Combinatorics and Analytical Number theory

Éric Balandraud

May 2016
Spring School in Analytical Number Theory

Contents

Introduction

Theorem (Lagrange)**.** *For any integer $n \in \mathbb{N}$, there are $(a, b, c, d) \in \mathbb{N}^4$, such that:*

$$n = a^2 + b^2 + c^2 + d^2.$$

It has been conjectured by Waring that for any power k, there exists an integer (denote $g(k)$ the minimal one), such that all integers can be written as a sum of $g(k)$ k-th powers. This has been proved by Hilbert. Lagrange theorem asserts that $g(2) = 4$, few values are known.

Conjecture (Goldbach)**.** *For any even integer greater or equal to* 4*, $n \in 2.(\mathbb{N} \setminus \{0, 1\}$, there are two prime numbers $(p, q) \in \mathbb{P}^2$, such that:*

$$n = p + q.$$

These two problems deal with sums whose terms are multiplicatively defined. Additive number theory would consider any set of terms (forget about the multiplicative definition of these particular problems) and try to prove that if the set is large enough, then so will be the sets of sums, up to a point where it can cover all the integers. This is the idea of the definition of an additive base.

Let A and B be two non-empty subsets of $\mathbb{Z}$, $\mathbb{Z}/p\mathbb{Z}$ or any abelian group, we define their sumset $A+B = \{a+b \mid a \in A,\ b \in B\}$. One want to find conditions to ensure that the sumset will be "big" enough in comparison to A and B.

Goldbach's conjecture can be restated in the following way

$$2.(\mathbb{N} \setminus \{0, 1\}) = \mathbb{P} + \mathbb{P}.$$

And Lagrange theorem:

$$\mathbb{N} = \square + \square + \square + \square.$$

Additive combinatorics would consider similar questions and developments on the integers, residues modulo a prime or any abelian group. In this course, we will restrain ourselves to the finite case.

The interested reader may appreciate the following references and the references therein:

- "Additive Number Theory, Inverse problems and the Geometry of Sumsets", M.B. Nathanson, GTM **165**, Springer-Verlag (1996).

- "Additive Combinatorics", T. Tao and V.H. Vu, Cambridge Studies in advanced mathematics **105**, Cambridge University Press.

I

Small sumsets in $\mathbb{Z}$ and $\mathbb{Z}/p\mathbb{Z}$

I.1 Sets of Integers

In the integers, one has an easy lower bound on the cardinality of the sumset of two finite sets and a caracterisation of the critical cases.

Theorem 1. *Let A and B be two non-empty subsets of $\mathbb{Z}$, then:*

$$|A + B| \geq |A| + |B| - 1.$$

One has equality if and only if

- *either* $\min\{|A|, |B|\} = 1$,
- *or A and B are arithmetical progressions with same difference.*

Proof. Denote $A = \{a_1 < a_2 < \cdots < a_d\}$ and $B = \{b_1 < b_2 < \cdots < b_\ell\}$ then in the table:

$$\begin{array}{|ccc||c||}
\hline
a_1 + b_1 & a_2 + b_1 & \ldots & a_d + b_1 \\
\hline
\hline
a_1 + b_2 & a_2 + b_2 & \ldots & a_d + b_2 \\
\vdots & \vdots & & \vdots \\
a_1 + b_\ell & a_2 + b_\ell & \ldots & a_d + b_\ell \\
\hline
\end{array}$$

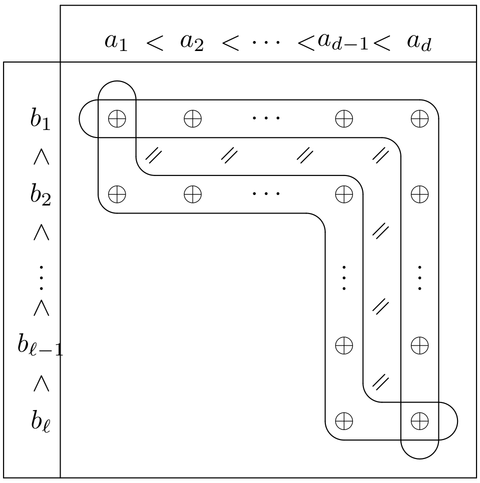
One has a increasing sequence of length $d + \ell - 1$ ($d + \ell - 2$ strict inequalities):

$$a_1 + b_1 < a_2 + b_1 < \cdots < a_d + b_1 < a_d + b_2 < \cdots < a_d + b_\ell.$$

So $A + B$ has cardinality at least $|A| + |B| - 1$.

