Set Addition Theorems

Éric Balandraud
eric.balandraud@imj-prg.fr

Journées Hadamard 2015

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 $g(k)$ is 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. Additive combinatorics would consider similar questions and developments on the integers, residues modulo a prime or any abelian group.

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.

First Session

Let A and B be two non-empty finite subsets of $\mathbb{Z}$, $\mathbb{Z}/p\mathbb{Z}$ or any abelian group, we define their sumset:

$$A + B = \{a + b \mid a \in A,\ b \in B\}.$$

Its cardinality is invariant by translation, indeed $|t + X| = |X|$ whatever is the set X, so that

$$|(t + A) + (s + B)| = |A + B|.$$

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:

$a_1 + b_1$	$a_2 + b_1$	$\dots$	$a_d + b_1$
$a_1 + b_2$	$a_2 + b_2$	$\dots$	$a_d + b_2$
$\vdots$	$\vdots$		$\vdots$
$a_1 + b_\ell$	$a_2 + b_\ell$	$\dots$	$a_d + b_\ell$

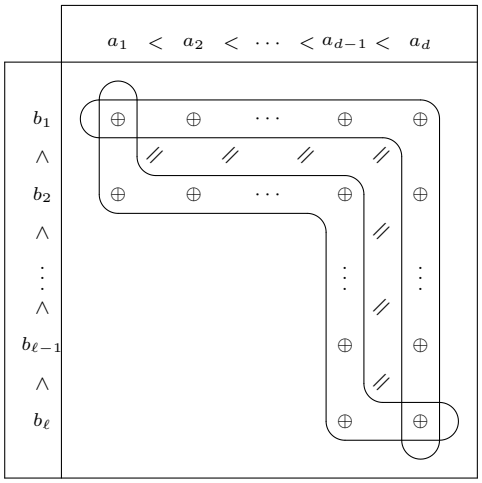
One has a increasing sequence of length $d + \ell - 1$ ($d + \ell - 2$ strict inequalities):

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

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 $d+\ell-1$:

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



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. □

Another topic of interest in additive combinatorics is the restricted sumset defined by:

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

This can be generalized for sums of more than two terms in the following way:

For a given set $A \subset \mathbb{Z}$, and $h \in \mathbb{N}$, one consider the h-fold restricted sumset:

$$h^{\wedge}A = \{a_1 + \cdots + a_h \mid a_i \in A,\ a_i \neq a_j\}.$$

Its cardinality is also invariant by translation, indeed $h^{\wedge}(t+A) = h.t + h^{\wedge}A$, so that

$$|h^{\wedge}(t+A)| = |h^{\wedge}A|.$$

The sets $h^{\wedge}A$ and $(|A|-h)^{\wedge}A$ are symmetric, indeed $(|A|-h)^{\wedge}A = \left(\sum_{a\in A} a\right) - h^{\wedge}A$, so

$$|(|A|-h)^{\wedge}A| = |h^{\wedge}A|.$$

Theorem 2. *Let A be a non-empty subsets of $\mathbb{Z}$, and $h \in [0, |A|]$, then:*

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

One has equality if and only if

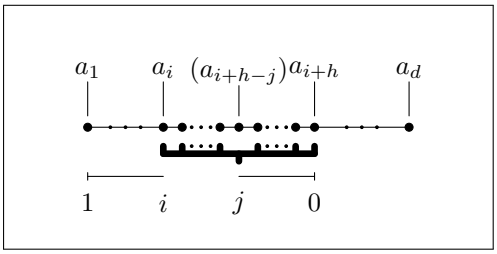
- *either $h \in \{0, 1, |A-1|, |A|\}$,*
- *or $h = 2$, $A = \{a_1 < a_2 < a_3 < a_4\}$ and its 4 elements satisfy $a_1 + a_4 = a_2 + a_3$,*
- *or $h \in [2, |A|-2]$, $|A| \geq 5$ and A is an arithmetical progression.*

Proof. Denote $A = \{a_1 < a_2 < \cdots < a_d\}$.

