Une introduction à la combinatoire additive

Éric Balandraud

Séminaire GT Combi du LiX

Plan

Un peu de théorie additive des nombres

Trois résultats ensemblistes dans $\mathbb{F}_p$

Deux problèmes d'ordonnancement

Quelques résultats séquentiels

Une inspiration géométrique

Problèmes fondateurs de théorie additive des nombres

Conjecture (Conjecture de Goldbach - 1742)

$$\forall\ n > 1,\ \exists\ p_1, p_2\ premiers,\ tels\ que\ 2n = p_1 + p_2.$$

Problèmes fondateurs de théorie additive des nombres

Conjecture (Conjecture de Goldbach - 1742)

$$\forall\ n > 1,\ \exists\ p_1, p_2\ premiers,\ tels\ que\ 2n = p_1 + p_2.$$

Théorème (Problème de Waring - 1770)

Etant donné, k, existe-t-il g tel que:

$$\forall\ n \in \mathbb{N},\ \exists\ x_1, x_2, \ldots, x_g\ tels\ que\ n = x_1^k + x_2^k + \cdots + x_g^k.$$

Problèmes fondateurs de théorie additive des nombres

Conjecture (Conjecture de Goldbach - 1742)

$$\forall\ n > 1,\ \exists\ p_1, p_2\ \textit{premiers, tels que}\ 2n = p_1 + p_2.$$

Théorème (Problème de Waring - 1770)

Etant donné, k, existe-t-il g tel que:

$$\forall\ n \in \mathbb{N},\ \exists\ x_1, x_2, \ldots, x_g\ \textit{tels que}\ n = x_1^k + x_2^k + \cdots + x_g^k.$$

$$2.\mathbb{N}^* \setminus \{2\} = \mathbb{P} + \mathbb{P}, \qquad \mathbb{N} = \underbrace{P_k + \cdots + P_k}_{g \text{ fois}}.$$

Etant donné $A \subset \mathbb{N}$, On dit que A est une base additive (resp. asymptotique), si il existe k (et N_0) tel que $k.A = \mathbb{N}$ (resp. $k.A = \mathbb{N}_{\geqslant N_0}$).

Etant donné $A \subset \mathbb{N}$, On dit que A est une base additive (resp. asymptotique), si il existe k (et N_0) tel que $k.A = \mathbb{N}$ (resp. $k.A = \mathbb{N}_{\geqslant N_0}$).

$$\underline{d}(A) = \liminf \frac{|A \cap [1, n]|}{n}, \ \overline{d}(A) = \limsup \frac{|A \cap [1, n]|}{n},$$

$$\sigma(A) = \inf \left\{ \frac{|A \cap [1, n]|}{n} \mid n \in \mathbb{N}^* \right\}.$$

Etant donné $A \subset \mathbb{N}$, On dit que A est une base additive (resp. asymptotique), si il existe k (et N_0) tel que $k.A = \mathbb{N}$ (resp. $k.A = \mathbb{N}_{\geqslant N_0}$).

$$\underline{d}(A) = \liminf \frac{|A \cap [1,n]|}{n}, \ \overline{d}(A) = \limsup \frac{|A \cap [1,n]|}{n},$$

$$\sigma(A) = \inf \left\{ \frac{|A \cap [1,n]|}{n} \mid n \in \mathbb{N}^* \right\}.$$

- Si $pgcd(A) = 1$, $0 \in A$ et $\overline{d}(A) < 1/2$, alors

$$\overline{d}(A+A) \geqslant \frac{3}{2}\overline{d}(A).$$

Etant donné $A \subset \mathbb{N}$, On dit que A est une base additive (resp. asymptotique), si il existe k (et N_0) tel que $k.A = \mathbb{N}$ (resp. $k.A = \mathbb{N}_{\geqslant N_0}$).

