Une propriété topologique de certains ensembles de Mills

Bruno DESCHAMPS

Résumé.– Dans cet article, nous montrons que l'ensemble des constantes de Mills, c'est-à-dire des constantes réelles M telles que, pour tout $n \geq 0$, l'entier $\left[M^{3^n}\right]$ soit un nombre premier, est la limite croissante d'ensembles homéomorphes à l'ensemble triadique de Cantor. Plus généralement, pour une fonction φ donnée et un ensemble A d'entiers, nous étudions l'ensemble de Mills $\mathscr{M}_\varphi(A) = \{\alpha \in \mathbb{R}/\ \forall n \in \mathbb{N},\ [\varphi_n(\alpha)] \in A\}$ (où $\varphi_n = \varphi \circ \cdots \circ \varphi$ n fois). Nous montrons que, sous certaines hypothèses sur φ et A, pour tout réel $w > \inf \mathscr{M}_\varphi(A)$, l'ensemble $\mathscr{M}_\varphi(A) \cap [2, w]$ est homéomorphe à l'ensemble triadique de Cantor.
Abstract.– In this article , we show that the set of Mills constants (real numbers M such that $\left[M^{3^n}\right]$ is prime for all $n \geq 0$) is the increasing limit of sets homeomorphic to the triadic Cantor's set. More generally, for a given function φ and a set A of integers, we studying the Mills set $\mathscr{M}_\varphi(A) = \{\alpha \in \mathbb{R}/\ \forall n \in \mathbb{N},\ [\varphi_n(\alpha)] \in A\}$ (where $\varphi_n = \varphi \circ \cdots \circ \varphi$ n times). We show that, under certain assumptions over φ and A, for all real $w > \inf \mathscr{M}_\varphi(A)$ the set $\mathscr{M}_\varphi(A) \cap [2, w]$ is homeomorphic to the triadic Cantor's set.
MSC2010 : 11A41, 11B05, 11B34.

Un célèbre théorème de Mills (voir [M]) affirme qu'il existe une constante réelle $M > 0$ telle que, pour tout $n \geq 0$, l'entier $\left[M^{3^n}\right]$ est premier (dans ce texte $[x]$ désigne la partie entière du réel x). Ce résultat formellement intrigant découle en fait d'une propriété sur la répartition des nombres premiers. L'exploitation de l'idée utilisée dans [M] permet de généraliser substantiellement ce résultat :

Théorème 1.– *On considère $\varphi : [2, +\infty[\longrightarrow \mathbb{R}$ une fonction continue, strictement croissante et qui vérifie que, pour tout réel $x \geq 0$, $\varphi(x) \geq x$. Si la fonction φ vérifie la propriété*

(R) pour tout $n \gg 0$, il existe un premier p tel que $\varphi(n) < p < \varphi(n+1) - 1$

(i.e. $\liminf_n (\pi(\varphi(n+1) - 2) - \pi(\varphi(n)) \neq 0$.)

alors il existe une constante réelle $M_\varphi > 0$ telle que, pour tout $n \geq 0$, l'entier $\left[\varphi_n(M_\varphi)\right]$ est un nombre premier (où $\varphi_n = \varphi \circ \cdots \circ \varphi$ désigne l'itérée de φ avec elle-même, n fois).

Preuve : La condition (R) permet de construire une suite strictement croissante de nombres premiers $(q_n)_n$ qui vérifie que, pour tout $n \geq 0$, $\varphi(q_n) < q_{n+1} < \varphi(q_n + 1) - 1$. Pour $n \geq 0$, on pose alors

$$\begin{aligned} u_n &= \varphi_n^{-1}(q_n) \\ v_n &= \varphi_n^{-1}(q_n + 1) \end{aligned}$$

où φ_n^{-1} désigne la fonction réciproque de φ_n (définie sur l'image de la fonction φ_n qui est un intervalle d'après les hypothèses). Par stricte croissance de la fonction φ_n^{-1}, on a immédiatement $u_n < v_n$ pour tout $n \geq 0$. Maintenant,

$$\begin{aligned} u_{n+1} &= \varphi_{n+1}^{-1}(q_{n+1}) > \varphi_{n+1}^{-1}(\varphi(q_n)) = \varphi_n^{-1}(q_n) = u_n \\ v_{n+1} &= \varphi_{n+1}^{-1}(q_{n+1}+1) < \varphi_{n+1}^{-1}(\varphi(q_n+1)) = \varphi_n^{-1}(q_n+1) = v_n \end{aligned}$$