Whenever $h \in \{0, 1, |A|-1, |A|\}$, the inequality, and the equality is clear. Notice that $h^{\wedge}A = \left(\sum_{a\in A} a\right) - (|A|-h)^{\wedge}A$.

Consider for a couple $(i,j) \in ([1, d-h] \times [0,h])$ the sum:

$$s_{i,j} = \sum_{\substack{k=0 \\ k\neq h-j}}^{h} a_{i+k}.$$



One has

$$s_{i,j+1} - s_{i,j} = a_{i+h-j} - a_{i+h-(j+1)} > 0,\ j \in [0, h-1],$$

and

$$s_{i,h} = s_{i+1,0}.$$

To summarize:

$$s_{i,0} < s_{i,1} < s_{i,2} < \cdots < s_{i,h} = s_{i+1,0}.$$

Therefore, one has at least $\underbrace{(h+1)}_{i=1} + h\underbrace{(d-h-1)}_{i\in[2,d-h]} = 1 + h(d-h)$ elements in $h^{\wedge}A$.

From now on, we consider that the inequality is an equality, so $h^{\wedge}A$ is exactly the set of the sums $s_{i,j}$.

Whenever $h \in \{0, 1, |A|-1, |A|\}$, the equality is clear.

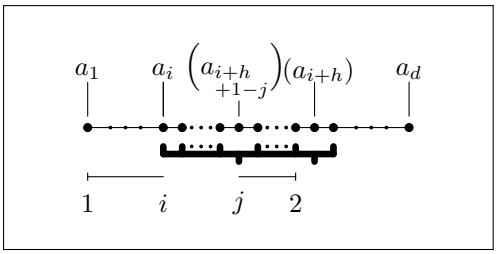
Suppose that $|A| = 4$ and $h = 2$, denote $A = \{a_1, a_2, a_3, a_4\}$, with $a_1 < a_2 < a_3 < a_4$, one has

$$a_1 + a_2 < a_1 + a_3 < \begin{matrix} a_2 + a_3 \\ a_1 + a_4 \end{matrix} < a_2 + a_4 < a_3 + a_4,$$

and $1 + 2(4-2) = 5$, so necessarily one has to have $a_2 + a_3 = a_1 + a_4$ and this condition is also sufficient.

Otherwise $|A| \geq 5$ and $h \in [2, |A|-2]$. Consider the new sums defined for a couple $(i,j) \in ([1, d-h-1] \times [2,h])$ the sum:

$$\begin{aligned} u_{i,j} &= \left(\sum_{\substack{k=0 \\ k\neq h+1-j}}^{h-1} a_{i+k} \right) + a_{i+h+1} \\ &= s_{i,j-1} + a_{i+h+1} - a_{i+h}. \end{aligned}$$



One has:

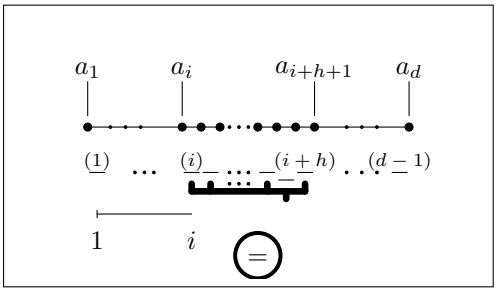
$$s_{i,1} < u_{i,2} < u_{i,3} < \cdots < u_{i,h} < s_{i+1,1}.$$

Since $h^{\wedge}A$ is composed by only the sums $s_{i,j}$ previously defined, one has $s_{i,j} = u_{i,j}$, or equivalently:

$$a_{i+h-j+1} - a_{i+h-j} = a_{i+h+1} - a_{i+h}.$$

Or considering that $j \in [2,h]$:

$$a_{i+1} - a_i = a_{i+2} - a_{i+1} = \cdots = a_{i+h-1} - a_{i+h-2} \underbrace{=}_{(+2\ !)} a_{i+h+1} - a_{i+h}.$$



