Progressions arithmétiques dans l'ensemble des nombres premiers

Reims - Sém JC
21 - 11 - 2014

1. Quelques propriétés (bien connues) de l'ensemble des nb premiers

Thm (Euclide) L'ensemble des nb premiers $\mathbb{P}$ est infini.

dém (Furstenberg - 1955 - durant ses années d'études)

On utilise les progressions arithmétiques : $S(a,b) = a\mathbb{Z} + b$ $(a \neq 0)$.

On définit sur $\mathbb{Z}$ la topologie ayant pour base d'ouverts les $S(a,b)$.

Pour cette topologie : $S(a,b) = \mathbb{Z} \setminus \left(\coprod_{j=1}^{a-1} S(a, b+j) \right)$ est aussi fermé.

OR $\mathbb{Z} \setminus \{-1, 1\} = \bigcup_{p \in \mathbb{P}} S(p, 0)$ est une union de fermés.

Si $\mathbb{P}$ est fini, $\mathbb{Z} \setminus \{-1,+1\}$ est serait fermé et $\{-1,1\}$ ouvert.

↳ impossible car $\{-1,1\}$ est fini !

■

Pb de la répartition des nombres premiers dans $\mathbb{Z}$

comportement presque aléatoire :

→ nb premiers jumeaux (p_1, p_2) tq $p_2 - p_1 = 2$.

exple $(3,5)$, $(17,19)$, $(857,859)$ ... on connait des nb premiers jumeaux à plus de 58000 chiffres !

Conjecture Il existe une infinité de nb premiers jumeaux.

→ À l'opposé : $\forall N \geq 1$, $\exists$ un intervalle d'entiers de longueur N ne contenant aucun nb premiers :

$[\![(N+1)! + 2 \,;\, \dots \,;\, (N+1)! + N+1]\!]$.

→ Thm de la progression arithmétique

$\forall n, m \in \mathbb{N}^*$, $\mathrm{pgcd}(n,m) = 1$, l'ensemble $(n + \mathbb{N}m) \cap \mathbb{P}$ est infini.

prop (Euler - 1737) $\displaystyle\sum_{p \in \mathbb{P}} \frac{1}{p} = +\infty$.

dém Fonction zêta de Riemann $\forall s > 1$, $\displaystyle\zeta(s) = \sum_{n=1}^{+\infty} \frac{1}{n^s}$

Faits . $\displaystyle\lim_{s \to 1^+} \zeta(s) = +\infty$.

. Produit Eulerien. $\displaystyle\zeta(s) = \prod_{p \in \mathbb{P}} \left(\frac{1}{1 - p^{-s}} \right)$ → lien entre nb premiers et fonction ζ.

On en déduit $\displaystyle\ln(\zeta(s)) = \ln\left(\prod_{p \in \mathbb{P}} \frac{1}{1 - p^{-s}} \right) \underset{(*)}{\leq} 2 \sum_{p \in \mathbb{P}} p^{-s}$.

Où $(*)$ provient de l'inég. des acc finis : $\displaystyle -\frac{\ln(1-x)}{x} \leq 2 \quad \forall x \in]0, \tfrac{1}{2}]$

soit puisque $\displaystyle\sum_{p \in \mathbb{P}} p^{-s} \leq \sum_{p \in \mathbb{P}} p^{-1}$: $\displaystyle\ln(\zeta(s)) \leq 2 \sum_{p \in \mathbb{P}} \frac{1}{p}$

et on passe à la limite quand $s \to 1^+$

$\blacksquare$

Thm des nb premiers (Hadamard - La Vallée - Poussin - 1896)

$$\pi(N) \underset{N \to +\infty}{\sim} \frac{N}{\ln(N)}$$

Où $\pi(N) = \mathrm{Card} \{ p \text{ premier}, p \leq N \}$

dém Repose sur le fait que (le prolongement de) ζ ne s'annule pas sur $\mathrm{Re}(s) = 1$.

Conséquence La densité des nombres premiers dans $\mathbb{N}$ est nulle :

$$\lim_{N \to +\infty} \frac{\pi(N)}{N} = 0.$$

II Progressions arithmétiques dans l'ensemble des nb premiers

On l'a vu, les nb premiers ont un comportement quasi-aléatoire. Cependant certains sous-ensembles de $\mathbb{P}$ ont une structure algébrique élémentaire, celle d'être en progression arithmétique.

exple · Progression arithmétique de longueur 3 : $(3,5,7)$

· de longueur 5 : $(5, 11, 17, 23, 29)$

· de longueur 6 : $(7, 157, 307, 457, 607, 757)$

...