Les suites $(u_n)_n$ et $(v_n)_n$ sont donc respectivement strictement croissante et décroissante. On en déduit que la suite $(u_n)_n$ converge vers un réel M_φ qui vérifie que, pour tout $n \geq 0$, $u_n < M_\varphi < v_n$. On a alors, pour tout $n \geq 0$,

$$q_n = \varphi_n(u_n) < \varphi_n(M_\varphi) < \varphi_n(v_n) = q_n + 1$$

ce qui assure que $\left[\varphi_n(M_\varphi)\right] = q_n$ est bien un nombre premier.

□

Formuler ainsi, on voit que le théorème original de Mills est l'application du précédent à la fonction $\varphi(x) = x^3$. Le fait que, pour ce choix de φ, la propriété (R) est bien vérifiée découle d'un théorème de Ingham (voir [I]) qui assure que $p_{n+1} - p_n = O(p_n^{5/8})$, comme nous le verrons plus loin. Le théorème des nombres premiers, permet d'exhiber beaucoup de fonction φ qui satisfont la propriété (R). Par exemple, la fonction $\varphi(x) = 2^x$ (le fait que φ satisfait la propriété (R) peut-être vu plus directement comme application du théorème de Bertrand-Tchebychev). Ainsi, il existe un réel $\alpha > 0$ tel que tous les entiers $[\alpha], [2^\alpha], \left[2^{2^\alpha}\right], \cdots$ sont des nombres premiers.

Bien sur, en terme de comportement asymptotique, plus la fonction φ a une croissance lente, plus il en est de même de la suite $([\varphi_n(M_\varphi)])_n$. Si l'on dispose de bonnes majorations de la suite $(p_{n+1} - p_n)_n$, on est en mesure d'exhiber des fonctions φ satisfaisant aux hyptohèses du théorème 1 et telles que les suites $([\varphi_n(M_\varphi)])_n$ aient une croissance bien plus modérée que celle de $([M^{3^n}])_n$. Une des conjectures les plus fortes sur le comportement de cette suite est celle de Cramér (cf [C]) qui prévoit que $p_{n+1} - p_n = O((\log p_n)^2)$, c'est-à-dire qu'il existe une constante réelle $K > 0$ telle que $p_{n+1} \leq p_n + K(\log p_n)^2$ pour tout $n \geq 1$. Plaçons-nous sous cette conjecture et considérons la fonction $f(x) = x(\log x)^\lambda$ où $\lambda > 2$ désigne une constante réelle. Pour $x \gg 0$ fixé, si p_n désigne le plus grand nombre premier tel que $p_n \leq f(x)$, on a

$$p_n \leq f(x) < p_{n+1} \leq p_n + K(\log p_n)^2 \leq f(x) + K(\log f(x))^2$$

Un calcul élémentaire de développement asymptotique montre que

$$f(x+1) - f(x) = (\log x)^\lambda + o\left((\log x)^\lambda\right)$$

Par ailleurs, on a

$$(\log f(x))^2 = (\log x)^2 + 2\lambda \log x \log\log x + \lambda^2(\log\log x)^2 = (\log x)^2 + o((\log x)^2)$$

On en déduit que pour $x \gg 0$, on a $f(x) + K(\log f(x))^2 < f(x+1) - 1$. Ainsi, si l'on considère alors la fonction continue et affine par morceaux φ qui vérifie

$\varphi(n) = [f(n)]$ pour tout $n \geq 2$ entier et φ est affine sur tous les intervalles $[n, n+1]$, alors φ satisfait aux conditions du théorème 1 et l'on voit que la suite $([\varphi_n(M_\varphi)])_n$ a une croissance bien inférieure à $([M^{3^n}])_n$.