The remaining case $a_{i+h} - a_{i+h-1} = a_{i+1} - a_i$ is an overlaping of the previous ones, whenever $h \in [3, k-3]$:

$$\begin{aligned} i \in [2, d-h-1], \quad a_{i+h} - a_{i+h-1} &= a_{(i-1)+(h+1)} - a_{(i-1)+h} \\ &= a_{(i-1)+(h-1)} - a_{(i-1)+(h-2)} \\ &= a_{i+h-2} - a_{i+h-3} \\ &= a_{i+1} - a_i. \end{aligned}$$

$$\begin{aligned} i = 1, \quad a_{1+h} - a_h &= a_{2+(h-1)} - a_{2+(h-2)} \\ &= a_{2+(h-1)} - a_{2+(h-2)} \\ &= a_{1+(h-1)} - a_{1+(h-2)} \\ &= a_2 - a_1. \end{aligned}$$

This proves that A is an arithmetical progression.

Whenever $h = 2$ (the case $h = d-2$ is symmetric), these equalities do not overlap, one only have $a_{i+1} - a_i = a_{i+3} - a_{i+1}$.

Since $|A| \geq 5$, the six smallest elements are given by:

$$a_1 + a_2 < a_1 + a_3 < \begin{array}{c} a_2 + a_3 < a_2 + a_4 < a_3 + a_4 \\ a_1 + a_4 < a_1 + a_5 < a_2 + a_5 \end{array} < a_3 + a_5,$$

therefore $a_1 + a_5 = a_2 + a_4$, or $a_5 - a_4 = a_2 - a_1$ and A is also an arithmetical progression.

□

For a given set $A \subset \mathbb{Z}$, one defines the set of subsums:

$$\Sigma(A) = \left\{ \sum_{a \in A'} a \mid A' \subset A \right\} = \sum_{a \in A} \{0, a\} = \bigcup_{h=0}^{|A|} (h^\wedge A).$$

Its cardinality is not invariant under translation, but it has a symmetry property that allows to exchange a element by its opposite. If $a \in A$ and $-a \notin A$, consider $A' = A \setminus \{a\} \cup \{-a\}$, since $\{0, -a\} = -a + \{0, a\}$ one has $\Sigma(A') = -a + \Sigma(A)$ and so:

$$|\Sigma(A')| = |\Sigma(A)|.$$

Theorem 3. *Let A be a non-empty subsets of $\mathbb{Z}$, such that $A \cap (-A) = \emptyset$, then:*

$$|\Sigma(A)| \geq 1 + \frac{|A|(|A|+1)}{2}.$$

One has equality, if and only if

- *either $|A| \leq 2$,*
- *or $|A| = 3$ and its 3 elements satisfy a relation of the type $\pm a_1 \pm a_2 \pm a_3 = 0$,*
- *or $|A| \geq 4$ and the absolute values of the elements of A form an arithmetical progression.*

Proof. The property $A \cap (-A) = \emptyset$ allows us to consider that A has only distinct positive elements. Hence $A = \{a_1, \ldots, a_d\}$, with $0 < a_1 < a_2 < \cdots < a_d$.

If $|A| = 1$, the result is obvious. We will state the result by induction.

Consider that $|\Sigma(a_1, \ldots, a_{d-1})| \geq 1 + \frac{d(d-1)}{2}$ and denote $m = \max(\Sigma(a_1, \ldots, a_{d-1}) = a_1 + \cdots + a_{d-1}$. One has d new elements greater than m in $\Sigma(A)$:

$$m < m + a_d - a_{d-1} < m + a_d - a_{d-2} < \cdots < m + a_d - a_2 < m + a_d - a_1 < m + a_d.$$

Therefore $|\Sigma(A)| \geq \left(1 + \frac{(d-1)d}{2}\right) + d = 1 + \frac{d(d+1)}{2}$. This concludes the proof of the inequality.

From now on, we consider that the inequality is an equality.

Whenever $d \leq 2$, the inequality is always an equality, because $0, a_1, a_2, a_1 + a_2$ are pairwise distinct.

