RAMDINMAWIA

Le 13 novembre, 2012

Première partie

Le théorème de Roth

Quelques définitions, notations et remarques :

(1) **Notation :** Pour un ensemble fini A, la **cardinalité** de A sera notée $|A|$.

(2) **Notation :** Le disque unité fermé de $\mathbb{C}$ sera noté $\overline{\mathbb{D}}$. Ainsi $\overline{\mathbb{D}} = \{z \in \mathbb{C} : |z| \leq 1\}$.

(3) **Notation :** Pour un réel x, on note $\lfloor x \rfloor$ le plus grand entier $\leq x$, et on note $\lceil x \rceil$ le plus petit entier $\geq x$.

(4) **Notation :** Pour deux entiers a et b avec $a \leq b$, on écrit

$$\begin{aligned}
[a,b] &= \{a, a+1, \cdots, b\} \\
[a,b[&= \{a, \cdots, b-1\} \\
]a,b] &= \{a+1, \cdots, b\} \\
]a,b[&= \{a+1, \cdots, b-1\}.
\end{aligned}$$

(5) **Définition :** Pour une fonction

$$f : \mathbb{Z}_N \to \mathbb{C}$$

on définit

$$\hat{f}(r) = \sum_{s \in \mathbb{Z}_N} f(s)\omega^{-rs}$$

où $\omega = e^{\frac{2\pi i}{N}}$.

(6) **Définition :** Si A, B sont deux parties d'un ensemble X, on appellera la ***densité de** A **dans** B* la quantité $\frac{|A \cap B|}{|B|}$.

(7) **Définition :** Si $A \subset [1, N]$ est de taille δN, (c-à-d si $|A| = \delta N$), alors la fonction **équilibrée** de A est définie par

$$f_A(x) = A(x) - \delta, \qquad (x \in \mathbb{Z}_N)$$

où on confond un ensemble et sa fonction indicatrice. (Ainsi $A(x) = 0$ si $x \notin A$ et $A(x) = 1$ si $x \in A$.)

(8) **Définition :** Une application

$$\phi : B \to \mathbb{Z}_N$$

(où $B \subset \mathbb{Z}_N$) est dite **affine** si elle a la forme $\phi(x) = ax + b$.

(9) **Définition :** Le **diamètre** d'un sous-ensemble $X \subset \mathbb{Z}_N$ de $\mathbb{Z}_N$ est le plus petit entier d tel que

$$X \subset [n, n+d]$$

pour un certain $n \in \mathbb{Z}_N$. On le note $\mathsf{diam}\, X$.

(10) **Définition :** Pour nous, une ***progression arithmétique*** ou une ***suite arithmétique*** sera un ensemble $P \subset \mathbb{N}$ de la forme $P = \{a, a+d, \cdots, a+(n-1)d\}$ avec $a, d, n \in \mathbb{N}$. Les entiers a et $a+(n-1)d$ sont les ***extrémités***, d la ***raison***, et n la ***longueur*** de la progression. On appelle la différence $a+(n-1)d - a = (n-1)d$ entres les extrémités l'**envergure**, ou l'**écart total** de la progression. Il est facile à voir que P est l'image sous l'application $\phi(x) = dx + a$ de l'ensemble $[1, n-1]$. Dans ce cas, l'ensemble $[1, n-1]$ (qui est lui aussi une progression arithmétique) sera appelé le ***principe*** de P. Pareillement, si A est une partie de P, l'image réciproque $\phi^{-1}(A)$ de A sous ϕ sera appelée le ***principe*** de A. Donc le principe de A est $\{t : dt + a \in A\}$. Réciproquement, P est l'**image** de son principe, et A celle de son principe.

(11) **Définition :** Une ***sous-progression arithmétique*** d'une progression arithmétique P est une partie $S \subset P$ qui est aussi une progression arithmétique. Un ***segment*** de P est une sous-progression de P *de même raison.*

(12) **Remarque :** Il est facile à montrer que

$$\hat{f}_A(r) = \hat{A}(r)$$

pour $r \neq 0$ et $\hat{f}_A(0) = 0$.

(13) **Remarque :** Le diamètre d'une progression arithmétique $P = \{a, a+d, \cdots, a+nd\}$ est au plus nd ; c'est-à-dire diam $P \leq nd$, ce qui est égale à l'envergure de la progression.

(14) **Remarque :** Si $q = \frac{n}{m}$ est un rationnel non négatif ($m, n \in \mathbb{N}, m > 0$) alors $n = mq = m\{q\}\left\lceil \frac{n}{m} \right\rceil + m(1-\{q\})\left\lfloor \frac{n}{m} \right\rfloor$, où $\{x\}$ dénote la partie fractionnaire d'un réel x ; c'est à noter que $m\{q\}$ est un entier.

