Hello to Additive Combinatorics

V. V. Phuc

Arithmetic Progressions

Definition

A k-**term arithmetic progression** (AP) is a set

$$\{a,\ a+d,\ a+2d,\ \ldots,\ a+(k-1)d\}, \quad d \neq 0.$$

Examples

- $\{2,5,8,11\}$ $\quad d=3$
- $\{5,11,17,23,29\}$ $\quad d=6$
- $\{2,4,6,\ldots,2n\}$ $\quad d=2$

Key fact

$$|A+A| = 2n-1$$

(smallest possible sumset)

APs are the most structured sets under addition.

Van der Waerden's Theorem

Theorem (Van der Waerden, 1927)

For every $r, k \geq 1$, there exists $W(r, k) < \infty$ such that:

any r-coloring of $\{1, 2, \ldots, W(r, k)\}$ contains a **monochromatic** k-term AP.

Small values

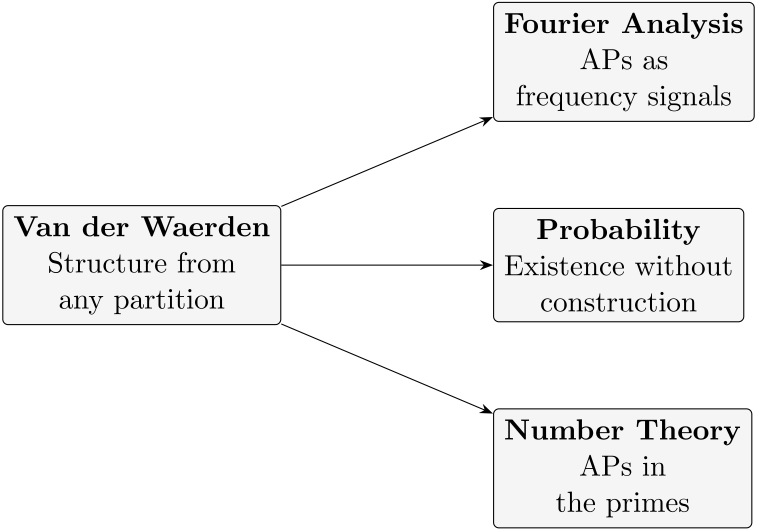
- $W(2, 3) = 9$
- $W(2, 4) = 35$
- $W(2, 5) = 178$
- $W(2, 6) = 1132$
- $W(2, 7) = ?$

What this says

- No coloring avoids APs forever
- Structure *emerges* from any partition
- Existence without explicit construction

Complete disorder is impossible

Structure, Randomness, and Three Bridges



Each bridge becomes a major branch of additive combinatorics.

The Probabilistic Method

Core idea (Erdős, 1947)

If a *random* object satisfies a property with positive probability,
then a concrete object with that property **must exist**.

First moment method

If $\mathbb{E}[Z] < 1$, then $\mathbb{P}[Z = 0] > 0$.

Application

Take $A_p \subseteq \{1, \ldots, N\}$, $p = N^{-2/3}$.
Expected # of 3-APs $\to 0$.

$\to$ Large AP-free sets exist

Why it matters

- Explicit constructions are hard
- Randomness has no algebraic bias
- Erdős: $R(k, k) > 2^{k/2}$ no explicit construction matches this today

Sumsets and Small Doubling

Sumset

$A + B \coloneqq \{a + b : a \in A,\, b \in B\}$ with trivial bounds
$|A| + |B| - 1 \leq |A + B| \leq |A| \cdot |B|$

Doubling constant

$K[A] \coloneqq |A + A| \,/\, |A|$. **Small doubling**: $K[A] = O(1)$.

Arithmetic progression

$|A+A| = 2|A|-1 \implies K[A] \approx 2$

Most structured.

Generic set

$|A+A| \approx |A|^2 \implies K[A] \approx |A|$

Least structured.

Small doubling $\iff$ set resembles a generalized AP.

Cauchy–Davenport and Vosper

Theorem (Cauchy–Davenport)

For prime p and $A, B \subseteq \mathbb{Z}/p\mathbb{Z}$ nonempty,

$$|A+B| \;\geq\; \min\bigl(p,\; |A|+|B|-1\bigr).$$

The trivial lower bound is always achieved or beaten.

Theorem (Vosper, 1956)

If $|A+B| = |A|+|B|-1$ with $|A|, |B| \geq 2$ and $|A|+|B| \leq p$,

then A and B are **both APs with the same common difference**.

Ruzsa Distance and Freiman's Theorem

Ruzsa distance

$$d(A,B) \;\coloneqq\; \log \frac{|A-B|}{\sqrt{|A|\,|B|}} \qquad \text{satisfies } d(A,C) \le d(A,B) + d(B,C)$$

Plünnecke–Ruzsa inequalities

If $|A+B| \le K|A|$, then $|mB - nB| \le K^{m+n}|A|$ for all $m,n \ge 0$.

Small doubling does not explode under iteration.

Theorem (Freiman)

$|A+A| \le K|A| \implies A$ is contained in a **generalized AP**

Fourier Analysis on Finite Groups

Fourier transform on $\mathbb{Z}/N\mathbb{Z}$

$$\hat{f}(\xi) \;=\; \sum_{x\in\mathbb{Z}/N\mathbb{Z}} f(x)\, e^{-2\pi i\xi x/N} \qquad \widehat{f*g}(\xi) = \hat{f}(\xi)\,\hat{g}(\xi)$$

Key identities

Parseval:

$$\sum_x |f|^2 = \frac{1}{N}\sum_\xi |\hat{f}|^2$$

Additive energy:

Why it works for APs

Counting 3-APs in A:

$$T(A) = \sum_{x,d} \mathbf{1}_A(x)\mathbf{1}_A(x+d)\mathbf{1}_A(x+$$

rewrites as a Fourier sum.

Roth's Theorem and Density Increment

Theorem (Roth, 1953)

Any $A \subseteq \{1, \ldots, N\}$ with $|A| \geq cN/\log\log N$ contains a 3-term AP.

Density increment argument:

1. Write $\mathbf{1}_A = \alpha + f, \quad \hat{f}(0) = 0$.
2. $T(A) = \alpha^3 N^2 +$ (error in $\hat{f}$).
3. No AP $\Rightarrow$ error dominates $\Rightarrow |\hat{A}(\xi)| \geq c\alpha^2 N$ for some $\xi \neq 0$.
4. Large coefficient $\Rightarrow$ A is **denser** on a subprogression.
5. Iterate until a 3-AP is forced.

Kelley–Meka (2023): $r_3(N) \leq N \exp\bigl(-c(\log N)^{1/9}\bigr)$

Modern Developments and Open Problems

Theorem (Szemerédi, 1975)

Every positive-density subset of $\{1, \ldots, N\}$ contains a k-term AP for *any* fixed k.

Theorem (Green–Tao, 2008)

The primes contain arithmetic progressions of arbitrary length.
Key tools: pseudorandom majorants, Gowers uniformity norms.

Erdős–Turán Conjecture (1936) ***Open***

$$\sum_{a \in A} \frac{1}{a} = \infty \quad \Longrightarrow \quad A \text{ contains APs of every length.}$$

Thank you.

V. V. Phuc