Whenever $d = 3$, the equality is $\left|\sum_{i=1}^{3} \{0, a_i\}\right| = 7$. In particular, one has the two sequences of inequalities:

$$\begin{aligned} 0 < a_1 < a_2 < \quad & a_1 + a_2 \\ < \quad & a_3 \quad < a_1 + a_3 < a_2 + a_3 < a_1 + a_2 + a_3. \end{aligned}$$

Since $a_2 < a_3$, the only necessary and sufficient equality is $a_3 = a_1 + a_2$.

Whenever $d = 4$, the equality is $\left|\sum_{i=1}^{4} \{0, a_i\}\right| = 11$. In particular, one has the four sequences of inequalities:

$$0 < a_1 < a_2 < a_1 + a_2$$
$$< a_3 < a_1 + a_3 < a_2 + a_3 < a_1 + a_2 + a_3$$
$$< a_4 < a_1 + a_4 < a_2 + a_4 < a_1 + a_2 + a_4$$
$$< a_3+a_4 < a_1+a_3+a_4 < a_2+a_3+a_4 < a_1+a_2+a_3+a_4$$

One needs the equalities:

$$\left| \begin{array}{lcl} a_1 + a_2 & = & a_3 \\ a_1 + a_3 & = & a_4 \\ a_2 + a_3 & = & a_1 + a_4. \end{array} \right.$$

They can be rewritten as

$$\begin{pmatrix} 1 & 1 & -1 & 0 \\ 1 & 0 & 1 & -1 \\ -1 & 1 & 1 & -1 \end{pmatrix} \begin{pmatrix} a_1 \\ a_2 \\ a_3 \\ a_4 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}.$$

This linear system (of rank 3) can be solved as:

$$\left| \begin{array}{lcl} a_2 & = & 2a_1 \\ a_3 & = & 3a_1 \\ a_4 & = & 4a_1. \end{array} \right.$$

Finally whenever $d > 4$, if we suppose that $\left|\sum_{i=1}^{d}\{0, a_i\}\right| = 1+(d+(d-1)+\cdots+1)$. The inequality $\left|\sum_{i=1}^{d}\{0, a_i\}\right| \geq \left|\sum_{i=1}^{d-1}\{0, a_i\}\right| + d$ has to be an equality and necessarily $\left|\sum_{i=1}^{d-1}\{0, a_i\}\right| = 1 + ((d-1) + \cdots + 1)$. From the induction hypothesis, one has $a_i = i.a_1$, and:

$$\sum_{i=1}^{d-1}\{0, a_i\} = \left[\!\left[0, \frac{d(d-1)}{2}\right]\!\right].a_1.$$

Therefore,

$$\sum_{i=1}^{d}\{0, a_i\} = \left[\!\left[0, \frac{d(d-1)}{2}\right]\!\right].a_1 \bigcup \left[\!\left[\frac{a_d}{a_1}, \frac{a_d}{a_1} + \frac{d(d-1)}{2}\right]\!\right].a_1.$$

If $\frac{a_d}{a_1}$ is not an integer or $\frac{a_d}{a_1} > \frac{d(d-1)}{2}$, these two sets are disjoint, one get $\left|\sum_{i=1}^{d}\{0, a_i\}\right| = d(d-1)+2$. So $1+\frac{d(d+1)}{2} = d(d-1)+2$ what implies $d = 1$ or $d = 2$, contradiction. Otherwise $\frac{a_d}{a_1}$ is an integer strictly greater than $d-1$ and $\frac{a_d}{a_1} \leq \frac{d(d-1)}{2}$. But then, one has $\left|\sum_{i=1}^{d}\{0, a_i\}\right| = \frac{d(d-1)}{2} + \frac{a_d}{a_1} + 1$. This yields the equality: $1 + \frac{d(d+1)}{2} = \frac{d(d-1)}{2} + \frac{a_d}{a_1} + 1$ what naturally implies $\frac{a_d}{a_1} = d$.

□

Suppose that the hypothesis $A \cup (-A) = \emptyset$ is not satisfied, consider the example $A = [-a, a]$, so $|A| = 2a + 1$. One has $\Sigma(A) = \left[-\frac{a(a+1)}{2}, \frac{a(a+1)}{2}\right]$ and $|\Sigma(A)| = a(a+1) + 1 = \frac{|A|-1}{2}\frac{|A|+1}{2} + 1 = \frac{|A|^2-1}{4} + 1 < 1 + \frac{|A|(|A|+1)}{2}$ and the conclusion of the theorem does not hold.