In the case of equality, it suffices to consider the second line and one before last column of this table to have another increasing sequence of length $d + \ell - 1$:

$$\begin{array}{cccccccc}
a_1 + b_1 < & a_2 + b_1 < & \cdots < & a_d + b_1 < & a_d + b_2 < & \cdots < & a_d + b_{\ell-1} < & a_d + b_\ell \\
a_1 + b_1 < & a_1 + b_2 < & \cdots < & a_{d-1} + b_2 < & a_{d-1} + b_3 < & \cdots < & a_{d-1} + b_\ell < & a_d + b_\ell
\end{array}$$



So these sequences are termwise equal. The second to d-th equalities are:

$$a_i - a_{i-1} = b_2 - b_1,\ i \in [2, d].$$

This proves that A is an arithmetical progressions with difference $b_2 - b_1$. And the d-th to the one before the last equalities are:

$$a_d - a_{d-1} = b_j - b_{j-1},\ j \in [2, \ell].$$

This proves that B is an arithmetical progression with difference $a_k - a_{k-1}$. So, A and B are arithmetical progressions with same difference. □

I.2 In $\mathbb{Z}/p\mathbb{Z}$

In the groups $\mathbb{Z}/p\mathbb{Z}$, where p is a prime number, the additive results are very similar, even if the group is finite. These groups share with $\mathbb{Z}^d$ the property to have no proper non-trivial finite subgroups.

Since there is no order relation compatible with the addition, one needs new tools to produce addition results.

I.2.1 The Dyson e-transform

Definition of the Dyson e-transform: Consider two sets A and B of an abelian group G, and $e \in G$, one considers:

$$\begin{aligned} A(e) =& A \cup (B + e) \\ B(e) =& B \cap (A - e). \end{aligned}$$

One has $A(e) + B(e) \subset A + B$ and $|A(e)| + |B(e)| = |A| + |B|$. Indeed:

$$\begin{aligned} |A| + |B| =& |A| + |B + e| \\ =& |A \cup (B + e)| + |A \cap (B + e)| \\ =& |A \cup (B + e)| + |(A - e) \cap B| \\ =& |A(e)| + |B(e)|. \end{aligned}$$

Moreover, if $e \in A - B$ then $B(e) \neq \emptyset$.

I.2.2 Cauchy-Davenport Theorem

Theorem 2 (Cauchy-Davenport)**.** *Let p be a prime number, A and B be two non-empty subsets of $\mathbb{Z}/p\mathbb{Z}$, then:*

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

Proof. If $|A|+|B| > p$, whatever $x \in \mathbb{Z}/p\mathbb{Z}$, the two sets $(x - A)$ and B have by the pigeonhole principle a common element and so $x \in A+B$ and $A+B = \mathbb{Z}/p\mathbb{Z}$.

Otherwise $|A| + |B| - 1 < p$, so $\min\{p, |A| + |B| - 1\} = |A| + |B| - 1$. The result is clear whenever $\min\{|A|, |B|\} = 1$. Consider a counter-example case (A, B), with $\min\{|A|, |B|\} \geq 2$, and $|B|$ minimal.

Consider $b_1 \neq b_2$ both in B and $a \in A$ such that $a - b_1 \notin A - b_2$. (Since $b_1 - b_2$ has additive order p, such an a exists.) Consider $e = a - b_1$, so $b_1 \in B(e)$ and $b_2 \notin B(e)$, otherwise there would be $a' \in A$ such that $b_2 = a' - e$ what implies that $a - b_1 = a' - b_2$.

Since,

$$|A(e) + B(e)| \leq |A + B| < |A| + |B| - 1 = |A(e)| + |B(e)| - 1,$$

then $(A(e), B(e))$ is another counter-example with $0 < |B(e)| < |B|$ a contradiction. □

This theorem can be easily generalize by induction on the number of sets to the following:

Theorem 3 (Cauchy-Davenport)**.** *Let A_i be a finite non-empty subset of $\mathbb{Z}/p\mathbb{Z}$ for $i \in [1, n]$:*

$$|A_1 + \cdots + A_n| \geq \min\left\{p, \sum_{i=1}^{n}(|A_i| - 1) + 1\right\}.$$

I.2.3 Applications and Critical cases

A direct application of Cauchy-Davenport theorem give a first property in the flavour of Waring's conjecture:

Theorem 4. *Let p be a prime number, and k a divisor of $p - 1$, then any $x \in \mathbb{Z}/p\mathbb{Z}$ is the sum of k k-th powers.*

Proof. Let P_k be the set of k-th powers in $\mathbb{Z}/p\mathbb{Z}$, one has $|P_k| = 1+\frac{p-1}{k}$. Adding P_k to itself k times, one get using the generalization of Cauchy-Davenport theorem:

$$|\underbrace{P_k + \cdots + P_k}_{k \text{ times}}| \geq \min\left\{p, k\left(\frac{p-1}{k}\right)+1\right\} = p.$$

□

This last result can easily be extend without the divisibility condition, notice that whenever $\gcd(k, p-1) = 1$, the multiplicative morphism $x \mapsto x^k$ is injective and every element in $\mathbb{Z}/p\mathbb{Z}$ is a k-th power.