LEMME 1. *Soit $m \leq n$ deux entiers, et E un ensemble de cardinalité n. Alors E admet une partition en l parties $E_1, \cdots, E_l$ ($\frac{n}{m} \leq l \leq \left\lceil \frac{n}{m} \right\rceil$) telles que $\frac{m}{2} \leq |E_j| \leq m \forall j$ et $||E_i| - |E_j|| \leq 1 \forall i, j$.*

DÉMONSTRATION. Posons $q = \left\lfloor \frac{n}{m} \right\rfloor$. Si m divise n, alors il est évident que E peut être partitionné en $q = \frac{n}{m}$ parties, chacune de cardinalité m. Donc on suppose que $m \nmid n$. Puisque $n = (q+1)\left(\frac{n}{q+1}\right)$ et $\frac{m}{2} \leq \frac{n}{q+1} \leq \frac{n}{\frac{n}{m}+1} < m$ on voit bien qu'il est possible de partitionner E en $q+1 = \left\lfloor \frac{n}{m} \right\rfloor + 1 = \left\lceil \frac{n}{m} \right\rceil$ parties $E_0, \cdots, E_q$ telles que $|E_j| = \left\lfloor \frac{n}{\frac{n}{m}+1} \right\rfloor = \left\lfloor \frac{mn}{m+n} \right\rfloor$ ou $|E_j| = \left\lceil \frac{mn}{m+n} \right\rceil$ ($j = 0, \cdots, q$) (par la remarque (9)).

□

LEMME 2. *Soit $\phi : \mathbb{Z}_N \to \mathbb{Z}_N$ une application affine et soient $r, s \leq N$ avec $rs \geq N$. Alors pour un certain $m \leq \sqrt{\frac{8rN}{s}}$ on peut partitionner l'ensemble $[0, r-1]$ en m progressions arithmétiques $P_1, \cdots, P_m$ telles que*

(1) $\frac{1}{2}\sqrt{\frac{rs}{N}} \leq |P_j| \leq \sqrt{\frac{rs}{N}}$.

(2) diam $\phi(P_j) \leq s \forall j$ et

$$||P_j| - |P_k|| \leq 1 \forall j, k. \tag{0.0.1}$$

DÉMONSTRATION. Soit $t = \left\lfloor \sqrt{\frac{rN}{s}} \right\rfloor$. Évidemment, $\sqrt{r} \leq t \leq r$. Parmi les entiers $\phi(0), \cdots, \phi(t)$ on peut trouver au moins une paire j, k telle que $|\phi(j) - \phi(k)| \leq \frac{N}{t}$ (par le principe du tiroir). Par l'*affinité* de ϕ on peut donc trouver un $u \leq t$ tel que $|\phi(u) - \phi(0)| \leq \frac{N}{t}$. On partitionne $[0, r-1]$ en u classes de reste modulo u, disons $C_0, \cdots, C_{u-1}$ où $v \equiv j \bmod u$ pour tout $v \in C_j$. Il est évident que

□

(1) **Fait 1.** Chaque classe C_j ($j = 0, \cdots, u-1$) est une progression arithmétique.

(2) **Fait 2.** C_j est de la forme $C_j = \{j, u+j, 2u+j, \cdots, (n_j-1)u+j\}$ avec $\left\lfloor \frac{r}{u} \right\rfloor \leq n_j = |C_j| \leq \left\lceil \frac{r}{u} \right\rceil$ ($j = 0, \cdots, u-1$) et, par conséquent,

(3) **Fait 3.** $||C_j| - |C_k|| \leq 1$ pour tous $j, k = 0, 1, \cdots, u-1$.

Maintenant on a $ut \leq t^2 \leq \frac{rN}{s}$ d'où $\frac{st}{N} \leq \frac{r}{u}$. Posons $l = \lfloor st/N \rfloor$. Alors on a $l \leq |C_j|$ pour tout j. Soit P un segment de C_j de longueur $\leq l$, disons $P = \{a_1u+j, \cdots, (a_1+q-1)u+j\}$ où $q \leq l$. Alors

$$\begin{aligned} \phi(P) &= \{a(a_1u+j)+b, \cdots, a((a_1+q-1)u+j)+b\} \\ &= \{a_1(au)+(aj+b), \cdots, (a_1+q-1)(au)+(aj+b)\}. \end{aligned}$$

(Ici on prend $\phi(x) = ax + b$). On voit bien que $\phi(P)$ est une progression arithmétique de raison au et d'envergure $(q-1)au$. Par la remarque (6) dessus, son diamètre $\mathsf{diam}\ \phi(P) \leq (q-1)au < lau \leq \frac{st}{N}au$. Maintenant, on sait que $|\phi(u) - \phi(0)| \leq \frac{N}{t}$, i.e., $au \leq \frac{N}{t}$. Donc

$$\mathsf{diam}\ \phi(P) \leq \frac{st}{N}au \leq \frac{st}{N}\frac{N}{t} = s.$$

Donc pour un tel P, il est toujours vrai que $\mathtt{diam}\ \ \phi(P) \leq s$.

