COMBINATOIRE ADDITIVE : LE THÉORÈME DE ROTH

Diego IZQUIERDO

22 MARS 2012

1 Introduction

Soit N un entier naturel non nul. On note $[N] = \{1, 2, \dots, N\}$. Dans cet exposé, nous nous intéresserons au problème de déterminer si une partie A de $[N]$ contient des suites arithmétiques.

Définition 1.1. Soit $k \in \mathbb{N} - \{0, 1, 2\}$. On note $r_k(N)$ le plus petit entier naturel r tel que toute partie A de $[N]$ de cardinal au moins r contient une suite arithmétique de raison non nulle et de longueur k .

Nous voulons donc étudier le nombre $r_k(N)$. Dans cet exposé, on ne s'intéressera qu'au cas où $k = 3$.

Exemple 1.2. Prenons $N = 6$ et $k = 3$. La partie $\{1, 2, 4, 5\}$ ne contient aucune suite arithmétique de raison non nulle et de longueur 3. Cependant, toute partie à 5 éléments de $[6]$ contient trois nombres consécutifs, donc $r_3(6) = 5$.

Nous pouvons déjà donner des propriétés tout à fait élémentaires de $r_3(N)$:

Proposition 1.3. (Premières propriétés de $r_3(N)$)

- (i) Pour $N \geq 12$, on a $r_3(N) \leq \frac{11}{12}N$.
- (ii) Pour tout $N \geq 1$, $r_3(N) \geq 2^{\lfloor \log_3(N) \rfloor}$.

Démonstration. (i) Écrivons $N = 3q + r$, avec $r \in \{0, 1, 2\}$. Soit A une partie de $[N]$ sans suites arithmétiques de longueur 3 et de raison non nulle. Considérons les ensembles $\{1, 2, 3\}$, $\{4, 5, 6\}$, ..., $\{3\lfloor \frac{N}{3} \rfloor - 2, 3\lfloor \frac{N}{3} \rfloor - 1, 3\lfloor \frac{N}{3} \rfloor\}$. La partie A contient au plus deux éléments dans chacun de ces ensembles, donc $|A| \leq 2\lfloor \frac{N}{3} \rfloor + r \leq 2\lfloor \frac{N}{3} \rfloor + 2$. On en déduit que $r_3(N) \leq 2\lfloor \frac{N}{3} \rfloor + 3 \leq \frac{2N}{3} + 3 \leq \frac{2N}{3} + \frac{N}{4} \leq \frac{11}{12}N$, car $N \geq 12$.

- (ii) Considérons A la partie de $[N]$ formée des éléments dont l'écriture en base 3 ne contient que des 0 et des 1. Il est alors quasiment immédiat de vérifier que, si x, y, z sont dans A et vérifient $x + y = 2z$, alors $x = y = z$. Donc $r_3(N) > |A| \geq 2^{\lfloor \log_3(N) \rfloor} - 1$, d'où le résultat. □

Remarque 1.4. La preuve de (i) permet aussi de montrer que, pour tout $\delta > \frac{2}{3}$, on a pour N assez grand : $r_3(N) \leq \delta N$.

L'objectif de cet exposé sera de montrer le théorème suivant :

Théorème 1.5. (Théorème de Roth, 1956)

Soit $\delta \in]0, 1]$. Alors il existe un entier naturel N_0 tel que, pour tout $N \geq N_0$, on a $r_3(N) \leq \delta N$.

En 1936, Erdős et Turán ont conjecturé ce résultat, qui a été prouvé par Roth en 1956. Szemerédi a résolu le cas $k = 4$ en 1969, puis le cas général en 1975.

2 Analyse de Fourier sur $\mathbb{Z}/N\mathbb{Z}$

Dans cette partie, on posera $G = \mathbb{Z}/N\mathbb{Z}$. On note $e : (x, \xi) \in G \times G \mapsto e^{\frac{2\pi i x \xi}{N}}$.

Définition 2.1. (Transformée de Fourier)

On appelle **transformée de Fourier** de f l'application $\widehat{f} : G \rightarrow \mathbb{C}$ définie par :

$$\widehat{f}(\xi) = \frac{1}{N} \sum_{x \in G} f(x) \overline{e(x, \xi)}.$$

Exemple 2.2. On a $\widehat{1}(x) = 0$ si $x \neq 0$ et $\widehat{1}(0) = 1$.

