)^{|A|+|B|-2} = \sum_{n=0}^{|A|+|B|-2} \binom{|A|+|B|-2}{n} x^n y^{|A|+|B|-2-n}.$$

The coefficient of  $x^{|A|-1}y^{|B|-1}$  is  $\binom{|A|+|B|-2}{|A|-1}$ . Since  $|A| + |B| \leq p$ ,  
no factors of  $p$  appear in the binomial coefficient, so it is nonzero.  
Previous lemma with  $h = 1$  tells us that

$$|\{\alpha + \beta : \alpha \in A, \beta \in B, h(\alpha, \beta) \neq 0\}| \geq |A| + |B| - 1$$

But since  $h \neq 0$  always,

$$\{\alpha + \beta : \alpha \in A, \beta \in B, h(\alpha, \beta) \neq 0\} = A + B.$$



## So what?

Define a *restricted sum set*  $A \hat{+} B = \{a + b : a \in A, b \in B, a \neq b\}$

Conjecture (Erdos, Heilbronn 1964)

$$|A \hat{+} A| \geq \min(2|A| - 3, p)$$

- ▶ Proved 1994 by da Silva, Hamidoune.
- ▶ Stronger result for  $A \hat{+} B$  proved in 1996 by Alon, Nathanson, Ruzsa

Proof.

Take  $h = (x - y)$ , and apply lemma. □

Similar technique can be used to give results in particle physics.

# Probabilistic method

## Philosophy

If you can prove something has the right probability in an appropriate space, that can be interpreted as proof.

## Example

Assign  $n$  balls to  $m$  bins at (uniform) random. Let  $P$  be the probability that any of the bins contain two or more balls. If  $P = 1$ , this is the pigeonhole principle.

## Example

Existence proof: If I can draw something at random with nonzero probability, it must exist.

## Usage

Fourier analysis can be framed as statements about probability and expectation.

## Fourier analysis definitions

- ▶ Let  $p$  be a prime,  $f, g : \mathbb{Z}/p\mathbb{Z} \rightarrow \mathbb{C}$
- ▶  $\hat{f}(\xi) = \frac{1}{p} \sum_{x \in \mathbb{Z}/p\mathbb{Z}} f(x) e^{-2\pi i x \xi / p}$
- ▶  $(f * g)(\xi) = \frac{1}{p} \sum_{x \in \mathbb{Z}/p\mathbb{Z}} f(x - \xi) g(\xi) = \frac{1}{p} \sum_{x \in \mathbb{Z}/p\mathbb{Z}} f(\xi) g(x - \xi)$
- ▶  $\text{supp } f = \{x \in \mathbb{Z}/p\mathbb{Z} : f(x) \neq 0\}$

### Upshots

- ▶  $\text{supp}(f * g) \subseteq \text{supp}(f) + \text{supp}(g)$  as an additive set.
- ▶  $\widehat{f * g} = \hat{f} \cdot \hat{g}$  (among other standard identities)

# Fourier analysis theorems

## Theorem (Tao, '05)

Let  $p$  be a prime,  $f : \mathbb{Z}/p\mathbb{Z} \rightarrow \mathbb{C}$  a random variable. Then  $|\text{supp } f| + |\text{supp } \hat{f}| \geq p + 1$ .

## Theorem (Tao, '05)

Let  $A, B$ , be nonempty subsets of  $\mathbb{Z}/p\mathbb{Z}$  with  $|A| + |B| \geq p + 1$ . Then  $\exists$  a function  $f : \mathbb{Z}/p\mathbb{Z} \rightarrow \mathbb{C}$  such that  $\text{supp } f = A$  and  $\text{supp } \hat{f} = B$ .

Proofs are not enlightening, so omitted.



## Proof 3 of Cauchy-Davenport [TV10]

Let  $A, B$  be additive sets in  $\mathbb{Z}/p\mathbb{Z}$ . We can choose sets  $X, Y$  so that

- ▶  $|X| = p + 1 - |A|$
- ▶  $|Y| = p + 1 - |B|$
- ▶  $|X \cap Y| = \max(|X| + |Y| - p, 1)$ .

### Example

Let  $A = \{1, 3, 5, 9\}$ ,  $B = \{2, 3, 4\} \subseteq \mathbb{Z}/11\mathbb{Z}$  so we want  $|X| = 8$  and  $|Y| = 9$ , and  $|X \cap Y| = 6$

$$X = \boxed{0, 1, 2, 3, 4, 5}, \boxed{6, 7}, \cancel{8}, \cancel{9}, \cancel{10}$$

$$Y = \boxed{0, 1, 2, 3, 4, 5}, \cancel{6}, \cancel{7}, \boxed{8, 9, 10}$$

The point is that the only data from  $A$  and  $B$  which we retain is their size.

## Proof 3 of Cauchy-Davenport [TV10]

By previous theorem, since  $|A| + |X| = p + 1$ , there is:

- ▶ A function  $f$  with  $\text{supp } f = A$  and  $\text{supp } \hat{f} = X$ .
- ▶  $g$  with  $\text{supp } g = B$  and  $\text{supp } \hat{g} = Y$ .

Now convolve  $f * g$ . We know

- ▶  $\text{supp}(f * g) \subseteq \text{supp } f + \text{supp } g = A + B$
- ▶  $\text{supp}(\widehat{f * g}) = \text{supp}(\hat{f} \cdot \hat{g}) = X \cap Y$

Then

$$\begin{aligned} |\text{supp}(f * g)| + |\text{supp}(\widehat{f * g})| &\geq p + 1 \\ |A + B| + |X \cap Y| &\geq p + 1 \\ |A + B| &\geq p + 1 - \max(|X| + |Y| - p, 1) \\ &= p + 1 - \max(p + 2 - |A| - |B|, 1) \\ &= \min(|A| + |B| - 1, p) \end{aligned}$$

□




# Poll

Which was your favorite?

1. Original proof exploiting (sub)group structure of  $\mathbb{Z}/p\mathbb{Z}$ ?
2. Proof counting the zeros of a certain polynomial?
3. **Exploiting the relationship between a Fourier transform and its convolution?**

Thank you!

# References

-  H. Davenport, *On the addition of residue classes*, Journal of the London Mathematical Society **s1-10** (1935), no. 1, 30–32.
-  Ben Green, *Additive combinatorics [book review of mr2289012]*, Bull. Amer. Math. Soc. (N.S.) **46** (2009), no. 3, 489–497. MR 2507281
-  Terence Tao and Van H. Vu, *Additive combinatorics*, Cambridge Studies in Advanced Mathematics, vol. 105, Cambridge University Press, Cambridge, 2010, Paperback edition [of MR2289012]. MR 2573797