Introduction à la théorie additive des nombres. Problèmes inverses.

1. Principes, Histoire et problèmes fondamentaux.

2. Résultats généraux. Outils de base.

3. Addition d'ensembles infinis. Densités.

4. Présentation de la méthode isopérimétrique.

Le problème de Waring.

- 1621: Bachet énonce sans démonstration: Tout entier est somme de quatre carrés.
- 1770: Waring émet la conjecture suivante:

  Conjecture 1 *Soit $n \geq 2$ un entier. Soit $A_n := \{0, 1^n, 2^n, \ldots\}$. Il existe un entier k tel que $\mathbb{N} = kA_n$. On note $g(n)$ le plus petit de ces entiers k.*

  Lagrange donne une démonstration de $g(2) = 4$.
- 1909: Hilbert prouve la conjecture de Waring.
- 1912: Wieferich et Kempner prouvent que $g(3) = 9$.
- 1964: Chen prouve que $g(5) = 37$.
- 1960-1970: On obtient l'expression $g(n) = 2^n + [(3/2)^n] - 2$ pour tout $6 \leq n \leq 471600000$.
- 1986: Balasubramanian, Deshouillers et Dress obtiennent $g(4) = 19$.

Définition 1 *Soit $n \geq 2$ un entier. On note $G(n)$ le plus petit entier k tel que $\mathbb{N} \setminus kA_n$ soit fini.*

Exemple 1 $G(3) \leq 7$ *et* $G(4) = 16$.

La conjecture de Goldbach.

- 1742: Dans une correspondance entre Goldbach et Euler, on trouve les conjectures suivantes:

  Conjecture 2 *Tout entier pair $n \geq 4$ est la somme de deux nombres premiers.*

  Conjecture 3 *Tout entier impair $n \geq 7$ est la somme de trois nombres premiers.*

- 1855: Desboves vérifie (2) pour $n < 10000$.
- 1923: Hardy et Littlewood montrent (3) pour $n > 10^{32}$ en supposant HRG (constante obtenue en 1926 par Lucke)
- 1937: Vinogradov montre (3) pour $n > 10^{7000000}$, constante ramenée à 10^{43000} par Chen et Wang récemment.
- 1997: Deshouillers, Effinger, Riele et Zinoviev montrent (3) sous HRG.
- 1998: Deshouillers, Riele et Saouter montrent sous HR que tout nombre pair est la somme d'au plus 4 nombres premiers et vérifient (2) pour $n < 10^{14}$.

Ensembles sans solution non triviale à une équation.

On notera toujours $r(n)$ la taille maximale d'un ensemble sans solution non triviale à (E) inclus dans $\{1, \ldots, n\}$.

Ensembles sum-free

$$(E) : x + y = z$$

Théorème 1

$$r(n) = \left[\frac{n+1}{2} \right].$$

Ensembles de Sidon

$$(E) : x + y = z + t$$

Théorème 2

$$\lim_{n \to \infty} \frac{r(n)}{\sqrt{n}} = 1.$$

Ensembles sans progression arithmétique

$$(E) : x + y = 2z$$

Théorème 3 (Roth) $r(n) = O(\frac{n}{\ln \ln(n)})$.

Addition d'ensembles infinis.Densités.

Soit A un ensemble d'entiers naturels.

Définition 2 *On appelle densité de Schnirelmann de A et on note $\sigma(A)$ la quantité*

$$\sigma(A) := \inf_{n \in \mathbb{N}} \frac{|A \cap [0; n]|}{n}.$$

Définition 3 *On appelle densité asymptotique inférieure et on note $\underline{d}(A)$ la quantité*

$$\underline{d}(A) := \liminf_{n \to \infty} \frac{|A \cap [0; n]|}{n},$$

et densité asymptotique supérieure la quantité

$$\overline{d}(A) := \limsup_{n \to \infty} \frac{|A \cap [0; n]|}{n}.$$

Si $\underline{d}(A) = \overline{d}(A)$, on appelle densité asymptotique et on note $d(A) := \underline{d}(A) = \overline{d}(A)$.