Maintenant, comme $\frac{st}{N} \leq \frac{r}{u}$, la remarque (7) et le lemme (1) nous montrent qu'on peut partitionner chaque C_j en moins de $\kappa = \left\lceil \frac{\lceil \frac{r}{u} \rceil}{\lfloor \frac{st}{N} \rfloor} \right\rceil \leq \frac{2rN}{stu}$ sous-progressions arithmétiques $Q_1^j, \cdots, Q_{\nu_j}^j$ (où $\nu_j \leq \kappa$) de longueurs entre $\frac{1}{2}\left\lfloor \frac{st}{N} \right\rfloor$ et $\left\lfloor \frac{st}{N} \right\rfloor$ telles que

$$\left| \left| Q_{n_1}^j \right| - \left| Q_{n_2}^j \right| \right| \leq 1 \quad \forall 1 \leq n_1, n_2 \leq \nu_j.$$

Comme on a u classes (à savoir $C_0, \cdots, C_{u-1}$), on voit donc qu'on a au plus $\rho := u\frac{2rN}{stu} = \frac{2rN}{st} \leq \frac{2rN}{s\sqrt{\frac{rN}{2s}}} = \sqrt{\frac{8rN}{s}}$ telles progressions arithmétiques, appelons-les $P_1, \cdots, P_m$ où $m \leq \rho$. Comme les longueurs de deux classes C_i et C_j diffèrent d'au plus 1, on voit bien que les inéquations (0.0.1) sont satisfaites. $\square$

COROLLAIRE 3. *Soit $f : [0, r-1] \to \overline{\mathbb{D}}$ une application de $[0, r-1]$ dans le disque unité fermé de $\mathbb{C}$, et soit $\phi : \mathbb{Z}_N \to \mathbb{Z}_N$ affine. On suppose que $\alpha > 0$. Si*

$$\left| \sum_{x=0}^{r-1} f(x)\omega^{-\phi(x)} \right| \geq \alpha r,$$

alors on peut partitionner $[0, r-1]$ en $m \leq \sqrt{\frac{32\pi r}{\alpha}}$ progressions arithmétiques $P_1, \cdots, P_m$ telles que

$$\sum_{j=1}^{m} \left| \sum_{x \in P_j} f(x) \right| \geq (\frac{\alpha}{2})r$$

et que $\frac{1}{4}\sqrt{\frac{\alpha r}{\pi}} \leq |P_j| \leq \frac{1}{2}\sqrt{\frac{\alpha r}{\pi}}$.

DÉMONSTRATION. Prenons $s = \frac{\alpha N}{4\pi}$. Par le lemme (2), pour un certain $m \leq \sqrt{\frac{8rN}{s}} \leq \sqrt{\frac{32\pi r}{\alpha}}$, on peut partitionner $[0, r-1]$ en m progressions arithmétiques $P_1, \cdots, P_m$ telles que

1. $\frac{1}{2}\sqrt{\frac{rs}{N}} \leq |P_j| \leq \sqrt{\frac{rs}{N}}$ (ce qui est équivalent à $\frac{1}{4}\sqrt{\frac{\alpha r}{\pi}} \leq |P_j| \leq \frac{1}{2}\sqrt{\frac{\alpha r}{\pi}}$)

2. diam $\phi(P_j) \leq s \forall j$.

Maintenant, par l'inégalité triangulaire, on a

$$\sum_{j=1}^{m} \left| \sum_{x \in P_j} f(x)\omega^{-\phi(x)} \right| \geq \alpha r.$$

Pour tout $x_j \in P_j$, on a $\left|\omega^{-\phi(x)} - \omega^{-\phi(x_j)}\right| \leq \frac{2\pi}{N}\mathsf{diam}\ \phi(P_j) \leq \frac{2\pi}{N} s \leq \frac{2\pi}{N}\frac{\alpha N}{4\pi} = \frac{\alpha}{2}$. Donc

$$\begin{aligned}
\sum_{j=1}^{m}\left|\sum_{x\in P_j} f(x)\right| &= \sum_{j=1}^{m}\left|\sum_{x\in P_j} f(x)\omega^{-\phi(x_j)}\right| \\
&= \sum_{j=1}^{m}\left|\sum_{x\in P_j} f(x)\omega^{-\phi(x)} + \sum_{x\in P_j} f(x)(\omega^{-\phi(x_j)} - \omega^{-\phi(x)})\right| \\
&\geq \sum_{j=1}^{m}\left|\sum_{x\in P_j} f(x)\omega^{-\phi(x)}\right| - \sum_{j=1}^{m}\left|\sum_{x\in P_j} f(x)(\omega^{-\phi(x_j)} - \omega^{-\phi(x)})\right| \\
&\geq \alpha r - \sum_{j=1}^{m}\sum_{x\in P_j}|f(x)|\left|\omega^{-\phi(x_j)} - \omega^{-\phi(x)}\right| \\
&\geq \alpha r - \sum_{j=1}^{m}|P_j|\frac{\alpha}{2} \\
&= \alpha r - r\frac{\alpha}{2} \\
&= \frac{\alpha}{2} r.
\end{aligned}$$