$$\underline{d}(A) = \liminf \frac{|A \cap [1,n]|}{n}, \ \overline{d}(A) = \limsup \frac{|A \cap [1,n]|}{n},$$

$$\sigma(A) = \inf \left\{ \frac{|A \cap [1,n]|}{n} \mid n \in \mathbb{N}^* \right\}.$$

- Si $pgcd(A) = 1$, $0 \in A$ et $\overline{d}(A) < 1/2$, alors

$$\overline{d}(A+A) \geqslant \frac{3}{2}\overline{d}(A).$$

- Si $\underline{d}(A+A) \leqslant (2-\epsilon)\underline{d}(A)$, alors A est un gros sous-ensemble d'une union de progressions arithmétiques de même raison N.

Théorème (Kneser - 1955)

Soient G un groupe abélien, A et B deux sous-ensembles finis non vides de G tels que:

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

alors $A+B$ est périodique.

Théorème (Kneser - 1955)

Soient G un groupe abélien, A et B deux sous-ensembles finis non vides de G tels que:

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

alors $A+B$ est périodique.

Théorème (Freiman - 1959)

Soit $A \subset \mathbb{N}$, si $|A+A| \leqslant 3|A| - 4$ alors A est inclus dans une progression arithmétique de longueur $\leqslant |A+A| - |A| + 1$.

Plan

Un peu de théorie additive des nombres

Trois résultats ensemblistes dans $\mathbb{F}_p$

Deux problèmes d'ordonnancement

Quelques résultats séquentiels

Une inspiration géométrique

Théorème (Cauchy-Davenport - 1813, 1935)

$p \in \mathbb{P}$, A, B deux sous-ensembles non vides de $\mathbb{F}_p$:

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

Théorème (Cauchy-Davenport - 1813, 1935)

$p \in \mathbb{P}$, A, B deux sous-ensembles non vides de $\mathbb{F}_p$:

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

Théorème (Vosper - 1956)

$p \in \mathbb{P}$, A, B deux sous-ensembles de $\mathbb{F}_p$, tels que $\min\{|A|,|B|\} > 1$ *et* $|\mathbb{F}_p \setminus (A+B)| > 1$.
Si $|A+B| = |A|+|B|-1$, A et B sont deux progressions arithmétiques de même raison.

Conjecture (Erdős-Heilbronn - 1964)

$p \in \mathbb{P}$, $A \subset \mathbb{F}_p$, *alors:*

$$|\{a_1 + a_2 \mid a_i \in A,\ a_1 \neq a_2\}| \geqslant \min\{p, 2|A| - 3\}$$

Conjecture (Erdős-Heilbronn - 1964)

$p \in \mathbb{P}$, $A \subset \mathbb{F}_p$, *alors:*

$$|\{a_1 + a_2 \mid a_i \in A,\ a_1 \neq a_2\}| \geqslant \min\{p, 2|A| - 3\}$$

Soit:

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

Conjecture (Erdős-Heilbronn - 1964)

$p \in \mathbb{P}$, $A \subset \mathbb{F}_p$, *alors:*

$$|\{a_1 + a_2 \mid a_i \in A,\ a_1 \neq a_2\}| \geqslant \min\{p, 2|A| - 3\}$$

Soit:

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

Théorème (Dias da Silva-Hamidoune - 1994)

$p \in \mathbb{P}$, $A \subset \mathbb{F}_p$, *et* $h \in [0, |A|]$, *on a:*

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

Conjecture (Selfridge - 1976)

p nombre premier impair, $A \subset \mathbb{Z}/p\mathbb{Z}$ sans sous-somme nulle de cardinal maximal, alors $|A|$ est le plus grand k tel que:

$$\frac{k(k+1)}{2} < p.$$

Conjecture (Selfridge - 1976)

p nombre premier impair, $A \subset \mathbb{Z}/p\mathbb{Z}$ sans sous-somme nulle de cardinal maximal, alors $|A|$ est le plus grand k tel que:

$$\frac{k(k+1)}{2} < p.$$

Théorème (B.)