Exercice 2.3. 1. Fixons $a, b \in \mathbb{Z}/N\mathbb{Z}$. Soit $A = \{ax + b | x \in \mathbb{Z}/N\mathbb{Z}\}$. Montrer que $\widehat{1_A}(x) = \frac{e(x, b)}{a \wedge N}$ si $\frac{N}{a \wedge N} | x$ et $\widehat{1_A}(x) = 0$ sinon.

2. Fixons $a, b \in [N]$ et $r \in \mathbb{N}$. On suppose que $ar < N$. Soit $A = \{ax + b | x \in \{\bar{0}, \bar{1}, \dots, \bar{r}\}\}$. Montrer que $|\widehat{1_A}(x)|$ est maximal pour x multiple de $\frac{N}{a \wedge N}$.

On peut définir un produit scalaire hermitien sur l'espace des fonctions $f : G \rightarrow \mathbb{C}$ par : $\langle f, g \rangle = \frac{1}{N} \sum_{x \in G} f(x) \overline{g(x)}$.

Proposition 2.4. (Propriétés élémentaires de la transformée de Fourier)

Si f, g sont deux fonctions $G \rightarrow \mathbb{C}$, on a :

(i) $\forall x \in G, f(x) = \sum_{\xi \in G} \widehat{f}(\xi) e(x, \xi)$.

(ii) $\langle f, g \rangle = \sum_{\xi \in G} \widehat{f}(\xi) \overline{\widehat{g}(\xi)}$ (égalité de Parseval).

(iii) $\|f\|^2 = \frac{1}{N} \sum_{x \in G} |f(x)|^2 = \sum_{x \in G} |\widehat{f}(x)|^2$ (égalité de Plancherel).

Exercice 2.5. Prouver la propriété précédente. Définir naturellement un produit de convolution $f \star g$ où $f, g : G \rightarrow \mathbb{C}$, et montrer que $\widehat{f \star g} = \widehat{f} \cdot \widehat{g}$.

3 Le théorème de Roth

3.1 Réduction à $\mathbb{Z}/N\mathbb{Z}$

Nous voulons utiliser l'analyse de Fourier sur $\mathbb{Z}/N\mathbb{Z}$ pour prouver le théorème de Roth. Cependant, l'ensemble sur lequel nous travaillons n'est pas $\mathbb{Z}/N\mathbb{Z}$ mais $[N]$. Il semble alors naturel d'identifier $[N]$ et $\mathbb{Z}/N\mathbb{Z}$ à l'aide de la projection canonique, que nous noterons p . Mais il faut prendre quelques précautions ! En effet, s'il est vrai qu'un triplet x, y, z de $[N]$ vérifiant $x + y = 2z$ satisfait aussi $p(x) + p(y) = 2p(z)$, la réciproque est totalement fautive. On peut très bien trouver $x, y, z \in [N]$ tels que $x + y \neq 2z$ et $p(x) + p(y) = 2p(z)$: par exemple, on peut prendre $N = 4$, $x = y = 2$ et $z = 4$.

Nous allons régler ce problème de la manière suivante. Supposons N impair. Soit A une partie de $[N]$ de cardinal au moins δN . Notons P (resp. I) l'ensemble des éléments pairs (resp. impairs) de A . Posons $B = P$ si $|P| \geq |I|$, $B = I$ sinon. Soient $x, y \in B$ et $z \in A$ tels que $p(x) + p(y) = 2p(z)$. Alors $x + y - 2z \in \{-N, 0, N\}$, et nécessairement, par parité, $x + y = 2z$.

Par conséquent, si l'on prouve que pour N assez grand impair, il existe $x, y \in B$ et $z \in A$ distincts tels que $x + y \equiv 2z \pmod{N}$, on pourra conclure que, pour N assez grand impair, $r_3(N) \leq \delta N$, et ce pour tout $\delta > 0$. On aura alors, pour N assez grand, $r_3(2N) \leq r_3(2N + 1) \leq \frac{\delta}{2}(2N + 1) \leq 2\delta N$, et donc le théorème de Roth sera prouvé.