Introduisons quelques définitions. On se donne une fonction φ comme dans l'énoncé du théorème (mais on ne suppose pas forcément que φ satisfait (R)). Pour une partie $A \subset \mathbb{N} - \{0, 1\}$ donnée, on appelle *constante de Mills* relative à φ et A tout réel $M > 0$ tel que, pour tout $n \geq 0$, $[\varphi_n(M)] \in A$. On définit alors l'*ensemble de Mills* relatif à φ et A comme étant l'ensemble $\mathscr{M}_\varphi(A)$ constitué de toutes les constantes de Mills (relative à φ et A). On a ainsi :

$$\mathscr{M}_\varphi(A) = \{\alpha \in \mathbb{R} / \ \forall n \in \mathbb{N}, \ [\varphi_n(\alpha)] \in A\}$$

On suppose désormais que φ vérifie $\varphi(\mathbb{N}) \subset \mathbb{N}$. Si l'on prend $\alpha \in \mathscr{M}_\varphi(A)$ et que, pour tout $n \geq 0$, on pose $p_n = [\varphi_n(\alpha)] \in A$ alors, puisque φ est croissante, on a $p_n \leq \varphi_n(\alpha) < p_n + 1 \Longrightarrow \varphi(p_n) \leq \varphi_{n+1}(\alpha) < \varphi(p_n + 1)$ et donc $\varphi(p_n) \leq p_{n+1} < \varphi(p_n + 1)$. Ainsi, avec cette hypothèse supplémentaire, il existe une application

$$\begin{array}{rccl} \theta_{\varphi,A} : & \mathscr{M}_\varphi(A) & \longrightarrow & \mathscr{E}_\varphi(A) = \left\{(p_n)_n \in A^{\mathbb{N}} / \ \forall n \geq 0, \ \varphi(p_n) \leq p_{n+1} < \varphi(p_n + 1)\right\} \\ & \alpha & \longmapsto & ([\varphi_n(\alpha)])_n \end{array}$$

Lemme 1.– *Si l'application φ vérifie qu'il existe $\lambda > 1$ tel que, pour tous $x, y \in [2, +\infty[$, on ait $|\varphi(x) - \varphi(y)| \geq \lambda |x - y|$ (e.g. φ dérivable et $\inf_{t \in [2,+\infty[} \varphi'(t) > 1$) alors l'application $\theta_{\varphi,A}$ est injective.*

Preuve : Soient $\alpha \neq \beta$ deux éléments de $\mathscr{M}_\varphi(A)$. Par récurrence immédiate, on a, pour tout $n \geq 0$, $|\varphi_n(\alpha) - \varphi_n(\beta)| \geq \lambda^n |\alpha - \beta|$. Pour un entier n_0 tel que $\lambda^{n_0} |\alpha - \beta| \geq 1$, on ne peut avoir $[\varphi_{n_0}(\alpha)] = [\varphi_n(\beta)]$, car dans ces conditions on aurait $|\varphi_n(\alpha) - \varphi_n(\beta)| < 1$. Ainsi, $\theta_{\varphi,A}(\alpha) \neq \theta_{\varphi,A}(\beta)$ et l'application $\theta_{\varphi,A}$ est donc bien injective.

□

On supposera désormais cette hypothèse satisfaite. En résumé : $\varphi : [2, +\infty[\longrightarrow \mathbb{R}$ est une application qui vérifie

a) La fonction φ est strictement croissante et continue.

b) Pour tout réel $x \geq 2$, $\varphi(x) \geq x$. (En particulier $\lim_{x \to +\infty} \varphi(x) = +\infty$ et donc φ est un homéomorphisme entre $[2, +\infty[$ et $[\varphi(2), +\infty[$).

c) Pour tout entier $n \geq 2$, $\varphi(n) \in \mathbb{N}$.

d) Il existe un réel $\lambda > 1$ tel que, pour tous réels $x, y \geq 2$, $|\varphi(x) - \varphi(y)| \geq \lambda |x - y|$.