The critical case of Cauchy-Davenport theorem does, as in the integers, contain the obvious examples where $|A| = 1$ or $|B| = 1$, but also the example, where $|A+B| = p-1$, indeed: If $A+B = \mathbb{Z}/p\mathbb{Z} \setminus \{x\}$, then the set $x - A$ and B are disjoint, (it would contradict $x \notin A+B$), and $|A|+|B| = |A+B|+1 = (p-1)+1 = p$, so necessarily $B = \mathbb{Z}/p\mathbb{Z} \setminus A$. This holds whatever is the set A.

Theorem 5 (Vosper)**.** *Let p be a prime number, A and B be two subsets of $\mathbb{Z}/p\mathbb{Z}$ such that* $\min\{|A|, |B|, |\mathbb{Z}/p\mathbb{Z} \setminus (A+B)|\} \geq 2$*, if*

$$|A+B| = |A|+|B|-1,$$

then A and B are arithmetical progressions with same difference.

The proof is similar in nature but more involved to the Cauchy-Davenport proof.

An interesting application of these two theorems is the following:

Proving that, whenever $k \mid p-1$ and $1 < k < \frac{p-1}{2}$, the set of k-th powers is not an arithmetic progression, Then its consecutive sumsets have to be even greater than what Cauchy-Davenport asserts. So one can prove the following:

Theorem 6 (Chowla-Mann-Straus)**.** *Let p be a prime number, if $k < \frac{p-1}{2}$, then every element of $\mathbb{Z}/p\mathbb{Z}$ can be written as a sum of $\left\lceil \frac{k+1}{2} \right\rceil$ k-th powers.*

There are analytic results that give far better bound, but the proof are much more involved.

II

Sumsets in abelian groups - Introduction to the isoperimetric method

II.1 Subgroups give small sumsets

As a sumset can be defined on any group, one can consider the same problems in a general abelian group. Working in a finite group, naturally the size of any sumset will be bounded by the above by the size of the group, and no lower bound can exceed its cardinality.

Lemma 1 (Prehistorical Lemma)**.** *Let $(G, +)$ be a finite group (non necessarily abelian), A and B be two non-empty subsets of G, if $|A| + |B| > |G|$ then $A + B = G$.*

Proof. Let $x \in G$, then the two sets $x - B$ and A have, by the pigeonhole principle, a common element. So there are $a \in A$ and $b \in B$ such that $x - b = a$, which gives $x = a + b \in A + B$. Since this holds for any $x \in G$, we have $G = A + B$. □

In any group, another kind of structure, the finite subgroups, will enable very small sumsets. Indeed:

Exercise 1. *Let A be a non-empty finite subset of any group $(G, +)$ (non necessarily abelian), one has*

$$|A + A| = |A|$$

if and only if A is a coset of a finite subgroup of G.

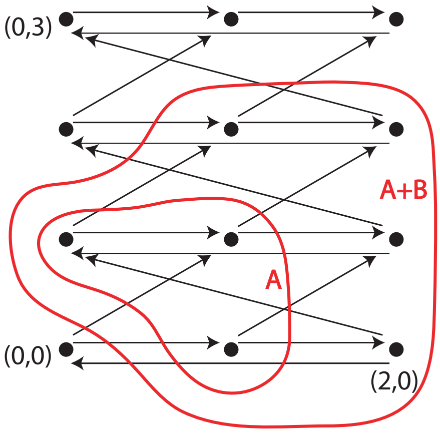
II.2 Introduction to the Isoperimetric Method

Let G be an abelian group. Consider one finite subset $B \subset G$, such that $0 \in B$. We define the perimeter function:

$$\partial \left| \begin{array}{rcl} \mathcal{P}_f(G) & \to & \mathcal{P}_f(G) \\ X & \mapsto & (X + B) \setminus X \end{array} \right.$$

where $\mathcal{P}_f(G)$ is the set of finite subsets of G and denote $D(X) = G\setminus(X+B)$ (that can be finite or not). Notice that a finite set X will have a small perimeter if and only if it makes a small sumset with B. The intuition relies on the notion of Cayley graphs, The Cayley graph associate to the pair (G, B) is the directed graph (digraph), whose set of vertices is G and the set of edges is $E = \{(x, x+b) \mid x \in G,\ b \in B\}$.

Example: $G = \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z},\ B = \{(0,0),(0,1),(1,1)\}$



One defines:

- The connectivity:

$$\kappa = \min\{|\partial X| \mid X \neq \emptyset,\ D(X) \neq \emptyset\}.$$

- A fragment is a set X, such that $X \neq \emptyset$, $D(X) \neq \emptyset$ and $|\partial X| = \kappa(B)$.
- An atom is a fragment X of minimal cardinality denoted $|X| = \alpha(B)$.