p nombre premier impair, $A \subset \mathbb{Z}/p\mathbb{Z}$, tel que $A \cap (-A) = \emptyset$.

$$|\Sigma(A)| \geqslant \min\left\{p, 1 + \frac{|A|(|A|+1)}{2}\right\},$$

$$|\Sigma^*(A)| \geqslant \min\left\{p, \frac{|A|(|A|+1)}{2}\right\}.$$

Plan

Un peu de théorie additive des nombres

Trois résultats ensemblistes dans $\mathbb{F}_p$

Deux problèmes d'ordonnancement

Quelques résultats séquentiels

Une inspiration géométrique

Théorème (Hall - 1952)

Soit G un groupe abélien fini, il existe $\sigma \in \mathfrak{S}_G$ tel que les sommes $x + \sigma(x)$ soient distinctes.

Snevily's Conjecture

G un groupe abélien fini d'ordre impair.

$a_1, \ldots, a_k$ distincts	
$b_1, \ldots, b_k$ distincts	
	.

Snevily's Conjecture

G un groupe abélien fini d'ordre impair.

$a_1, \ldots, a_k$ distincts	Il existe π telle que
$b_1, \ldots, b_k$ distincts	$a_1 + b_{\pi(1)}, \ldots, a_k + b_{\pi(k)}$
	soient distincts.

Snevily's Conjecture

G un groupe abélien fini d'ordre impair.

$a_1, \ldots, a_k$ distincts	Il existe π telle que
$b_1, \ldots, b_k$ distincts	$a_1 + b_{\pi(1)}, \ldots, a_k + b_{\pi(k)}$
	soient distincts.

$G = \mathbb{Z}/p\mathbb{Z}$ (Alon - 1999),
$G = \mathbb{Z}/n\mathbb{Z}$ (Dasgupta, Karolyi, Serra, Szegedy - 2001),

Snevily's Conjecture

G un groupe abélien fini d'ordre impair.

$a_1, \ldots, a_k$ distincts	Il existe π telle que
$b_1, \ldots, b_k$ distincts	$a_1 + b_{\pi(1)}, \ldots, a_k + b_{\pi(k)}$
	soient distincts.

$G = \mathbb{Z}/p\mathbb{Z}$ (Alon - 1999),
$G = \mathbb{Z}/n\mathbb{Z}$ (Dasgupta, Karolyi, Serra, Szegedy - 2001),

Théorème (Arsovski - 2011)

Plan

Un peu de théorie additive des nombres

Trois résultats ensemblistes dans $\mathbb{F}_p$

Deux problèmes d'ordonnancement

Quelques résultats séquentiels

Une inspiration géométrique

Théorème (Erdős-Ginzburg-Ziv - 1961)

G groupe abélien ($|G| = n$). $(g_1, g_2, \ldots, g_{2n-1})$ suite d'éléments de G.

Théorème (Erdős-Ginzburg-Ziv - 1961)

G groupe abélien ($|G| = n$). $(g_1, g_2, \ldots, g_{2n-1})$ suite d'éléments de G. Il existe $i_1 < i_2 < \cdots < i_n$ tels que:

$$g_{i_1} + g_{i_2} + \cdots + g_{i_n} = 0.$$

Théorème (Erdős-Ginzburg-Ziv - 1961)

G groupe abélien ($|G| = n$). $(g_1, g_2, \ldots, g_{2n-1})$ suite d'éléments de G. Il existe $i_1 < i_2 < \cdots < i_n$ tels que:

$$g_{i_1} + g_{i_2} + \cdots + g_{i_n} = 0.$$

- $\mathbb{Z}/p\mathbb{Z}$, on réordonne dans [0,p-1]:

$$g_1 \leqslant g_2 \leqslant \cdots \leqslant g_{2p-1}.$$

Théorème (Erdős-Ginzburg-Ziv - 1961)