Ainsi, on s'est ramené à résoudre le problème suivant dans $G = \mathbb{Z}/N\mathbb{Z}$: montrer que pour N assez grand impair, il existe $x, y \in B$ et $z \in A$ distincts tels que $x + y \equiv 2z \pmod{N}$. Nous avons donc interprété le problème dans G ce qui nous permet d'utiliser l'analyse de Fourier, mais il ne faut pas oublier que le problème peut aussi être vu dans $[N]$ ce qui nous permettra d'utiliser des inégalités : c'est ce double point de vue qui va nous permettre de prouver le théorème de Roth !

3.2 Lien entre le nombre de suites arithmétiques et la transformée de Fourier

Commençons par exprimer le nombre Δ de triplets $(x, y, z) \in B \times B \times A$ tels que $x + y \equiv 2z \pmod{N}$ à l'aide de la transformée de Fourier :

Proposition 3.1. (*Combinatoire et transformée de Fourier*)

Notons 1_A (resp. 1_B) la fonction caractéristique de A (resp. de B). Alors

$$\Delta = N^2 \sum_{g \in G} \widehat{1_B}(g)^2 \widehat{1_A}(-2g).$$

Démonstration. On a :

$$\begin{aligned}
N^2 \sum_{g \in G} \widehat{1_B}(g)^2 \widehat{1_A}(-2g) &= \frac{1}{N} \sum_{g \in G} \left(\sum_{x \in G} 1_B(x) \overline{e(x, g)} \right)^2 \sum_{x \in G} 1_A(x) \overline{e(x, -2g)} \\
&= \frac{1}{N} \sum_{g \in G} \left(\sum_{x, y, z \in G} 1_B(x) 1_B(y) 1_A(z) \overline{e(x + y - 2z, g)} \right) \\
&= \frac{1}{N} \sum_{x, y \in B, z \in A} \left(\sum_{g \in G} \overline{e(x + y - 2z, g)} \right) \\
&= \frac{1}{N} \sum_{x, y \in B, z \in A, x+y \equiv 2z \pmod{N}} N \\
&= \Delta.
\end{aligned}$$

□

Parmi les triplets (x, y, z) avec $x, y \in B$, $z \in A$ et $x + y \equiv 2z \pmod{N}$, ceux vérifiant $x = y = z$ ne nous intéressent pas. Ainsi, nous voulons montrer que, pour N assez grand, $\Delta - |B| > 0$. D'après ce qui précède :

$$\Delta - |B| = N^2 \sum_{g \in G, g \neq 0} \widehat{1_B}(g)^2 \widehat{1_A}(-2g) + \frac{|A||B|^2}{N} - |B|.$$

Exercice 3.2. On suppose N impair. À l'aide de la transformée de Fourier, exprimer le nombre de suites arithmétiques de longueur 4 et de raison non nulle contenues dans $[N]$.

3.3 Le cas où A est uniformément distribué dans les sous-suites arithmétiques de $[N]$

Soit $\epsilon > 0$. Supposons que, pour tout $g \in G$ non nul, $|\widehat{1_A}(g)| \leq \epsilon$. Si ϵ est petit, cela correspond intuitivement au cas où A est uniformément distribué dans $[N]$. On a alors, grâce à l'identité de Plancherel :

$$\begin{aligned}
N^2 \left| \sum_{g \in G} \widehat{1_B}(g)^2 \widehat{1_A}(-2g) \right| &\leq \epsilon N^2 \sum_{g \in G} |\widehat{1_B}(g)|^2 \\
&\leq \epsilon N \sum_{g \in G} |1_B(g)|^2 \\
&\leq \epsilon N |B|.
\end{aligned}$$

Prenons $\epsilon = \frac{\delta^2}{4}$. Alors : $N^2 \left| \sum_{g \in G} \widehat{1_B}(g)^2 \widehat{1_A}(-2g) \right| \leq \frac{|A|^2 |B|}{4N} \leq \frac{|A||B|^2}{2N}$. Donc $\Delta - |B| \geq \frac{|A||B|^2}{2N} - |B| \geq |B| \left(\frac{|A||B|}{2N} - 1 \right) \geq |B| \left(\frac{\delta^2}{4} N - 1 \right) > 0$, pour $N > \frac{4}{\delta^2}$.