Second Session

As a sumset can be defined on any group, one can consider the same problems in a larger group.

To work on 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.

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.

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 $B(e) \neq \emptyset$.

Theorem 4 (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 $a - b_1 \notin A - b_2$. ($b_1 - b_2$ has order p.) 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. □

Exercise 2. *Prove the generalization, let $i \in [1, n]$, A_i finite non-empty subset of $\mathbb{Z}/p\mathbb{Z}$:*

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

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

Exercise 3. *Let p be a prime number, and k a divisor of $p - 1$, prove that any $x \in \mathbb{Z}/p\mathbb{Z}$ is the sum of k k-th powers.*

The proof of Cauchy-Davenport has been generalized to any cyclic groups with an extra condition:

Theorem (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 $B \setminus \{0\} \subset (\mathbb{Z}/n\mathbb{Z})^*$ then:*

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

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.

To establish the full caracterisation of the critical case, one needs the following lemma on arithmetic progressions:

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

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

if one of the sets A, B, or $\mathbb{Z}/p\mathbb{Z} \smallsetminus (A + B)$ is an arithmetical progression then the two others are also arithmetical progressions with the same difference.

Proof. Denote $C = \mathbb{Z}/p\mathbb{Z} \smallsetminus (A + B)$, one has $|C| = p - (|A| + |B| - 1)$ and $0 \notin A + B + C$. But Cauchy-Davenport Theorem implies that

$$|A+B+C| \geq |A+B|+|C|-1 = (|A|+|B|-1)+(p-(|A|+|B|-1))-1 = p-1.$$

So we have equality $|A + B + C| = p - 1$, and this implies that also $|A + C| = |A| + |C| - 1$ and $|B + C| = |B| + |C| - 1$. The three sets A, B and C play the same role.

Hence consider that A is an arithmetical progressions with difference r, $A = \{a_0, a_0 + r, \ldots, a_0 + (a - 1).r\}$.

If $|A| = 2$, consider the minimal decomposition of B into arithmetical progressions of difference r: $B = \bigcup_{i=1}^{n} B_i$, one has $(B_i \pm r) \cap B_j = \emptyset$, and $|B + \{0, r\}| = |B| + n$. Since it has the cardinality of $|A + B| = |A| + |B| - 1 = |B| + 1$, then $n = 1$ and B is an arithmetical progression of difference r.

If there is no element b in B such that $(b + \{r, \ldots, (a - 1).r\}) \cap B = \emptyset$ then naturally

$$A + B = a_0 + (\{0, r, \ldots, (a - 1).r\} + B) = \mathbb{Z}/p\mathbb{Z}.$$

Otherwise, there is such an element $b_0 \in B$, which we will call an end, and the "final" element $b_0 + a_0 + (a-1).r$ admits only one writing as a sum of an element in A and a element in B. Indeed, if $b_0 + a_0 + (a - 1).r = b' + a_0 + i.r$, then $b' = b_0 + (a - 1 - i).r$, what can be possible only if $i = a - 1$ because b_0 is an end, and so $b' = b$.

Removing the last element of A: Denoting $A' = A \setminus \{a_0 + (a - 1).r\}$, one has $|A'| = |A| - 1$ and

$$|A'| + |B| - 1 \leq |A' + B| \leq |A + B| - 1 = |A| + |B| - 2 = |A'| + |B| - 1.$$

In particular, $|A' + B| = |A'| + |B| - 1$ and by induction, B is an arithmetical progression of difference r. □

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

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

then A and B are arithmetical progressions with same difference.

Proof. If one of these sets has cardinality 2, the result is easy. We will then consider that $\min\{|A|, |B|, |\mathbb{Z}/p\mathbb{Z} \setminus (A+B)|\} > 2$.