· de longueur 26 (12 avril 2010 - 75 ordinateurs pour l'obtenir)

$$43,142,746,595,714,191 + 23,681,770 \times 223,092,870 \times n$$

$$n = 0, \dots, 25.$$

question Progressions arithmétiques de longueur infinie dans $\mathbb{P}$?

NON : si $a\mathbb{N}+b \subseteq \mathbb{P}$ $(a \neq 0)$ alors la densité de $\mathbb{P}$ dans $\mathbb{N}$ serait $> \frac{1}{a}$ ...

Thm (Green-Tao-2004) L'ensemble $\mathbb{P}$ contient des progressions arithmétiques de toutes longueurs.

Terence Tao (UCLA) a notamment obtenu la médaille Fields en 2006 pour ces travaux.

Idée de la démonstration Elle repose sur trois points

1) Thm (Szemerédi-1975) Tout ensemble d'entiers de densité > 0 contient des progressions arithmétiques de toutes longueurs.

Version finie $\forall k \geq 2$ et $\delta > 0$, $\exists$ un entier $N = N(k,\delta)$ tq tout sous-ensemble E de $[0, N]$ tq $\mathrm{Card}(E) \geq \delta N$ contienne une prog. arithmétique de longueur $k+1$.

⇝ démonstration ergodique de ce résultat par Furstenberg dont Tao et Green s'inspirent.

<u>Problème</u> $\mathbb{P}$ est de densité nulle dans $\mathbb{N}$, et le Thm de Szemerédi ne s'applique pas à cette situation.

2) <u>Reformulation du Thm de Szemerédi</u>

$\mathrm{Card}(E)/N \geq \delta$ peut être vu comme la moyenne de $\mathbb{1}_E$ sur $[\![0,N[\![$

ie $E(\mathbb{1}_E \mid [\![0,N[\![)$

d'où la nouvelle formulation du Thm de S.

<u>Thm</u> Pour tout $\delta > 0$, il existe une constante $c(\delta) > 0$ tq, pour toute fonction $f : [\![0,N[\![\to \mathbb{R}$ avec

$0 \leq f(x) \leq 1$ pour tout x et $E(f \mid [\![0,N[\![) \geq \delta$

On a

$$E(f(x)f(x+t)\dots f(x+kt) \mid x,t \in [\![0,N[\![) \geq c(\delta)$$

⇝ On retrouve le thm de S en prenant $f = \mathbb{1}_E$ avec E de densité > 0

<u>Pb</u> Si on prend une fonction nulle en dehors de $\mathbb{P}$, majorée par 1,

$$E(f/\mathbb{N}) = 0.$$

G et T s'en affranchissent en remplaçant la condition $f \leq 1$ par $f \leq \nu$ où $\nu : [\![0,N[\![\to \mathbb{R}^+$ poids pseudo aléatoire (satisfaisant deux conditions asymptotiques). ⇝ $0 \leq f(x) \leq \nu(x)$

3) Construire f et ν tq :
- f est nulle en dehors de $\mathbb{P}$
- $0 \leq f(x) \leq \nu(x) \quad \forall x.$
- $E(f \mid [\![0,N[\![) \geq \delta$

↳ Théorie des nombres (fonction de Von Mangoldt).

Deux problèmes ouverts sur ce sujet :

<u>Conjecture</u> (Erdős et Turán - 1936) Supposons que $A = \{a_1 < a_2 < \dots\}$ est une suite infinie d'entiers > 0 tq $\sum \frac{1}{a_i} = +\infty$.
Alors A contient des progressions arithmétiques de longueur arbitraire.

↳ Thm de GT : preuve de cette conjecture pour $A = \mathbb{P}$.

<u>Conjecture</u> (Hardy et Littlewood) Le nb de progressions arithmétiques de nombres premiers de longueur k est asymptotiquement

$$C_k \, N^2 / \log^k(N) \quad \text{pour } C_k > 0 \text{ explicite.}$$

III Progressions polynomiales dans l'ensemble $\mathbb{P}$

<u>Thm</u> (Tao - Ziegler - 2008) Soient $P_1, \dots, P_k \in \mathbb{Z}[X]$ tq $P_1(0) = \dots = P_k(0) = 0$.
Alors il existe une infinité d'entiers x, m tq

$$x + P_1(m), \dots, x + P_k(m) \in \mathbb{P}.$$

<u>Cas particuliers</u> (i) $P_1(X) = X, \dots, P_k(X) = kX$ ↝ on obtient le thm de GT - 2004.

(ii) $P_1(X) = X^2, \dots, P_k(X) = kX^2$: existence de progressions arithmétiques dans $\mathbb{P}$ de n'importe quelle longueur dont <u>la raison est un carré</u>.