3.4 Le cas où A est concentré dans une sous-suite arithmétique de $[N]$ de raison différente de 1

Reste donc à régler le cas où il existe $g^* \in G$ non nul tel que $|\widehat{1_A}(g^*)| \geq \frac{\delta^2}{4}$. Cela correspond intuitivement au cas où A n'est pas uniformément réparti dans $[N]$, mais est concentré autour de g^* . Dans ce cas,

$$\frac{1}{N} \left| \sum_{x \in G} (1_A(x) - \delta) \overline{e(x, g^*)} \right| \geq \frac{\delta^2}{4}.$$

Proposition 3.3. (Théorème de Dirichlet)

Soient $x \in \mathbb{R}^+$ et $Q \in \mathbb{N}^*$. Alors il existe b et q deux entiers naturels, $q \neq 0$, tels que $|qx - b| \leq \frac{1}{Q}$, $q \leq Q$ et $b \wedge q = 1$.

Démonstration. On considère les $Q + 1$ réels $0, \{x\}, \{2x\}, \dots, \{Qx\}$, et on subdivise l'intervalle $[0, 1]$ en Q sous-intervalles $[0, 1/Q], [1/Q, 2/Q], \dots, [(Q-1)/Q, 1]$. D'après le principe des tiroirs, il existe j, k entre 0 et Q , distincts, tels que $\{jx\}$ et $\{kx\}$ appartiennent au même sous-intervalle de $[0, 1]$. Par conséquent, si l'on pose $q' = |k - j|$, il existe b' entier naturel tel que $|q'x - b'| \leq \frac{1}{Q}$. Si $d = b' \wedge q'$, alors $q = q'/d$ et $b = b'/d$ démontrent la proposition. $\square$

Considérons $Q = Q(N)$ une fonction de N à valeurs dans les entiers naturels non nuls avec $Q(N) \leq N$. On peut alors appliquer le théorème de Dirichlet, et trouver b, q deux entiers naturels, $q \neq 0$, tels que $|\frac{g^*}{N} - \frac{b}{q}| \leq \frac{1}{qQ}$, $b \wedge q = 1$ et $q \leq Q$.

Nous allons maintenant effectuer une partition de $\{0, 1, \dots, N-1\}$ en suites arithmétiques de raison q . Plus précisément, on commence par considérer les suites arithmétiques de raison q , maximales (au sens de l'inclusion) dans $[N]$: il y en a exactement q , et elles sont toutes de longueur $\lfloor \frac{N}{q} \rfloor$ ou $\lfloor \frac{N}{q} \rfloor + 1$. Notons-les $s^0, \dots, s^{q-1}$. Pour chaque i entre 0 et $q-1$, on note l_i la longueur de s^i , et on note $s_1^i, \dots, s_{l_i}^i$ les éléments de s^i en ordre croissant. On va maintenant découper ces suites en morceaux de taille plus petite. Soit $M = M(N)$ une fonction de N à valeurs dans les entiers naturels non nuls. On découpe s^i en suites arithmétiques de longueur $L = \lfloor \frac{N}{qM} \rfloor + 1$: pour chaque i entre 0 et $q-1$, on note $I_1^i = \{s_1^i, \dots, s_L^i\}$, $I_2^i = \{s_{L+1}^i, \dots, s_{2L}^i\}$, ..., $I_{\lfloor \frac{l_i}{L} \rfloor}^i = \{s_{(\lfloor \frac{l_i}{L} \rfloor - 1)L + 1}^i, \dots, s_{l_i}^i\}$. Ainsi, les I_j^i forment une partition de $\{0, \dots, N-1\}$ en suites arithmétiques de raison q et de longueur au moins L et au plus $2L$. Notons $\mathcal{P}$ l'ensemble des I_j^i . L'idée dans la suite va consister à remplacer $[N]$ par un élément de $\mathcal{P}$, dans lequel la densité de A sera plus grande que δ .