□

Corollaire 4. *(**Lemme d'augmentation de densité**) Soit $A \subset \mathbb{Z}_N$. Si $\left|\hat{A}(a)\right| \geq \alpha N$ pour un certain $a \neq 0$, alors on peut trouver une progression arithmétique $P \subset [0, N-1]$ de longueur au moins $\sqrt{\frac{\alpha N}{16\pi}}$ telle que $|A \cap P| \geq (\delta + \frac{\alpha}{8\sqrt{2}})\,|P|$.*

Démonstration. Prenons

$$\begin{aligned}
\phi : \mathbb{Z}_N &\to \mathbb{Z}_N. \\
x &\mapsto ax
\end{aligned}$$

Soit f la fonction équilibrée de A. L'hypothèse nous dit que $\left|\sum_{x=0}^{N-1} f(x)\omega^{-\phi(x)}\right| = |\sum_{x=0}^{N-1} f(x)\omega^{-ax}| \geq \alpha N$. Donc, par le corollaire précédent (Corollaire (3)), on peut partitionner l'ensemble $[0, N-1]$ en $m \leq \sqrt{\frac{32\pi N}{\alpha}}$ progressions arithmétiques $P_1, \cdots, P_m$ de longueurs entre $\frac{1}{4}\sqrt{\frac{\alpha N}{\pi}}$ et $\frac{1}{2}\sqrt{\frac{\alpha N}{\pi}}$ telles que $\mathsf{diam}\ \phi(P_j) \leq \frac{\alpha N}{4\pi}$ et

$$\sum_{j=1}^{m}\left|\sum_{x\in P_j} f(x)\right| \geq (\frac{\alpha}{2})N.$$

Puisque l'application f est réelle et $\sum_{j=1}^{m}\sum_{x\in P_j} f(x) = 0$, on voit facilement que

$$\sum_{j\in J}\sum_{x\in P_j} f(x) \geq \frac{\alpha N}{4},$$

où $J = \{j : \sum_{x\in P_j} f(x) \geq 0\}$. Donc

$$\sum_{x\in P_j} f(x) \geq \frac{\alpha N}{4\,|J|} \geq \frac{\alpha N}{4m}$$

pour au moins un $j \in J$. Puisque $|P_j| \leq \frac{1}{2}\sqrt{\frac{\alpha N}{\pi}} \leq \frac{2\sqrt{2}N}{m}$, on a

$$\sum_{x \in P_j} f(x) \geq \frac{\alpha N}{4m} = \frac{2\sqrt{2}N}{m}\frac{\alpha}{8\sqrt{2}} \geq |P_j|\,\frac{\alpha}{8\sqrt{2}}. \tag{0.0.2}$$

Mais, par la définition de f, on a $\sum_{x\in P_j} f(x) = |A \cap P_j|\,(1-\delta) + (|P_j| - |A \cap P_j|)(-\delta) = |A \cap P_j| - |P_j|\,\delta$. Donc l'inégalité (0.0.2) implique que

$$|A \cap P_j| \geq (\delta + \frac{\alpha}{8\sqrt{2}})\,|P_j|\,.$$

Finalement, on constate que $|P_j| \geq \frac{1}{4}\sqrt{\frac{\alpha N}{\pi}}$.

□

THÉORÈME 5. **(Théorème de Roth, [G2])** *Soit $\delta > 0$. Si $N \geq \exp\exp(c\delta^{-1})$ (où c est une constante absolue) et $A \subset [1, N]$ est une partie de $[1, N]$ de taille $\geq \delta N$, alors A contient une progression arithmétique de longueur trois.*

DÉMONSTRATION. Soit A_0 une partie de $[1, N_0]$ de taille $\geq \delta_0 N_0$, et soit p un nombre premier entre $\frac{N_0}{3}$ et $\frac{2N_0}{3}$.

AFFIRMATION 6. **Notre but :** On va montrer que même si A_0 ne contient pas de progression arithmétique de longueur trois, on peut toujours trouver une progression arithmétique $P \subset [1, N_0]$ de longueur $\geq \sqrt{\frac{\delta^2 N}{160\pi}} \geq \sqrt{\frac{\delta^2 N_0}{480\pi}}$ (avec $\delta = \delta_0(1 - \frac{\delta_0}{160})$) telle que $|A_0 \cap P| \geq \delta_0(1 + \frac{\delta_0}{320})\,|P|$.