Lemme 2.– *Une suite $(p_n)_n \in \mathscr{E}_\varphi(A)$ n'est pas dans l'image de $\theta_{\varphi,A}$ si et seulement si $\forall n \gg 0$, $p_{n+1} + 1 = \varphi(p_n + 1)$. En conséquence de quoi, l'application $\theta_{\varphi,A}$ est bijective si et seulement si l'ensemble A vérifie la condition (S) suivante :*

$$(S) \ \forall (p_n)_n \in \mathscr{E}_\varphi(A) \ \forall n_0 \geq 0 \ \exists n \geq n_0 \ p_{n+1} \neq \varphi(p_n + 1) - 1$$

Preuve : Reprenons la construction introduite dans la preuve du théorème : pour tout entier n, posons

$$u_n = \varphi_n^{-1}(p_n)$$
$$v_n = \varphi_n^{-1}(p_n + 1)$$

Ces réels sont bien définis, à cause de la définition de $\mathscr{E}_\varphi(A)$. Par stricte croissance de la fonction φ_n^{-1}, on a immédiatement $u_n < v_n$ pour tout $n \geq 0$. Maintenant,

$$u_{n+1} = \varphi_{n+1}^{-1}(p_{n+1}) \geq \varphi_{n+1}^{-1}(\varphi(p_n)) = \varphi_n^{-1}(p_n) = u_n$$
$$v_{n+1} = \varphi_{n+1}^{-1}(p_{n+1} + 1) \leq \varphi_{n+1}^{-1}(\varphi(p_n + 1)) = \varphi_n^{-1}(p_n + 1) = v_n$$

Les suites $(u_n)_n$ et $(v_n)_n$ sont donc respectivement croissante et décroissante et elles convergent donc respectivement vers des réels u_∞ et v_∞ qui vérifient $u_\infty \leq v_\infty$. Elles sont en fait adjacentes (i.e. $u_\infty = v_\infty$). En effet, si $\alpha \in]u_\infty, v_\infty[$, alors, pour tout $n \geq 0$, on a $u_n < \alpha < v_n$ et donc $p_n = \varphi_n(u_n) < \varphi_n(\alpha) < \varphi_n(v_n) = p_n + 1$. Ainsi, $[\varphi_n(\alpha)] = p_n$. Ceci prouve que tous les éléments de $]u_\infty, v_\infty[$ ont même image par $\theta_{\varphi,A}$, ce qui nie l'injectivité de cette application si $]u_\infty, v_\infty[\neq \emptyset$.

Posons $\alpha = u_\infty = v_\infty$ et distinguons deux cas :

1/ La suite $(v_n)_n$ est stationnaire. Cette hypothèse équivaut alors à la condition de l'énoncé : $\forall n \gg 0,\ p_{n+1} + 1 = \varphi(p_n + 1)$. Si $\alpha' \in \mathbb{R}$ était tel que $(p_n)_n = \theta_{\varphi,A}(\alpha')$, alors pour tout $n \gg 0$, on aurait $u_n \leq \alpha' < v_n = \alpha$, ce qui rendrait impossible le fait que $\lim_n u_n = \alpha$. Le suite $(p_n)_n$ n'est donc pas dans l'image de $\theta_{\varphi,A}$.

2/ La suite $(v_n)_n$ n'est pas stationnaire. Ceci implique que, pour tout $n \geq 0$, $u_n \leq \alpha < v_n$ et donc que $p_n \leq \varphi_n(\alpha) < p_n + 1$. Ainsi, $[\varphi_n(\alpha)] = p_n$ pour tout $n \geq 0$ et $(p_n)_n = \theta_{\varphi,A}(\alpha)$.