From the previous lemma, it suffices to prove that $\mathbb{Z}/p\mathbb{Z} \setminus (A+B)$ is an arithmetical progression. We will prove that a proper e-transform can be done to (A, B), so that the complementary of $A+B$ remains unchanged and the sets $B(e)$ satisfy $2 \leq |B(e)| < |B|$.

If we consider a e-transform of a critical pair (A, B), one has:

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

therefore all these inequalities are equalities. In particular $A+B = A(e)+B(e)$.

Let $b_0 \in B$, define $X = \{e \in A - b_0 \mid B(e) \neq B\}$, therefore $b_0 \in B(e)$ and $B(e)$ is not empty whenever $e \in X$, (and $|B(e)| < |B|$).

Suppose that $e \in (A - b_0) \setminus X = Y$, therefore $B(e) = B$ and so $B \subset A - e$, or $e + B \subset A$, then $Y + B \subset A$, and by Cauchy-Davenport:

$$\begin{aligned} |A| &\geq |Y + B| \\ &\geq |Y| + |B| - 1 \\ &= |A| - |X| + |B| - 1 \end{aligned}$$

so

$$|X| \geq |B| - 1 \geq 2.$$

Now let us prove that for some $e \in A - b_0$, one has $|B(e)| \geq 2$. Suppose the opposite: for all $e \in A - b_0$, $B(e) = B \cap (A - e) = \{b_0\}$, therefore $(X + (B \setminus \{b_0\})) \cap A = \emptyset$, so $(X + (B \setminus \{b_0\})) \subset (A + B) \setminus A$, and by Cauchy-Davenport, one has:

$$|X| + |B| - 2 = |X| + (|B| - 1) - 1 \leq |X + (B \setminus \{b_0\})| \leq |A + B| - |A| = |B| - 1,$$

what gives a contradiction to $|X| \geq 2$.

After several applications of e-transforms, one would reach a situation where $|\tilde{B}| = 2$ and $|\tilde{A} + \tilde{B}| = |\tilde{A}| + |\tilde{B}| - 1 < p - 1$, so $\tilde{A} + \tilde{B} = A + B$ is an arithmetical progression, and so are A and B by the previous lemma.

□

An interesting application of these two theorems is the following:

Proving that, whenever $k \mid p - 1$ and $k \neq \frac{p-1}{2}$, 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 (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.*

An application of this last theorem is:

Exercise 4. *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 seqences, 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 $\ell \geq n - 1$.

Third Session

Today, we will consider a larger context, we will consider sumsets in any abelian group. And we will use this larger scope to prove a deeper structural result on the integers.

The eventual presence of finite subgroups have to be taken into account, 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).

Lemma 3. *Let $C = C_1 \cup \cdots \cup C_n$ be an union of n non empty sets of an abelian group G, then:*

$$\min_{i \in \{1,\dots,n\}} \{|C_i| + |H(C_i)|\} \leq |C| + |H(C)|.$$

Proof. We prove this lemma by induction on n. Whenever $n \geq 3$, the induction step is obvious:

$$\begin{aligned}
&\min_{i \in \{1,\dots,n\}} \{|C_i| + |H(C_i)|\} \\
=&\min\{\min_{i \in \{1,\dots,n-1\}} \{|C_i| + |H(C_i)|\}, |C_n| + |H(C_n)|\} \\
\leq&\min\left\{\left|\bigcup_{i=1}^{n-1} C_i\right| + \left|H\left(\bigcup_{i=1}^{n-1} C_i\right)\right|, |C_n| + |H(C_n)|\right\} \\
\leq&|C| + |H(C)|.
\end{aligned}$$

It remains to prove the lemma for $n = 2$. If one of these sets is C itself, the claim is obvious, otherwise one can consider that the sets C_1 and C_2 are proper subsets of C. Denote H_i the period of C_i, for $i \in \{1, 2\}$, and $h_i = |H_i|$ and H the period of C.

We may assume that $H_1 \cap H_2 = \{0\}$, since otherwise one can reduce the problem modulo the subgroup $H_1 \cap H_2$. We denote $\overline{H} = H_1 + H_2$, $|\overline{H}| = h_1 h_2$.