□

Cas 1. Si $|A_0 \cap [1, p]| \leq \delta_0(1 - \frac{\delta_0}{160})p$ alors on a

$$\begin{aligned} |A_0 \cap [p+1, N_0]| &\geq \delta_0 N_0 - \delta_0(1 - \frac{\delta_0}{160})p \\ &= \delta_0(N_0 - p + \frac{\delta_0}{160}p) \\ &\geq \delta_0(1 + \frac{\delta_0}{320})(N_0 - p) \qquad (\because p \geq \frac{N_0 - p}{2}). \end{aligned}$$

Pour ce cas, on a donc trouvé une progression arithmétique $P = [p+1, N_0] \subset [1, N_0]$ de longueur $N_0 - p \geq N_0 - \frac{2N_0}{3} = \frac{N_0}{3}$ telle que $|A_0 \cap P| \geq \delta_0(1 + \frac{\delta_0}{320})\,|P|$.
▲

Cas 2. Si $|A_0 \cap [1, p]| > \delta_0(1 - \frac{\delta_0}{160})p$, soient $N = p$, $A = A_0 \cap [1, N]$ et $\delta = \delta_0(1 - \frac{\delta_0}{160})$. Posons $B = A \cap [\frac{N}{3}, \frac{2N}{3}[$ et $\alpha = \frac{\delta^2}{10}$.

Cas i. $|\mathbf{B}| \leq \frac{\delta \mathbf{N}}{\mathbf{5}}$. Supposons que $|B| \leq \frac{\delta N}{5}$. Alors, il est clair qu'au moins un des nombres $\left|A \cap [1, \frac{N}{3}[\right|$ et $\left|A \cap [\frac{2N}{3}, N]\right|$ est supérieur ou égal à $\frac{2\delta N}{5}$. Donc on a trouvé une progression arithmétique $P \subset [1, N_0]$ de longueur $\frac{N}{3} - 1$ (à savoir soit $P = [1, \frac{N}{3}[$ ou $P = [\frac{2N}{3}, N]$) telle que $|A_0 \cap P| \geq |A \cap P| \geq \frac{2\delta N}{5} > \frac{6\delta}{5}(\frac{N}{3} - 1) = \frac{6\delta}{5}\,|P| \geq \delta_0(1 + \frac{\delta_0}{320})\,|P|$. ▲

Cas ii. $|\mathbf{B}| > \frac{\delta \mathbf{N}}{\mathbf{5}}$.

Cas a. On suppose que $\left|\hat{A}(a)\right| \leq \alpha N$ pour tout $a \neq 0$. Dans ce cas, le nombre n de triples $(x, y, z) \in A \times B \times B$ tels que

$x+y=2z$ (dans $\mathbb{Z}_N$) est exactement

$$\begin{aligned}
n &= \frac{1}{N}\sum_{x\in A}\sum_{y,z\in B}\sum_{a=0}^{N-1}\omega^{-a(x+y-2z)} \\
&= \frac{1}{N}|A|\,|B|^2-\frac{1}{N}\sum_{a\neq 0}\hat{A}(a)\hat{B}(a)\hat{B}(-2a) \\
&\geq \delta|B|^2-N^{-1}\max_{a\neq 0}\left|\hat{A}(a)\right|\Big(\sum_{r\neq 0}\left|\hat{B}(a)\right|^2\Big)^{\frac{1}{2}}\Big(\sum_{r\neq 0}\left|\hat{B}(-2a)\right|^2\Big)^{\frac{1}{2}} \\
&\geq \delta|B|^2-\alpha\,(N|B|)^{\frac{1}{2}}\,(N|B|)^{\frac{1}{2}} \\
&= \delta|B|^2-\alpha|B|\,N.
\end{aligned}$$

Puisque, en plus, on a $|B|>\frac{\delta N}{5}$, on voit bien que

$$\begin{aligned}
n &\geq \delta\left(\frac{\delta N}{5}\right)^2-\alpha\left(\frac{\delta N}{5}\right)N \\
&= \frac{\delta^3N^2}{50}.
\end{aligned}$$

Maintenant, il est clair que si $x+y=2z$ dans $\mathbb{Z}_N$ avec $x\in A, y\in B, z\in B$, alors $x+y=2z$ dans $\mathbb{Z}$. Donc n ne compte que des progressions arithmétiques dans $\mathbb{Z}$. Mais il est à remarquer que n compte aussi les progressions arithmétiques dégénérées ; mais on n'a que N progressions arithmétiques dégénérées. Donc pour $N\geq\frac{100}{\delta^3}$, on a au moins N progressions arithmétiques de longueurs trois. ▲