G groupe abélien ($|G| = n$). $(g_1, g_2, \ldots, g_{2n-1})$ suite d'éléments de G. Il existe $i_1 < i_2 < \cdots < i_n$ tels que:

$$g_{i_1} + g_{i_2} + \cdots + g_{i_n} = 0.$$

- $\mathbb{Z}/p\mathbb{Z}$, on réordonne dans [0,p-1]:

$$g_1 \leqslant g_2 \leqslant \cdots \leqslant g_{2p-1}.$$

- Si $g_i = g_{i+p-1}$, on a p termes consécutifs égaux.

Théorème (Erdős-Ginzburg-Ziv - 1961)

G groupe abélien ($|G| = n$). $(g_1, g_2, \ldots, g_{2n-1})$ suite d'éléments de G. Il existe $i_1 < i_2 < \cdots < i_n$ tels que:

$$g_{i_1} + g_{i_2} + \cdots + g_{i_n} = 0.$$

- $\mathbb{Z}/p\mathbb{Z}$, on réordonne dans [0,p-1]:

$$g_1 \leqslant g_2 \leqslant \cdots \leqslant g_{2p-1}.$$

- Si $g_i = g_{i+p-1}$, on a p termes consécutifs égaux.
- Sinon Cauchy-Davenport sur les ensembles $A_i = \{g_i, g_{i+p-1}\}$

Théorème (Erdős-Ginzburg-Ziv - 1961)

G groupe abélien ($|G| = n$). $(g_1, g_2, \ldots, g_{2n-1})$ suite d'éléments de G. Il existe $i_1 < i_2 < \cdots < i_n$ tels que:

$$g_{i_1} + g_{i_2} + \cdots + g_{i_n} = 0.$$

- $\mathbb{Z}/p\mathbb{Z}$, on réordonne dans [0,p-1]:

$$g_1 \leqslant g_2 \leqslant \cdots \leqslant g_{2p-1}.$$

- Si $g_i = g_{i+p-1}$, on a p termes consécutifs égaux.
- Sinon Cauchy-Davenport sur les ensembles $A_i = \{g_i, g_{i+p-1}\}$
- écriture de $-g_{2p-1}$.

Théorème (Erdős-Ginzburg-Ziv - 1961)

Parmi $2n-1$ éléments de C_n, répétitions autorisées, on peut toujours trouver exactement n éléments dont la somme vaut zéro.

Théorème (Erdős-Ginzburg-Ziv - 1961)

Parmi $2n-1$ éléments de C_n, répétitions autorisées, on peut toujours trouver exactement n éléments dont la somme vaut zéro.

Théorème (Reiher - 2007)

Parmi $4n-3$ éléments de C_n^2, répétitions autorisées, on peut toujours trouver exactement n éléments dont la somme vaut zéro.

Théorème (Erdős-Ginzburg-Ziv - 1961)

Parmi $2n-1$ éléments de C_n, répétitions autorisées, on peut toujours trouver exactement n éléments dont la somme vaut zéro.

Théorème (Reiher - 2007)

Parmi $4n-3$ éléments de C_n^2, répétitions autorisées, on peut toujours trouver exactement n éléments dont la somme vaut zéro.

Constante de Davenport G abélien fini, $D(G)$ le plus petit entier tel que toute suite de longueur plus grande contient une sous-suite de somme nulle.

Constante de Davenport G abélien fini, $D(G)$ le plus petit entier tel que toute suite de longueur plus grande contient une sous-suite de somme nulle.

Constante de Davenport G abélien fini, $D(G)$ le plus petit entier tel que toute suite de longueur plus grande contient une sous-suite de somme nulle.