One will prove a structural result on atoms and fragments.
These objets do have a symmetry property:
Since G is abelian:

$$|(X+B)\setminus X| = |((-X)+(-B))\setminus(-X)|$$

and so one has $\kappa(-B) = \kappa(B)$ and subsequently $\alpha(-B) = \alpha(B)$.

Whenever G is finite, these objets do also have a duality property: Since $(D(X)-B)\setminus D(X) \subset (X+B)\setminus X$ and $\kappa(B) = \kappa(-B)$ then $(D(X)-B)\setminus D(X) = (X+B)\setminus X$ and the dual of a fragment for B is also a fragment for $-B$.

This allows us to prove the lemma:

Lemma 2. *Let A and F be respectively an atom and a fragment, then either $A \subset F$ or $A \cap F = \emptyset$.*

Proof. Suppose that $A \cap F \neq \emptyset$.

One consider the crossed partition of the two partitions of G: $\{A, \partial A, D(A)\}$ and $\{F, \partial F, D(F)\}$

$\cap$	F	∂F	$D(F)$
A	R_{11}	R_{12}	R_{13}
∂A	R_{21}	R_{22}	R_{23}
$D(A)$	R_{31}	R_{32}	R_{33}

Since R_{11} is not empty and that $\emptyset \neq D(A) \subset D(R_{11})$, then $|\partial R_{11}| \geq \kappa(B)$. Notice that in this crossed partition, all part are finite except possibly R_{33}.

- If G is infinite, then $A \cup F \neq \emptyset$ and $D(A \cup F) \neq \emptyset$ because it is infinite, so one also have:

$$|\partial(A \cup F)| = |R_{32} \cup R_{22} \cup R_{23}| \geq \kappa(B).$$

- If G is finite, since one has $\partial R_{11} \subset R_{21} \cup R_{22} \cup R_{12}$ and $\kappa(B) = |R_{21}| \cup |R_{22}| \cup |R_{23}|$, therefore $|R_{12}| \geq |R_{23}|$.

  This can be extend to $|R_{12} \cup R_{13}| \geq |R_{23} \cup R_{13}|$, or $|A \backslash F| \geq |D(F) \backslash D(A)|$. This leads to

$$|D(A \cup F)| = |R_{33}| = |D(F) \cap D(A)| \geq |D(F)| - |D(F) \backslash D(A)| \geq \alpha(B) - |A \backslash F| \geq |A \cap F| \neq 0.$$

  Therefore one also has $|\partial(A \cup F)| \geq \kappa(B)$.

Moreover, one has:

$$|\partial(A \cup F)| + |\partial(A \cap F)| \leq |R_{12}| + |R_{21}| + |R_{32}| + |R_{23}| + 2|R_{22}| = |\partial A| + |\partial F| = 2\kappa(B),$$

and both terms are bigger than $\kappa(B)$ then $|\partial(A \cap F)| = \kappa(B)$, what implies by minimality of the cardinal of an atom that $A \cap F = A$.

□

Proposition 1. *Let A be an atom that contain 0, then A is a finite subgroup of G.*

Proof. Whatever $a \in A$, the two atoms A and $a + A$ contain both a, so they included one in the other, so $a + A = A$. Since A is finite and $A + A = A$, this implies that A is a finite subgroup of G. □

II.3 Addition Theorems in Groups

Theorem 7 (Mann)**.** *Let G be an abelian group. Let A and B be two non-empty finite subsets of G such that $A + B \neq G$. Then there exists a finite proper subgroup H of G, such that:*

$$|A + B| \geq |A| + |B + H| - |H|.$$

Proof. It suffices to consider the atom of (G, B). □

In the particular case of cyclic groups, one deduce:

Theorem 8 (Chowla)**.** *Let $n \in \mathbb{N} \setminus \{0,1\}$, A and B be two non-empty subsets of $\mathbb{Z}/n\mathbb{Z}$, such that $0 \in B$ and $B \setminus \{0\} \subset (\mathbb{Z}/n\mathbb{Z})^\times$ then:*

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

Proof. If $|A|+|B| > n$, whatever $x \in \mathbb{Z}/n\mathbb{Z}$, the two sets $(x-A)$ and B have by the pigeonhole principle a common element and so $x \in A+B$ and $A+B = \mathbb{Z}/n\mathbb{Z}$.