Cas b. Supposons que $\left|\hat{A}(a)\right|>\alpha N$ pour un certain $a\neq 0$. Dans ce cas, le corollaire (4) nous donne une progression arithmétique P de longueur $\geq\sqrt{\frac{\alpha N}{16\pi}}$ telle que

$$|A\cap P|\geq(\delta+\frac{\delta^2}{80\sqrt{2}})\,|P|\,.$$

Donc on a réussi à trouver une progression arithmétique de longueur $\geq\sqrt{\frac{\alpha N}{16\pi}}$ telle que $|A_0\cap P|\geq|A\cap P|\geq(\delta+\frac{\delta^2}{80\sqrt{2}})\,|P|>\delta_0(1+\frac{\delta_0}{320})\,|P|$. ▲

On a réussi à montrer notre but (6). Ainsi, on voit que, même si une partie A_0 de $[1,N_0]$ de taille $\geq\delta_0N_0$ ne contient pas de progression arithmétique de longueur trois, il y a toujours une progression arithmétique $P_1\subset[1,N_0]$ de longueur $N_1\geq\sqrt{\frac{\alpha N}{16\pi}}\geq\sqrt{\frac{\alpha N_0}{48\pi}}=\delta\sqrt{\frac{N_0}{480\pi}}=\delta_0(1-\frac{\delta_0}{160})\sqrt{\frac{N_0}{480\pi}}\geq c(\delta_0)\sqrt{N_0}$ (avec $c(x)=\frac{1}{\sqrt{480\pi}}x(1-\frac{x}{160})$), telle que $|A_0\cap P_1|\geq\delta_0(1+\frac{\delta_0}{320})\,|P_1|=c'(\delta_0)\,|P_1|$ (où $c'(x)=x(1+\frac{x}{320})$) ; c'est-à-dire qu'on peut trouver une progression arithmétique dans laquelle la densité de A_0 est plus grande que celle dans $[1,N_0]$.

On suppose que A_0 ne contient pas de suite arithmétique de longueur trois. Soit $A_1^{'}$ le principe de $A_0\cap P_1$ (on remarque que le principe de P_1, c'est $[1,N_1]$) ; posons $\delta_1=c'(\delta_0)$. Alors $A_1^{'}$ est une partie de $[1,N_1]$ de taille $\geq\delta_1N_1$. Puisque $A_1^{'}$ ne contient pas de suite arithmétique de longueur trois, on peut trouver une suite arithmétique $P_2^{'}\subset[1,N_1]$ de longueur $N_2\geq c(\delta_1)\sqrt{N_1}$ telle que $\left|A_1^{'}\cap P_2^{'}\right|\geq c'(\delta_1)\left|P_2^{'}\right|$. Soit P_2 l'image de $P_2^{'}$ et A_1

celle de $A_1^{'}$. Donc on a trouvé une sous-progression arithmétique P_2 de P_1 de longueur $N_2 \geq c(\delta_1)\sqrt{N_1}$ telle que

$$|A_0 \cap P_2| \quad \geq \quad |A_1 \cap P_1| \geq c^{'}(\delta_1)\,|P_2|\,.$$

Donc la densité de A_0 dans P_2 a augmenté par au moins $\frac{\delta_1^2}{320}$.

On peut maintenant faire un argument itératif : à la $m^{\text{ième}}$ étape on a une progression arithmétique P_m de longueur $N_{m+1} \geq c(\delta_m)\sqrt{N_m}$ telle que

$$|A_0 \cap P_m| \geq c^{'}(\delta_{m-1})\,|P_m|$$

où $|A_0 \cap P_{m-1}| \geq \delta_{m-1}\,|P_{m-1}|$. À la prochaine étape, on obtient une progression arithmétique P_{m+1} de longueur $N_{m+2} \geq c(\delta_{m+1})\sqrt{N_{m+1}}$ telle que

$$|A_0 \cap P_{m+1}| \geq c^{'}(\delta_m)\,|P_{m+1}|\,.$$

Maintenant, $\delta_{m+1} = c^{'}(\delta_m) = \delta_m + \frac{\delta_m^2}{320} \forall m \geq 0$. On démontre facilement (par récurrence) que $\delta_m \geq \delta_0 + m\frac{\delta_0^2}{320} \forall m \geq 0$. Donc, si $m \geq \frac{320(1-\delta_0)}{\delta_0^2}$, alors

$$\begin{aligned}
\delta_m &\geq \delta_0 + m\frac{\delta_0^2}{320} \\
&\geq \delta_0 + \frac{320(1-\delta_0)}{\delta_0^2}\,\frac{\delta_0^2}{320} \\
&= 1.
\end{aligned}$$