□

Remarques.– a) La condition (S) est satisfaite par la condition plus forte

$$(S')\ \exists a_0 \geq 0,\ \forall a \in A,\ a \geq a_0 \Longrightarrow \varphi(a+1) - 1 \notin A$$

b) L'ensemble $\mathscr{E}_\varphi(A) - \theta(\mathscr{M}_\varphi(A))$ est au plus dénombrable. En effet, d'après ce qui précède, cet ensemble peut être vu comme un sous-ensemble du produit cartésien $\mathscr{F} \times \mathscr{R}$ où $\mathscr{F}$ désigne l'ensemble des suites finies d'entiers et $\mathscr{R}$ l'ensemble des suites récurrentes $(\lambda_n)_n$ vérifiant $\lambda_0 \in \mathbb{N}$ et pour tout $n \geq 0$, $\lambda_{n+1} = \varphi(\lambda_n + 1) - 1$. Ces deux ensembles sont visiblement dénombrables.

c) En application du lemme 2 on voit, par exemple, que si

$$A = \{2, \varphi(3) - 1, \varphi_2(3) - 1, \cdots\}$$

alors $\mathscr{M}_\varphi(A) = \emptyset$. De même, si l'on considère la partie

$$A = \{2, \varphi(2), \varphi_2(2), \varphi_3(2), \cdots\}$$

on voit que $\mathscr{M}_\varphi(A) = A$ est une partie discrète de $\mathbb{R}$ et donc fermée. Cette propriété est en fait très générale :

Lemme 3.– *Si l'ensemble A vérifie la condition (S) alors l'ensemble $\mathscr{M}_\varphi(A)$ est une partie fermée de $\mathbb{R}$.*

Preuve : Soit $(\alpha_k)_k$ une suite d'éléments de $\mathscr{M}_\varphi(A)$ convergeant vers un réel α. Fixons un entier n. Par continuité, on a $\lim_k \varphi_n(\alpha_k) = \varphi_n(\alpha)$ si bien qu'il existe un indice k_0 tel que pour tout $k \geq k_0$, on a $|\varphi_n(\alpha_k) - \varphi_n(\alpha)| < 1$ et, par suite, on a

$$[\varphi_n(\alpha_k)] \in \{[\varphi_n(\alpha)], [\varphi_n(\alpha)] + 1, [\varphi_n(\alpha)] - 1\}$$

Le dernier ensemble considéré comptant un nombre fini d'éléments, il existe donc une sous-suite $(\alpha_{\sigma(k)})_k$ telle que la suite $([\varphi_n(\alpha_{\sigma(k)})])_k$ soit constante (égale à un certain $p_n \in A$). Puisque pour tout $k \geq 0$, $p_n \leq \varphi_n(\alpha_{\sigma(k)}) < p_n + 1$, par passage à la limite sur k, on a donc soit $[\varphi_n(\alpha)] = p_n \in A$, soit $\varphi_n(\alpha) = [\varphi_n(\alpha)] = p_n + 1$. Montrons que ce dernier cas est exclu : si $\varphi_n(\alpha) = p_n + 1$, alors, on peut choisir la sous-suite $(\alpha_{\sigma(k)})_k$ de manière à ce qu'elle soit croissante. Elle ne peut bien sur pas être constante, car alors on aurait $[\varphi_n(\alpha)] = p_n$. En appliquant le même raisonnement que précédemment au rang $n+1$, on voit qu'il existe une sous-suite $(\alpha_{\psi(k)})_k$ de la suite $(\alpha_{\sigma(k)})_k$ telle que pour tout $k \geq 0$, $p_{n+1} \leq \varphi_{n+1}(\alpha_{\psi(k)}) < p_{n+1} + 1$ pour un certain entier $p_{n+1} \in A$. La suite $(\alpha_{\psi(k)})_k$ est croissante et non constante et comme $\varphi_{n+1}(\alpha)$ est entier, on en déduit que $\varphi_{n+1}(\alpha) = p_{n+1} + 1$, c'est-à-dire $p_{n+1} = \varphi(p_n + 1) - 1$. Par récurrence, on construit ainsi une suite $(p_n)_n \in \mathscr{E}_\varphi(A)$ qui empêche à l'ensemble A de satisfaire à la condition (S).