Otherwise $|A|+|B|-1 < n$, so $\min\{n, |A|+|B|-1\} = |A|+|B|-1$. Suppose $A+B \neq \mathbb{Z}/n\mathbb{Z}$. Applying Mann's Theorem (or considering the atom of (G,B)), there is a proper subgroup such that:

$$|A| + |B+H| - |H| \leq |A+B|.$$

But whatever is the proper subgroup H, the condition on B implies that $H \cap B = \{0\}$, and consequently $|B+H|-|H| \geq |B|-1$, so $|A+B| \geq |A|+|B|-1$. □

An application of this last theorem is:

Exercise 2. *Let n be an odd integer, consider for some $\ell \in \mathbb{N}^*$, the sets of sequences $(a_1, \ldots, a_\ell) \in (\mathbb{Z}/n\mathbb{Z})^*$. Prove that for any of these sequences, any $x \in \mathbb{Z}/n\mathbb{Z}$ admits a writing of the type:*

$$x = \pm a_1 \pm a_2 \cdots \pm a_\ell,$$

if and only if $\ell \geq n-1$.

Proof. For $\ell = n-1$, consider any sequence $(a_1, \ldots, a_{n-1})$, define $c = a_1 + \cdots + a_{n-1}$, then one has:

$$\sum_{i=1}^{n-1} \{0, 2a_i\} = x + \left\{ \sum_{i=1}^{n-1} \epsilon_i a_i \mid \epsilon_i \in \{\pm 1\} \right\}.$$

Since both 2 and a_i are invertible modulo n, all the sets $\{0, 2a_i\}$ do satisfy Chowla's theorem condition. By induction, one has:

$$\left| \sum_{i=1}^{n-1} \{0, 2a_i\} \right| \geq \min\left\{ n, \sum_{i=1}^{n-1} (2-1) + 1 \right\} = n.$$

And the signed sums do cover all the elements of $\mathbb{Z}/n\mathbb{Z}$.

For $\ell = n-2$, consider the particular sequence $(a_1, \ldots, a_{n-2}) = (1, \ldots, 1)$.

All the sums $\pm 1 \cdots \pm 1$ covers the set $\pm\{1, 3, \ldots, n-2\} = \mathbb{Z}/n\mathbb{Z} \setminus \{0\}$.

So the minimal value for ℓ is $n-1$. □

To describe a deeper result, we will need the following notion:

For a given set $X \subset G$, one defines its period:

$$H(X) = \{g \in G \mid g + X = X\},$$

it is a simple exercise to show that, $H(X)$ is a subgroup of G (finite if X is finite).

Theorem 9 (Kneser)**.** *Let A and B be two non-empty finite subsets of an abelian group $(G, +)$, one has:*

$$|A + B| \geq |A + H| + |B + H| - |H|,$$

where $H = H(A + B)$ is the period of $A + B$.

Theorem 10 (Kneser)**.** *Let A and B be two non-empty finite subsets of an abelian group $(G, +)$, if $|A + B| < |A| + |B| - 1$ then:*

$$|A + B| = |A + H| + |B + H| - |H|,$$

where $H = H(A + B)$ is the period of $A + B$.

One can explain the equivalence between these two formulations.

Proof. 9 $\implies$ 10: Suppose that $|A + B| < |A| + |B| - 1$, then one has:

$$|A + H| + |B + H| - |H| \leq |A + B| < |A| + |B| - 1 < |A + H| + |B + H|.$$

In this chain of inequality, the two extremities are consecutive multiples of $|H|$. Moreover since $A + B$ is a union of coset modulo H, its cardinality is a multiple of $|H|$, so necessarily $|A + B| = |A + H| + |B + H| - |H|$.

10 $\implies$ 9: Suppose that $|A + B| < |A + H| + |B + H| - |H|$, then one would have in the quotient G/H: $|\overline{A} + \overline{B}| < |\overline{A}| + |\overline{B}| - 1$ and in this quotient the period of $\overline{A} + \overline{B}$ is reduced to $\{\overline{0}\}$, then Theorem 10 gives the contradiction

$$|\overline{A}| + |\overline{B}| - 1 = |\overline{A} + \overline{B}| < |\overline{A}| + |\overline{B} - 1.$$

□

III

Larger small sumsets in the integers

From this result, that holds in the general context of any abelian group, one can go back in the integers and extend the first theorem of this course (the critical case of Theorem 1).

Theorem 11 ($(3k-4)$-Freiman)**.** *Let A be a finite non-empty subset of $\mathbb{Z}$, if*

$$|A+A| \leq 3|A| - 4$$

then A is contained in an arithmetical progression of length at most $|A+A| - |A| + 1$.

Proof. Up to dilatation and translation, one can consider that $\gcd(A) = 1$, $\min(A) = 0$. Denote $m = \max(A)$.

One considers $\overline{A} \subset \mathbb{Z}/m\mathbb{Z}$, its cardinality is $|\overline{A}| = |A| - 1$.

The sumset $\overline{A} + \overline{A}$ is the image of $A + A$. Since 0, m and $m + m$ are equal modulo m, and $0 + a$ and $m + a$ are equal modulo m for $a \in A \setminus \{0, m\}$, one has: $|\overline{A} + \overline{A}| \leq |A + A| - ((|A| - 2) + 2) = |A + A| - |A| \leq 2|A| - 4 = 2|\overline{A}| - 2$.