Donc pour un tel m, $A_0 \cap P_m = P_m$, de sorte que la progression arithmétique P_m est contenue dans A_0. Maintenant, la longueur de P_m est

$$\begin{aligned}
N_{m+1} &\geq c(\delta_m)\sqrt{N_m} \\
&\geq c(\delta_m)\sqrt{c(\delta_{m-1})\sqrt{c(\delta_{m-2})\sqrt{c(\delta_{m-3})\cdots\sqrt{\cdots\sqrt{c(\delta_0)\sqrt{N_0}}}}}} \qquad \text{(par récurrence)} \\
&= \kappa N_0^{\frac{1}{2^{m+1}}}
\end{aligned}$$

où

$$\kappa = c(\delta_m)\sqrt{c(\delta_{m-1})\sqrt{c(\delta_{m-2})\sqrt{c(\delta_{m-3})\cdots\sqrt{\cdots\sqrt{c(\delta_0)}}}}}.$$

Donc il suffit d'avoir $\kappa N_0^{\frac{1}{2^{m+1}}} \geq 3$ pour garantir l'existence d'une progression arithmétique de longueur trois. Maintenant, pour $x > y$ on a $c(x) > c(y)$ tant que $x + y < 160$. Donc on voit bien que

$$\begin{aligned}
c(\delta_n) &\geq c(\delta_0 + n\frac{\delta_0^2}{320}) \qquad\qquad (n = 0, 1, \cdots, m) \\
&\geq c(\delta_0) \\
&= \frac{1}{\sqrt{480\pi}}\delta_0(1 - \frac{\delta_0}{160}),
\end{aligned}$$

ce qui donne

$$\begin{aligned}
\kappa &\geq \left(\frac{1}{\sqrt{480\pi}}\delta_0(1-\frac{\delta_0}{160})\right)^{1+\frac{1}{2}+\frac{1}{4}+\cdots+\frac{1}{2^m}} \\
&> \left(\frac{1}{\sqrt{480\pi}}\delta_0(1-\frac{\delta_0}{160})\right)^{2} \\
&\geq \frac{\delta_0^4}{480\pi} \qquad (\because \delta_0(1-\frac{\delta_0}{160}) \geq \delta_0^2 \text{ pour } \delta_0 \text{ assez petit})
\end{aligned}$$

d'où $N_{m+1} \geq \frac{\delta_0^4}{480\pi} N_0^{\frac{1}{2^{m+1}}}$. Évidemment, il est largement suffisant d'avoir $\frac{\delta_0^4}{480\pi} N_0^{\frac{1}{2^{m+1}}} \geq 3$ (pour garantir $N_{m+1} \geq 3$), ce qui revient à dire que $N_0 \geq \left(\frac{1440\pi}{\delta_0^4}\right)^{2^{m+1}} = \exp\exp(\lambda\delta_0^{-1})$ avec λ constant. On a utilisé le fait que, pour $m \geq \frac{C}{\delta_0}$ avec C une constante absolue, on peut garantir $\delta_m \geq 1$. En effet, il suffisait d'itérer au plus $\frac{320}{\delta_0}(1+\frac{1}{2}+\frac{1}{4}+\frac{1}{8}+\cdots) = \frac{640}{\delta_0}$ fois pour garantir $\delta_m \geq 1$. (On a montré que la densité (appelons-la ϵ) se double après au plus $\frac{320}{\epsilon}$ étapes) $\square$

Deuxième partie

Quelques résultats

THÉORÈME 7. **(Szemerédi, [SZ])** *Il existe une constante absolue $c > 0$ telle que chaque partie $A \subset [1, N]$ de taille $\geq N \exp(-c\sqrt{\log\log N})$ contient trois termes en progression arithmétique, pour N assez grand.* $\square$

THÉORÈME 8. **(Jean Bourgain, [JB])** *Il existe une constante absolue $c > 0$ telle que chaque partie de $[1, N]$ de taille $\geq Nc\sqrt{\frac{\log\log N}{\log N}}$ contient au moins une progression arithmétique de longueur trois.*

THÉORÈME 9. **(Tom Sanders, [TS])** *Si $A \subset [1, N]$ ne contient pas de progression arithmétique de longueur trois, alors*

$$|A| = O\left(\frac{N(\log\log N)^5}{\log N}\right).$$

THÉORÈME 10. **(L'exemple de Behrend, [FB])** *Il existe une partie $A \subset [1, N]$ avec $|A| \gg N \exp(-c\sqrt{\log N})$ qui ne contient pas de progression arithmétique de longueur trois.*