Ainsi, pour tout $n \geq 0$, $[\varphi_n(\alpha)] \in A$ et donc $\alpha \in \mathscr{M}_\varphi(A)$. L'ensemble $\mathscr{M}_\varphi(A)$ est bien fermé.

□

Le caractère injectif de l'application $\theta_{\varphi,A}$ montre que le cardinal de $\mathscr{M}_\varphi(A)$ est intimement lié au nombre d'éléments de A qui figurent dans les intervalles $[\varphi(a), \varphi(a+1)[$ quand a parcourt A. Par exemple, si A vérifie la condition

$$(T)\ \exists M > 0,\ \forall a \in A,\ a \geq M \Longrightarrow \sharp A \cap [\varphi(a), \varphi(a+1)[\geq 2$$

alors l'ensemble $\mathscr{E}_\varphi(A)$ est à la puissance du continu (ce qui est donc aussi le cas de $\mathscr{M}_\varphi(A)$, d'après ce qui précède). Pour voir ce fait, considérons un élément $a \in A$ tel que $a \geq M$. Il existe alors deux éléments distincts $\omega(0), \omega(1) \in [\varphi(a), \varphi(a+1)[$. De même, il existe deux éléments distincts $\omega(0,0), \omega(0,1) \in [\varphi(\omega(0)), \varphi(\omega(0)+1)[$ et deux éléments distincts $\omega(1,0), \omega(1,1) \in [\varphi(\omega(1)), \varphi(\omega(1)+1)[$. Par récurrence, on construit donc une application

$$\omega : \bigsqcup_{n\geq 1} \{0,1\}^n \longrightarrow A$$

qui vérifie que, pour tout $n \geq 1$ et tout $(i_1, \cdots, i_n) \in \{0,1\}^n$, on ait $\omega(i_1, \cdots, i_n, 0) \neq \omega(i_1, \cdots, i_n, 1)$ et $\omega(i_1, \cdots, i_n, 0), \omega(i_1, \cdots, i_n, 1) \in [\varphi(\omega(i_1, \cdots, i_n)), \varphi(\omega(i_1, \cdots, i_n))+1)[$. Il est clair que l'application ω est injective. Par passage à la limite, on en déduit que l'application

$$\begin{array}{rccc} \Omega : & \{0,1\}^{\mathbb{N}^*} & \longrightarrow & \mathscr{E}_\varphi(A) \\ & (i_n)_n & \longmapsto & (a, \omega(i_1), \omega(i_1,i_2), \omega(i_1,i_2,i_3), \cdots) \end{array}$$

est elle-même injective, ce qui prouve que le cardinal de $\mathscr{E}_\varphi(A)$ est $2^{\aleph_0}$.

Dans cette situation, on a une intéressante conséquence topologique :

Lemme 4.– *Si l'ensemble A vérifie la condition (T) alors l'ensemble $\mathscr{M}_\varphi(A)$ est sans point isolé.*

Preuve : Considérons un élément $\alpha \in \mathscr{M}_\varphi(A)$ et un réel $\varepsilon > 0$. Notons $(p_n)_n = \theta_{\varphi,A}(\alpha)$ et considérons un indice n_0 tel que $p_{n_0} \geq M$ (le M de la condition (T)) et $1/\lambda^{n_0} < \varepsilon$ (le λ de la condition d) satisfaite par φ). Pour $n \leq n_0$ posons $q_n = p_n$. Par (T), il existe $q_{n_0+1} \in [\varphi(p_{n_0}), \varphi(p_{n_0}+1)[\cap A$ tel que $q_{n_0+1} \neq p_{n_0+1}$. Toujours par (T), on voit que pour tout $n \geq n_0+2$ on peut choisir $q_n \in A$ de sorte que la suite $(q_n)_n$ soit élément de $\mathscr{E}_\varphi(A)$ et qu'elle vérifie que pour tout $n \geq n_0+2$ on ait $q_{n+1} \neq \varphi(p_n+1)-1$. On peut donc considèrer l'élément $\beta = \theta^{-1}_{\varphi,A}((q_n)_n)$ qui vérifie, par construction, que $\alpha \neq \beta$.