From Kneser's theorem, one deduce that $\overline{A} + \overline{A}$ is periodic, with an non-trivial period $H = d\mathbb{Z}/m\mathbb{Z} < \mathbb{Z}/m\mathbb{Z}$, with $d \mid m$. and that:

$$|\overline{A} + \overline{A}| = 2|\overline{A} + H| - |H|.$$

- If $\overline{A} + \overline{A} = \mathbb{Z}/m\mathbb{Z}$, then $m \leq |A + A| - |A|$, what implies that $m + 1 \leq |A + A| - |A| + 1$. And A is included in the arithmetical progression $[0, m]$.
- If $\overline{A} + \overline{A} \neq \mathbb{Z}/m\mathbb{Z}$, denote d, the divisor of m such that $H = d\,(\mathbb{Z}/m\mathbb{Z})$ is the period of $\overline{A}+\overline{A}$. In this case, one have $d \underset{\neq}{\mid} m$ and therefore, A intersects H and at least another classe modulo H since otherwise all the elements of A would be multiples of $\frac{m}{d}$, which is impossible because $\gcd(A) = 1$.

  Consider that A intersect $1 + u$ classes modulo H, with $u \geq 1$. Denote $\overline{A}_0 = \overline{A} \cap H$, and $\overline{A}_1, \ldots, \overline{A}_u$ the other classes, with $|\overline{A_u}|$ minimal. These classes are almost full, indeed $2|\overline{A}+H| - |H| < 2|\overline{A}| - 1$, therefore $|\overline{A}+H| -$

$|\overline{A}| < \frac{1}{2}(|H|-1)$ and whatever is the class $\overline{A_i}$, one has $|\overline{A}_i + H| - |\overline{A}_i| < \frac{1}{2}(|H|-1)$. Consider now the sets of integers A_i of all the elements in A whose images are in $\overline{A}_i$. The only cardinal difference is $|A_0| = |\overline{A_0}| + 1$. Since $|\overline{A} + \overline{A}| = 2|\overline{A} + H| - |H| = 2(u+1)|H| - |H| = (2u+1)|H|$ counts at least $2u+1$ classes, lets us denote $\overline{A_{\alpha(i)}} + \overline{A_{\beta(i)}}$ for $i \in [1,u]$, u classes in $(\overline{A} + \overline{A}) \setminus \overline{A}$.

Since the classes are disjoint, the above sets are disjoint and we have:

$$|A + A| \geq \sum_{i=0}^{u} |A_0 + A_i| + \sum_{i=1}^{u} |A_{\alpha(i)} + A_{\beta(i)}|$$

One isolate the first term of the first sum and the u-th term of both sums:

$$\begin{aligned}
\geq & |A_0 + A_0| + \left(\sum_{i=1}^{u-1} |A_0 + A_i| \right) + |A_0 + A_u| \\
& + \left(\sum_{i=1}^{u-1} |A_{\alpha(i)} + A_{\beta(i)}| \right) + |A_{\alpha(u)} + A_{\beta(u)}| \\
\geq & (2|A_0| - 1) + \left(\sum_{i=1}^{u-1} |(0 + A_i) \cup (m + A_i)| \right) + (|A_0| + |A_u| - 1) \\
& + \left(\sum_{i=1}^{u-1} |A_{\alpha(i)} + A_{\beta(i)}| \right) + (|A_{\alpha(u)}| + |A_{\beta(u)}| - 1)
\end{aligned}$$

Since the classes are full $|A_{\alpha(i)} + A_{\beta(i)}| \geq |H|$ and since $|A_u|$ is minimal, $|A_{\alpha(u)}| \geq |A_u|$ and $|A_{\beta(u)}| \geq |A_u|$:

$$\begin{aligned}
\geq & (2|A_0| - 1) + \left(2 \sum_{i=1}^{u-1} |A_i| \right) + (|A_0| + |A_u| - 1) + (u-1)|H| + (2|A_u| - 1) \\
\geq & 2|A| - 3 + (|A_0| + |A_u| + (u-1)|H|)
\end{aligned}$$

And finally since $|A| = |A_0| + \left(\sum_{i=1}^{u-1} |A_i| \right) + |A_u| \leq |A_0| + (u-1)|H| + |A_u|$:

$$\geq 3|A| - 3.$$

One reaches a contradiction and the end of the proof.

□

This result is optimal in the sense that the set

$$A_x = [0, a-1] \cup [x, x+b-1]$$

with $x > a - 2 + \max\{a, b\}$, it has cardinality $a + b$ and sumset:

$$A_x + A_x = [0, 2a-2] \cup [x, x+a+b-2] \cup [2x, 2x+2b-2]$$

of cardinality $(2a-1) + (a+b-1) + (2b-1) = 3(a+b) - 3$, and it cannot be included in any small arithmetical progression since x can be as large as desired.