DÉMONSTRATION. Pour deux entiers d et k, on considère l'ensemble $T := \{(x_1, ..., x_k) : x_1, ..., x_k \in [0, d]\}$. On a $|T| = (d+1)^k$. Il est clair que $\sum_{i=1}^k x_i^2 \in [0, kd^2]$ pour tout $(x_1, ..., x_k) \in T$. Donc (par le principe du tiroir) il existe au moins un $n \leq kd^2$ tel que $\sum_{i=1}^k x_i^2 = n$ pour plus de $\frac{(d+1)^k}{kd^2+1}$ éléments $(x_1, ..., x_k)$ de T. Donc la sphère $S := \{(x_1, \cdots, x_k) : \sum_{i=1}^k x_i^2 = n\}$ contient au moins $\frac{(d+1)^k}{kd^2+1}$ points de T. Cela revient à dire que $|S \cap T| \geq \frac{(d+1)^k}{kd^2+1}$.

Considérons maintenant l'ensemble $A := \{\sum_{i=1}^k x_i(2d+1)^{i-1} : (x_1, \cdots, x_k) \in S \cap T\}$. Évidemment[1], $|A| \geq \frac{(d+1)^k}{kd^2+1}$. Il est facile à montrer que $a < (2d+1)^k \forall a \in A$. En effet, pour $a = \sum_{i=1}^k x_i(2d+1)^{i-1} \in A$, on a

$$\begin{aligned} a &\leq \sum_{i=1}^k d(2d+1)^{i-1} \\ &= \frac{(2d+1)^k - (2d+1)}{2} \\ &< (2d+1)^k. \end{aligned}$$

Nous affirmons que A est sans progression arithmétique de longueur trois. Par l'absurde, on suppose que

$$\sum_{i=1}^k x_i(2d+1)^{i-1} + \sum_{i=1}^k y_i(2d+1)^{i-1} = 2\sum_{i=1}^k z_i(2d+1)^{i-1}$$

avec $x_i, y_i, z_i \in S \cap T$. Il est évident que [1] $x_i + y_i = 2z_i \forall i$. Donc les trois points $(x_1, \cdots, x_k), (y_1, \cdots, y_k)$ et $(z_1, \cdots, z_k)$ sont alignés. Mais ce n'est pas possible parce qu'ils sont tous les trois sur la sphère S. Donc A ne contient aucune progression arithmétique de longueur trois.

Maintenant, on prend $k = \lfloor\sqrt{\log N}\rfloor$, et on choisit un d tel que $(2d+1)^k \leq N < (2d+3)^k$. Alors A est une partie de $[1, N]$ de taille $\geq \frac{(d+1)^k}{kd^2+1} > \frac{(d+1)^{k-2}}{k} \geq \frac{(N^{\frac{1}{k}}-1)^{k-2}}{2^{k-2}k} =$

1. Note : Si $\sum_{k=0}^n a_k x^k = 0$ avec $a_k, x \in \mathbb{Z}$ et $|a_k| < |x|$ alors $a_k = 0 \forall k = 0, \cdots, n$. En effet, d'emblée, il est clair que x divise a_0 ; comme $|a_0| < |x|$, on a $a_0 = 0$ etc.

$\frac{N^{1-\left(\frac{2}{k}\right)}}{2^{k-2}k}(1-N^{-\left(\frac{1}{k}\right)})^{k-2}$; pour N suffisamment grand, cette quantité est $> \frac{N^{1-\left(\frac{2}{k}\right)}}{2^{k-1}k} = \frac{N\exp(-\frac{2}{k}\log N)}{\exp(\log n+n\log 2)} = N\exp(-\frac{2}{k}\log N - \log k - k\log 2) \geq N\exp(-2\sqrt{\log N} - \frac{1}{2}\log\log N - \sqrt{\log N}\log 2) \geq N\exp(-c\sqrt{\log N})$ avec c une constante absolue. Donc $|A| \geq N\exp(-c\sqrt{\log N})$ et A ne contient pas de progression arithmétique de longueur trois.

$\square$

Bibliographie

[FB] F. A. Behrend. On sets of integers which contain no three terms in arithmetic progression. *Proceedings of national academy of sciences,* **32** :331-332, 1946.

[JB] J. Bourgain. On triples in arithmetic progression. *Geometric and functional analysis,* vol. 9 (1999) 968-984.

[G1] W.T. Gowers. A new proof of Szemerédi's theorem for arithmetic progressions of length four. *Geometric and functional analysis,* vol. 8 (1998) 529-551.

[G2] W.T. Gowers. A new proof of Szemerédi's theorem. *Geometric and functional analysis,* vol. 11 (2011) 465-588.

[TS] T. Sanders. On Roth's theorem on progressions. *Annals of Mathematics* **174** (2011), 619-636.

[SZ] E. Szemerédi. An old new proof of Roth's theorem. *Centre de recherches mathématiques Proceedings & lecture notes,* vol. **43** : 51-54, 2007.