Définition 4 *On dit que A est une base d'ordre h si $hA = \mathbb{N}$.*
On dit que A est une base asymptotique d'ordre h si $\mathbb{N} \setminus hA$ est fini.

Lemme 1 $\sigma(A) > 0 \Longleftrightarrow 1 \in A$ *et* $\underline{d}(A) > 0$.

Proposition 1 *Si $0 \in A \cap B$, alors*

$$\sigma(A + B) \geq \sigma(A) + \sigma(B) - \sigma(A)\sigma(B).$$

Proposition 2 *Si $0 \in A$ et $\sigma(A) > 0$, A est une base d'ordre fini.*

Proposition 3 *Si $0 \in A$, $\gcd(A) = 1$ et $\underline{d}(A) > 0$, alors A est une base asymptotique d'ordre fini.*

Théorème 4 *Soit P l'ensemble des nombres premiers. On a $\underline{d}(2P) > 0$.*

Théorème 5 (Schnirelmann) *Il existe une constante C telle que tout entier est la somme d'au plus C nombres premiers.*

Soit A un ensemble d'entiers. Soit $\varepsilon > 0$.

Théorème 6 (Kneser) *Si $\underline{d}(A+A) \leq (2-\varepsilon)\underline{d}(A)$, alors A est un gros sous-ensemble d'une union de classes résiduelles modulo un entier N.*

Théorème 7 (Freiman) *Si $0 \in A$, $\gcd(A) = 1$ et $\underline{d}(A) < \alpha_0$, avec $\alpha_0 < \frac{1}{2}$ fixé. Si $\underline{d}(A+A) \leq (2-\varepsilon)\underline{d}(A)$, alors A est un gros sous-ensemble d'une union de classes résiduelles modulo un entier N, de plus ces classes sont en progression arithmétique.*

Théorème 8 *Soit $0 \in A$, $\gcd(A) = 1$, et $\overline{d}(A) < \frac{1}{2}$. Alors, $\overline{d}(A+A) \geq \frac{3}{2}\overline{d}(A)$.*

Théorème 9 *Si $0 \in A$, $\gcd(A) = 1$ et $\underline{d}(A) < \alpha_0$, avec $\alpha_0 < \frac{1}{2}$ fixé. Si $\overline{d}(A+A) \leq (\frac{5}{3}-\varepsilon)\overline{d}(A)$ avec $\frac{1}{18} \leq \varepsilon \leq \frac{1}{6}$, alors on est dans un des deux cas suivants:*

- *<u>Cas non archimédien:</u> il existe $N \in \mathbb{N}$ et t premier à N tels que*

$$\alpha \geq \frac{18}{(11-12\varepsilon)N}$$

et

$$A \subseteq \{iN; i \in \mathbb{N}\} \cup \{t+iN; i \in \mathbb{N}\}.$$

- <u>Cas archimédien:</u> il existe une suite croissante d'entiers $(y_j)_{j\geq 1}$ avec

$$\lim_{j\to\infty} \frac{A(y_j)}{y_j} = \alpha,$$

et deux suites $(b_j)_{j\geq 1}$ et $(t_j)_{j\geq 1}$ avec $0 \leq b_j \leq t_j \leq y_j$ telles que, si on note

$$\sigma := \frac{5}{3} - \varepsilon,$$

et

$$\lambda_j := \frac{b_j}{y_j - t_j},$$

on a $A(b_j, t_j) = 0$ pour tout $j \geq 1$, et

$$\lambda := \lim_{j\to\infty} \lambda_j \leq \frac{2\sigma - 3}{2\sigma - 2}\Big(\frac{1}{2\sigma - 2} - \alpha\Big)^{-1},$$

$$\lim_{j\to\infty} \frac{A(t_j, y_j)}{y_j - t_j + 1} \geq \Big(\frac{1}{2\sigma - 2} + \lambda\big(\frac{1}{2\sigma - 2} - \alpha\big)\Big).$$