Fixons $I \in \mathcal{P}$ et $x \in I$. Alors il existe $\epsilon \in [-1, 1]$ tel que :

$$\overline{e(x, g^*)} = e^{2i\pi x \frac{g^*}{N}} = e^{2i\pi x (\frac{b}{q} + \frac{\epsilon}{qQ})}.$$

Maintenant, si l'on choisit $y \in I$, alors il existe r entier tel que $y = x + rq$ et $|r| \leq \frac{2N}{qM}$, et donc :

$$\left| \frac{\overline{e(y, g^*)}}{\overline{e(x, g^*)}} - 1 \right| = \left| e^{-2i\pi (br + \frac{\epsilon r}{Q})} - 1 \right| = \left| e^{-2i\pi \frac{\epsilon r}{Q}} - 1 \right| = 2 \left| \sin \left(\frac{\pi \epsilon r}{Q} \right) \right| \leq \frac{2\pi r}{Q} \leq \frac{4\pi N}{qQM}.$$

Ainsi :

$$\begin{aligned}
N \frac{\delta^2}{4} &\leq \sum_{g \in G} (1_A(x) - \delta) \overline{e(x, g^*)} | \\
&\leq \sum_{I \in \mathcal{P}} \left| \sum_{x \in I} (1_A(x) - \delta) \overline{e(x, g^*)} \right| \\
&\leq \sum_{I \in \mathcal{P}} \left(\left| \sum_{x \in I} (1_A(x) - \delta) \right| + \frac{4\pi N |I|}{qQM} \right) \\
&\leq \sum_{I \in \mathcal{P}} \left| \sum_{x \in I} (1_A(x) - \delta) \right| + \frac{4\pi N^2}{qQM}.
\end{aligned}$$

Il faut maintenant choisir les fonctions Q et M . Pour obtenir des inégalités non triviales, on veut que $\frac{4\pi N^2}{qQM}$ soit petit (en tous cas, inférieur à $N\delta^2/4$). Dans le meilleur des cas, on peut espérer que $N\frac{\delta^2}{4} - \frac{4\pi N^2}{qQM}$ va être minoré par une fonction de la forme CN avec $C > 0$. Si l'on est ambitieux, on peut même essayer de faire en sorte que C soit de l'ordre de δ^2 , par exemple $C = \frac{\delta^2}{8}$. On voudrait donc que QM soit proche de $\frac{16\pi N}{q\delta^2}$. Puisque le choix de q dépend du choix de Q , le facteur $1/q$ doit apparaître dans M .

On choisit $Q(N) = \lceil \sqrt{N} \rceil$ et $M(N) = \lceil \frac{32\pi\sqrt{N}}{q\delta^2} \rceil$. Alors on a :

$$\sum_{I \in \mathcal{P}} \left| \sum_{x \in I} (1_A(x) - \delta) \right| \geq \frac{N\delta^2}{8}.$$

D'autre part, $\sum_{I \in \mathcal{P}} \sum_{x \in I} (1_A(x) - \delta) \geq 0$. On en déduit qu'il existe $I \in \mathcal{P}$ tel que $\sum_{x \in I} (1_A(x) - \delta) \geq \frac{\delta^2 L}{16}$. On en déduit que :

$$\frac{|A \cap I|}{|I|} \geq \delta + \frac{\delta^2}{32}.$$

On a de plus : $|I| \geq L \geq \frac{N}{qM} \geq \frac{N}{q(\frac{32\pi\sqrt{N}}{q\delta^2} + 1)} \geq \frac{\delta^2\sqrt{N}}{33\pi}$.

3.5 L'argument d'augmentation de densité

À l'aide d'une transformation affine, on peut identifier I à un ensemble de la forme $[N_1]$ avec $N_1 \geq \frac{\delta^2\sqrt{N}}{33\pi}$. L'ensemble $A \cap I$ est alors identifié à une partie A_1 de $[N_1]$, de densité au moins $\delta_1 = \delta + \frac{\delta^2}{32}$. Comme l'identification est affine, une suite arithmétique de $A \cap I$ correspond à une suite arithmétique de A_1 .