IV

Introduction to the polynomial method

IV.1 The Combinatorial Nullstellensatz

Theorem 12 (Alon)**.** *Let $\mathbb{F}$ be a field and $P \in \mathbb{F}[X_1, \dots, X_d]$ a polynomial. If P has degree $\sum_{i=1}^{d} k_i$ and has a nonzero (leading) coefficient of the monomial $\prod_{i=1}^{d} X_i^{k_i}$,*
Therefore whatever family of sets $(A_1, \dots, A_d)$, satisfying $|A_i| > k_i$, there is $(a_1, \dots, a_d) \in A_1 \times \dots \times A_d$ such that:

$$P(a_1, \dots, a_d) \neq 0.$$

In the case, where $d = 1$, the combinatorial formulation just says that a polynomial of degree l has a non zero value on any set of cardinality $|A| > l$.

The proof is based on some polynomial reduction similar to the euclidean division, that does not hold in generality in $\mathbb{F}[X_1, \dots, X_d]$.

Theorem 13 (Alon)**.** *Let $\mathbb{F}$ be a field, $(A_1, \dots, A_d)$ a family of subsets of $\mathbb{F}$. Define $g_i(X_i) = \prod_{a_i \in A_i} (X_i - a_i)$.*
If $P \in \mathbb{F}[X_1, \dots, X_d]$ vanishes on the cartesian product $A_1 \times \dots \times A_d$, then there are polynomials $h_i \in \mathbb{F}[X_1, \dots, X_d]$, satisfying $\deg(h_i) \leq \deg(P) - \deg(g_i)$ such that:

$$P = \sum_{i=1}^{d} h_i g_i.$$

As stated, it says that the ideal of polynomial that vanish on a cartesian product is radical and spanned by the polynomials $g_i(X_i)$ for i from 1 to d. It is called the Combinatorial Nullstellensatz due to the comparaison to the Hilbert Nullstellensatz:

Theorem 14 (Hilbert)**.** *Let $\mathbb{F}$ be an algebraically closed field, If $P \in \mathbb{F}[X_1, \dots, X_d]$ vanishes on the set of common zeros of a family of polynomials $g_i \in \mathbb{F}[X_1, \dots, X_d]$, $i = 1 \dots n$ then there exists $k \in \mathbb{N}^*$ and some polynomials $h_i \in \mathbb{F}[X_1, \dots, X_d]$, such that:*

$$P^k = \sum_{i=1}^{n} h_i g_i.$$

The similarity of these two expressions and the numerous combinatorial applications gave its name to the Combinatorial Nullstellensatz. Nevertheless, one notice the differences:

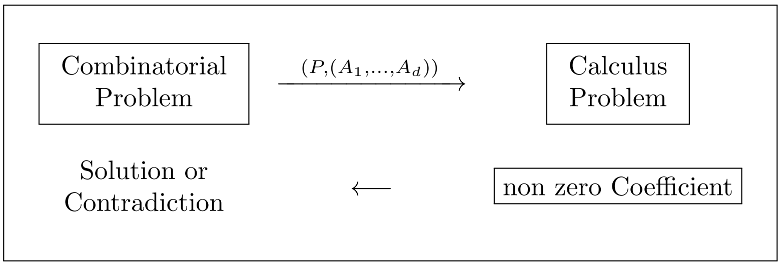
Credits to the Combinatorial Nullstellensatz:

- The field does not need to be algebraically closed.
- There is no power involved in the expression of P. (the radical of this ideal.)
- It is a effective version, the degrees of the h_i are bounded. There is no compensation above the degree of P.

Credits to the Hilbert Nullstellensatz:

- The polynomials g_i are whatever, it makes it a far more sophisticated result.

The polynomial method can be understood by the following scheme:



IV.2 Applications in Additive Combinatorics

IV.2.1 Cauchy-Davenport Theorem

Theorem 15 (Cauchy-Davenport)**.** *Let A and B be two non-empty subsets of $\mathbb{F}_p$:*

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

Proof. Consider first the case where $|A| + |B| - 1 \leq p$:

Let us suppose that $|A + B| < |A| + |B| - 1$, and consider any set C such that $A + B \subset C$ and $|C| = |A| + |B| - 2 \leq p - 1$, then the polynomial

$$\prod_{c \in C} (X + Y - c)$$

does vanish on the cartesian product $A \times B$ and has degree $|A| + |B| - 2$.

The higher degree monomials of P are exactly the same as those of $(X + Y)^{|C|} = (X+Y)^{|A|+|B|-2}$. So the coefficient of $X^{(|A|-1)}Y^{(|B|-1)}$ is $\binom{|A|+|B|-2}{|A|-1} \neq 0 \pmod{p}$ and then the Combinatorial Nullstellensatz contradicts the vanishing of P on $A \times B$.