Théorème (Narkiewicz-Rémond - 1966)

Soit $F(x)$ le nombre d'irréductibles de $\mathcal{O}_{\mathbf{K}}$ non associés deux à deux, dont la norme n'excède pas x en valeur absolue. Alors, il existe un réel $C > 0$ tel que l'on ait :

$$F(x) \sim C \frac{x}{\log x} (\log \log x)^{\mathrm{D}(G)-1},$$

où G est le groupe de classes d'idéaux de l'anneau $\mathcal{O}_{\mathbf{K}}$.

Plan

Un peu de théorie additive des nombres

Trois résultats ensemblistes dans $\mathbb{F}_p$

Deux problèmes d'ordonnancement

Quelques résultats séquentiels

Une inspiration géométrique

Une question d'Erdős

Conjecture (Erdős)

p nombre premier, $(a_1, \ldots, a_p)$ éléments de $\mathbb{F}_p^\times$, non tous égaux.
L'équation $a_1x_1 + \cdots + a_px_p = 0$ a au moins p $(0-1)$-solutions.

Une question d'Erdős

Conjecture (Erdős)

p nombre premier, $(a_1, \ldots, a_p)$ *éléments de* $\mathbb{F}_p^\times$, *non tous égaux.*
L'équation $a_1x_1 + \cdots + a_px_p = 0$ *a au moins p* $(0-1)$*-solutions.*

Théorème (Olson - 1987)

G groupe abélien $(|G| = n)$, $(a_1, \ldots, a_n)$ *éléments de* $G \setminus \{0\}$, *non tous égaux.*
L'équation $a_1x_1 + \cdots + a_nx_n = 0$ *a au moins n* $(0-1)$*-solutions.*

Pour $A = (a_1, \ldots, a_\ell)$, on pose

$$\dim(A) = \dim(\langle A^\perp \cap \{0,1\}^\ell \rangle).$$

Pour $A = (a_1, \ldots, a_\ell)$, on pose

$$\dim(A) = \dim(\langle A^\perp \cap \{0,1\}^\ell \rangle).$$

Théorème (B.-Girard)

p un nombre premier, $A = (a_1, \ldots, a_\ell)$ une suite de $\ell > p$ éléments de $\mathbb{F}_p^\times$:

$$\dim(A) = \ell - 1.$$

Théorème (B.-Girard)

$p \in \mathbb{P}$, $A = (a_1, \ldots, a_p)$ une suite de p éléments de $\mathbb{F}_p^\times$:

Théorème (B.-Girard)

$p \in \mathbb{P}$, $A = (a_1, \ldots, a_p)$ une suite de p éléments de $\mathbb{F}_p^\times$:

- $\dim(A) = 1$,
$$(a_1, \ldots, a_p) = (r, \ldots, r).$$

Théorème (B.-Girard)

$p \in \mathbb{P}$, $A = (a_1, \ldots, a_p)$ une suite de p éléments de $\mathbb{F}_p^\times$:

- $\dim(A) = 1$,
$$(a_1, \ldots, a_p) = (r, \ldots, r).$$
- $\dim(A) = p - 2$, $\exists t \in [1, p-3]$,
$$(a_{\sigma(1)}, \ldots, a_{\sigma(p)}) = (\underbrace{r, \ldots, r}_{t}, \underbrace{-r, \ldots, -r}_{p-2-t}, -(t+1)r, -(t+1)r).$$

Théorème (B.-Girard)

$p \in \mathbb{P}$, $A = (a_1, \ldots, a_p)$ une suite de p éléments de $\mathbb{F}_p^\times$:

- $\dim(A) = 1$,
$$(a_1, \ldots, a_p) = (r, \ldots, r).$$
- $\dim(A) = p-2$, $\exists t \in [1, p-3]$,
$$(a_{\sigma(1)}, \ldots, a_{\sigma(p)}) = (\underbrace{r, \ldots, r}_{t}, \underbrace{-r, \ldots, -r}_{p-2-t}, -(t+1)r, -(t+1)r).$$
- $\dim(A) = p-1$.