We want to prove that for some $i \in \{1, 2\}$.

$$|C \setminus C_i| \geq h_i - |H|.$$

Let us consider a non-empty intersection of C with a $\overline{H}$-coset, $x + \overline{H}$. It intersects C_1 on k_1 H_1-cosets, so $0 \leq k_1 \leq h_2$, and C_2 on k_2 H_2-cosets, so $0 \leq k_2 \leq h_1$.

Since C_i is H_i-periodic and that each pair of a H_1-coset and a H_2-coset intersect in one element, one has:

$$|(C \setminus C_2) \cap (x + \overline{H})| = k_1(h_1 - k_2),$$

$$|(C \setminus C_1) \cap (x + \overline{H})| = k_2(h_2 - k_1).$$

- If there is a coset such that $0 < k_1 < h_2$ and $0 < k_2 < h_1$, then one has:

  $$|C \setminus C_2||C \setminus C_1| \geq k_1k_2(h_1 - k_2)(h_2 - k_1) \geq (h_1 - 1)(h_2 - 1).$$

  And so one of the two $|C \setminus C_i|$ has to be greater than $h_i - 1$.

- Otherwise, consider that there is a coset such that $k_1 = 0$ and $k_2 > 0$ and another one such that $k_2 = 0$ and $k_1 > 0$. One has:

  $$|C \setminus C_2| \geq h_1,$$

  $$|C \setminus C_1| \geq h_2.$$

  So

  $$|C \setminus C_2||C \setminus C_1| \geq h_1h_2,$$

  what is even stronger the previously.

- Finally in the last case, whenever there is no $\overline{H}$-coset with $k_1 = 0$ (or symmetrically $k_2 = 0$). The set C intersect an $\overline{H}$-coset in either the whole coset, or $k_1 < h_1$ and $k_2 < h_2$, what implies that $k_2 = 0$, therefore C is an union of H_1-cosets. Thus $H_1 < H$ and $h_1 - |H| \leq 0$, which proves that

  $$|C \setminus C_1| \geq h_1 - |H|.$$

□

Theorem 6 (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 $A + B$.

Proof. Let us now prove the theorem, let us consider for any $b \in B$, the set of pairs of (A', B') such that:

$$\begin{aligned} A \subset A',\, b \in B' \\ A' + B' \subset A + B \\ |A'| + |B'| = |A + H| + |B + H|. \end{aligned}$$

The pair $(A + H, B + H)$ does satisfy these conditions, so the set is not empty.

Among all these pairs, let us consider a pair (A_b, B_b) with $|A_b|$ maximal (and so $|B_b|$ minimal), $a \in A_b$ and define $e = a - b$. We apply the e-transform to (A_b, B_b) to obtain $(A_b(e), B_b(e))$. The properties of the e-transform imply

that $(A_b(e), B_b(e))$ still satisfy the above conditions. Necessarily, since $|A_b|$ is maximal, one has $A_b(e) = A_b$. This means that $e + B_b = a - b + B_b \subset A_b$ for any $a \in A_b$, therefore

$$A_b \subset A_b + B_b - b \subset A_b.$$

We then have $B_b - b \subset H(A_b) = H(A_b + B_b)$ and $|A_b| \leq |A_b + B_b|$, so:

$$|A + H| + |B + H| = |A_b| + |B_b| \leq |A_b + B_b| + |H(A_b + B_b)|.$$

Since this inequality is valid whatever the element $b \in B$, and that the sets $A_b + B_b$ have union $A + B$, one has from the previous lemmas:

$$|A + H| + |B + H| \leq \min_{b \in B}\{|A_b + B_b| + |H(A_b + B_b)|\} \leq |A + B| + |H|.$$

□

Exercise 5. *Proof the equivalence with this second formulation of Kneser's theorem:*

Theorem 7 (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 $A + B$.

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 8 ($(3k-4)$-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 $d \mid m$ 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 $2|\overline{A}+H| - |H| \leq 2|\overline{A}| - 1$, 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 $|\overline{A} + \overline{A}| = |\overline{A + H}| - |H| = 2(u + 1)|H| - |H| = (2u + 1)|H|$ 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.