Maintenant, on veut voir si A_1 contient une suite arithmétique. Si c'est le cas, A en contiendra aussi. Trois cas se présentent : soit A_1 vérifie les hypothèses de 3.3 et on a terminé, soit $\delta_1 > 11/12$ et on a terminé, soit A_1 vérifie les hypothèses de 3.4. Dans ce dernier, on procède de nouveau comme en 3.4, et on construit $N_2 \geq \frac{\delta_1^2\sqrt{N}}{33\pi}$

et A_2 une partie de $[N_2]$ de densité au moins $\delta_2 = \delta_1 + \frac{\delta_1^2}{32}$. Et on continue ainsi en construisant $N_3, N_4, \dots, A_3, A_4, \dots, \delta_3, \delta_4, \dots$, avec $N_{n+1} \geq \frac{\delta_n^2 \sqrt{N_n}}{33\pi}$ et $\delta_{n+1} = \delta_n + \frac{\delta_n^2}{32}$ et A_n de densité au moins δ_n .

On vérifie alors immédiatement que $\delta_n \geq \delta + n \frac{\delta^2}{32}$. Soit $n_1 = \lceil \frac{32}{\delta} \rceil$. Alors $\delta_{n_1} \geq 2\delta$. De même, si $n_2 = \lceil \frac{32}{2\delta} \rceil$, on a $\delta_{n_1+n_2} \geq 4\delta$. On continue ainsi, en posant $n_k = \lceil \frac{32}{2^k \delta} \rceil$ et en remarquant que $\delta_{n_1+n_2+\dots+n_k} \geq 2^{k-1}\delta$. Soit $K = \lceil \frac{\ln(\frac{11}{12\delta})}{\ln 2} \rceil$. On a alors $\delta_{n_1+\dots+n_K} \geq \frac{11}{12}$, et donc le processus précédent s'arrête au bout d'au plus $n_1 + \dots + n_K$ étapes. Or $n_1 + \dots + n_K \leq K + \frac{64}{\delta} \leq \frac{\ln(\frac{11}{12\delta})}{\ln 2} + \frac{64}{\delta} + 1$. Donc le processus s'arrête au bout d'au plus $\frac{\ln(\frac{11}{12\delta})}{\ln 2} + \frac{64}{\delta} + 1$ étapes.

Pour pouvoir utiliser la proposition 1.3(i), la partie 3.3 et itérer la partie 3.4, il faut que le dernier N_n soit au moins $\max(12, \frac{4}{\delta^2})$. Or $N_n \geq \frac{\delta^2 \sqrt{N_{n-1}}}{33\pi} \geq \left(\frac{\delta^2}{33\pi}\right)^{1+\frac{1}{2}+\frac{1}{4}+\dots} N^{\frac{1}{2^n}} \geq \left(\frac{\delta^2}{33\pi}\right)^2 N^{\frac{1}{2^n}}$. Il suffit donc que

$$\ln \ln N \geq \ln \ln \left(\left(\frac{33\pi}{\delta^2} \right)^2 \max \left(12, \frac{8}{\delta^2} \right) \right) + \left(\frac{\ln(\frac{11}{12\delta})}{\ln 2} + \frac{64}{\delta} + 1 \right) \ln 2.$$

3.6 Conclusions

Nous avons donc prouvé le théorème de Roth :

Théorème 3.4. (Théorème de Roth, 1956)

Soit $\delta \in]0, 1]$. Alors il existe un entier naturel N_0 tel que, pour tout $N \geq N_0$, on a $r_3(N) \leq \delta N$.

Mais en fait nous avons prouvé mieux :

Théorème 3.5. (Théorème de Roth, 1956)

Soit $A \subseteq \mathbb{N}$ ne contenant pas de suites arithmétiques non triviales de longueur 3. On note $\delta_N = \frac{|A \cap [N]|}{N}$. Alors, quand $N \rightarrow +\infty$, $\delta_N = O\left(\frac{1}{\ln \ln N}\right)$.

Voici quelques corollaires immédiats du théorème de Roth :

Corollaire 3.6. (Théorème de Roth, 1956)

Si $A \subseteq \mathbb{N}$ est tel que $\limsup_{N \rightarrow +\infty} \frac{|A \cap [N]|}{N} > 0$, alors A contient une infinité de suites arithmétiques non triviales de longueur 3.