Consider now the case where $|A| + |B| - 1 \geq p$:

Choose any $A' \subset A$ such that $|A'| + |B| - 1 = p$, by the previous case, one has $|A' + B| = p$ and $A' + B \subset A + B$, so $|A + B| = p$.

□

IV.2.2 Erdős-Heilbronn Conjecture

Let us consider the restricted set addition:

$$A \dot{+} B = \{a + b | a \in A,\ b \in B,\ a \neq b\}\,.$$

Theorem 16 (Erdős-Heilbronn Conjecture)**.** *Let A be a non-empty subset of $\mathbb{F}_p$:*

$$|A \dot{+} A| \geq \min\{p, 2|A| - 3\}.$$

Stated in 1964, this conjecture has been proved only in 1994, by Dias da Silva and Hamidoune, using exterior algebras. The following proof is due to Alon, Nathanson and Rusza.

Proof. In fact, one will prove that for two sets A and B, if $|A| \neq |B|$ then:

$$|A \dot{+} B| \geq \min\{p, |A| + |B| - 2\}.$$

It suffices then to set $B = A \setminus \{a\}$ to get the claim.

Consider first the case where $|A| + |B| - 2 \leq p$:

Let us suppose that $|A \dot{+} B| < |A| + |B| - 2$, and consider any set C such that $A \dot{+} B \subset C$ and $|C| = |A| + |B| - 3 \leq p - 1$, then the polynomial

$$(X - Y) \prod_{c \in C} (X + Y - c)$$

does vanish on the cartesian product $A \times B$ and has degree $|A| + |B| - 2$.

The higher degree monomials of P are exactly the same as those of $(X - Y)(X+Y)^{|C|} = (X-Y)(X+Y)^{|A|+|B|-3}$. So the coefficient of $X^{(|A|-1)}Y^{(|B|-1)}$ is:

$$\binom{|A| + |B| - 3}{|A| - 2} - \binom{|A| + |B| - 3}{|A| - 1} = (|A| - |B|)\frac{(|A| + |B| - 3)!}{(|A| - 1)!(|B| - 1)!} \neq 0 \pmod{p}$$

and then the Combinatorial Nullstellensatz contradicts the vanishing of P on $A \times B$.

Consider now the case where $|A| + |B| - 2 \geq p$:

One can consider that $|B| < |A|$ and choose a set $B' \subset B$, so $|B'| < |A|$, with $|B'| + |A| - 2 = p$, by the previous case, one has $|A \dot{+} B'| = p$ and $A \dot{+} B' \subset A \dot{+} B$, so $|A \dot{+} B| = p$. □

IV.2.3 Dias da Silva-Hamidoune Theorem

The result of Dias da Silva and Hamidoune was a bit more general:

For a subset $A \subset \mathbb{F}_p$, and a integer $h(\in [0, |A|])$, one define:

$$h^\wedge A = \left\{ \sum_{a \in U} a \middle| U \subset A,\ |U| = h \right\}.$$

Theorem 17 (Dias da Silva-Hamidoune)**.** *Let p be a prime and $A \subset \mathbb{F}_p$, given an integer h, one has:*

$$|h^\wedge A| \geq \min\{p, h(|A| - h) + 1\}.$$

Suppose on the contrary that there is a set C that contains $h^\wedge A$ of cardinality $|C| = \min\{p - 1, h(|A| - h)\}$.

One consider the polynomial:

$$P(X_1, \ldots, X_h) = \prod_{c \in C} (X_1 + \cdots + X_h - c) \prod_{1 \leq i < j \leq h} (X_j - X_i).$$

It has degree $|C| + \frac{h(h-1)}{2}$. It vanishes on A^h, notice that the degree is very small for this cartesian product:

In the case where $|C| = h(|A| - h)(\leq p - 1)$, we will consider the reduced cartesian product:

$$\begin{array}{lll}
A_1 & = \big\{ a_1, \ldots, a_{|A|-h}, a_{|A|-h+1} \big\} & \\
A_2 & = \big\{ a_1, \ldots, a_{|A|-h}, a_{|A|-h+1}, a_{|A|-h+2} \big\} & \\
\vdots & = \ \vdots & \ddots \\
A_{h-1} & = \big\{ a_1, \qquad \ldots & , a_{|A|-1} \big\} \\
A_h & = \big\{ a_1, \qquad \ldots & , a_{|A|-1}, a_{|A|} \big\} ,
\end{array}$$

Here $|A_i| = |A| - h + i$, so $\sum_{i=1}^{h} (|A_i| - 1) = \deg(P)$ and it remains to compute the coefficient of the monomial $\prod_{i=1}^{h} X_i^{|A|-h+i-1}$.