Corollaire 3.7. (Théorème de Van der Warden, 1927)

On dispose de r couleurs. On colorie chaque entier naturel avec une de ces r couleurs. Alors il existe trois entiers naturels distincts qui sont de la même couleur et qui forment une suite arithmétique.

Corollaire 3.8. (Un petit résultat amusant...)

Soit $b > 1$ un entier. Soit a_n la somme des n premiers chiffres après la virgule dans l'écriture en base b de π . Alors l'ensemble $\{a_1, a_2, \dots\}$ contient une infinité de suites arithmétiques de longueur 3 non triviales.

4 L'exemple de Behrend

Pour terminer, nous allons donner une majoration de $r_3(N)$ due a Behrend :

Theoreme 4.1. (*Exemple de Behrend, 1946*)

Il existe $C > 0$ tel que, pour N suffisamment grand, $r_3(N) \geq Ne^{-C\sqrt{\ln(N)}}$.

Demonstration. Fixons k et d deux entiers naturels, que nous choisirons convenablement dans la suite. La preuve de Behrend repose sur une remarque tout a fait evidente : dans un espace vectoriel rel de dimension k , une sphere et une droite se coupent en au plus 2 points. Ainsi, si u, v, w sont trois vecteurs de meme norme tels que $u + v = 2w$, alors $u = v = w$.

Soit $S = \{0, 1, \dots, d\}^k$. Pour tout $(x_1, \dots, x_d) \in S$, on a $x_1^2 + \dots + x_d^2 \in \{0, 1, \dots, kd^2\}$. Ainsi, d'apres le principe des tiroirs, il existe $M \in \{1, \dots, kd^2\}$ tel que la sphere de rayon $\sqrt{M}$ contient au moins $\frac{(d+1)^k - 1}{kd^2}$ points de S . Il nous faut maintenant identifier ces points a des entiers naturels. Pour ce faire, on fait appel aux bases de numeration : notons $A = \{\sum_{i=1}^d x_i(2d+1)^{i-1} \mid \sum_{i=1}^d x_i^2 = M\}$.

Il nous faut d'abord verifier que $S \rightarrow \mathbb{N}, (x_1, \dots, x_k) \mapsto \sum_{i=1}^k x_i(2d+1)^{i-1}$ est injective, mais cela est evident par unicite de l'ecriture d'un nombre en base $2d+1$. Ensuite, si A contenait des suites arithmetiques de longueur 3 et de raison non nulle, alors la sphere de rayon $\sqrt{M}$ dans $\mathbb{R}^k$ contiendrait trois points distincts alignes : absurde ! Donc A ne contient pas de suites arithmetiques de longueur 3 et de raison non nulle. Finalement, il est clair que $\max(A) \leq (2d+1)^k$.

Posons maintenant $k = \lfloor \sqrt{\ln(N)} \rfloor$ et $d = \lfloor \frac{N^{1/k}}{2} \rfloor - 1$. Alors, comme $(2d+1)^k \leq N$, on a $A \subseteq [N]$, et A ne contient pas de suites arithmetiques non triviales de longueur 3. De plus, comme $N^{1/k} \rightarrow +\infty$ quand $N \rightarrow +\infty$, on a pour N assez grand :

$$\begin{aligned} |A| &\geq \frac{(d+1)^k - 1}{kd^2} \geq \frac{\left(\frac{N^{1/k}}{2} - 1\right)^k - 1}{k\left(\frac{N^{1/k}}{2} - 1\right)^2} \geq \frac{\left(\frac{N^{1/k}}{2} - 1\right)^{k-2}}{2k} \\ &\geq \frac{N^{1-2/k}}{2k4^k} \geq N \exp\left(\ln(2k) - k \ln(4) - \frac{2}{k} \ln(N)\right) \geq Ne^{-C\sqrt{\ln(N)}}. \end{aligned}$$

□

Cette minoration de $r_3(N)$ prouve que, pour tout $\epsilon > 0$ et tout $\delta > 0$, on a, pour N assez grand, $r_3(N) \geq \delta N^{1-\epsilon}$. Cela met en evidence que le theoreme de Roth fournit une assez bonne majoration de $r_3(N)$.