Puisque $[\varphi_{n_0}(\alpha)] = p_{n_0} = q_{n_0} = [\varphi_{n_0}(\beta)]$, on en déduit que $|\varphi_{n_0}(\alpha) - \varphi_{n_0}(\beta)| < 1$. Mais comme, $|\varphi_{n_0}(\alpha) - \varphi_{n_0}(\beta)| \geq \lambda^{n_0}|\alpha-\beta|$, on en déduit finalement que $|\alpha-\beta| < \varepsilon$. Le point α n'est donc pas un point isolé de l'ensemble $\mathscr{M}_\varphi(A)$.

□

On va maintenant s'intéresser à trouver une condition suffisante simple pour que $\mathscr{M}_\varphi(A)$ soit un espace topologique totalement discontinu. Commençons par remarquer que dans $\mathbb{R}$, puisque les parties connexes sont les intervalles, une partie est totalement discontinue si et seulement si elle est d'intérieur vide. Ainsi, on a

$$\begin{array}{ll} & \mathscr{M}_\varphi(A) \text{ n'est pas totalement discontinu} \\ \iff & \overset{\circ}{\mathscr{M}_\varphi}(A) \neq \emptyset \\ \iff & \exists \alpha < \beta,\ ]\alpha,\beta[\subset \mathscr{M}_\varphi(A) \\ \iff & \exists \alpha < \beta,\ \forall n \geq 0,\ \{\{\varphi_n(\alpha), \varphi_n(\beta)\}\} \subset A \end{array}$$

où, pour $x < y$, $\{\{x,y\}\} = \{[t] /\ t \in]x,y[\}$. On voit donc qu'il est très facile de construire des parties A telles que $\mathscr{M}_\varphi(A)$ ne soit pas totalement discontinu, par exemple la partie

$$A = \bigcup_{n\geq 0} \{\{\varphi_n(\alpha), \varphi_n(\beta)\}\}$$

Les intervalles $[\varphi_n(\alpha), \varphi_n(\beta)]$ ont une longueur qui croît au moins aussi vite que $|\alpha-\beta|\lambda^n$, de sorte que, pour que $\mathscr{M}_\varphi(A)$ ne soit pas totalement discontinu, il faut que A contienne des intervalles d'entiers de longueur arbitrairement grande. On obtient ainsi :

Lemme 5.– *Si les intervalles d'entiers inclus dans A sont de longueurs bornées, c'est-à-dire si A vérifie la condition*

$$(U)\ \exists k \geq 0,\ \forall n \geq 0,\ [\![n, n+k]\!] \not\subset A$$

alors l'ensemble $\mathscr{M}_\varphi(A)$ est une partie totalement discontinue de $\mathbb{R}$.

Remarque : A la différence des conditions (T) et (S), la condition (U) est indépendante du choix de la fonction φ.

Théorème 2.— *Si l'ensemble A satisfait aux conditions (S), (T) et (U) alors l'ensemble de Mills $\mathscr{M}_\varphi(A)$ est non vide et est la limite croissante d'ensembles homéomorphes à l'ensemble triadique de Cantor (plus précisément, pour tout réel $w > \inf \mathscr{M}_\varphi(A)$, la partie $\mathscr{M}_\varphi(A) \cap [2, w]$ est homéomorphe à l'ensemble triadique de Cantor).*

Preuve : Ce théorème est la conséquence du fait qu'un espace topologique est homéomorphe à l'ensemble triadique de Cantor si et seulement si c'est un espace métrique compact, totalement discontinu et sans point isolé.

□

Corollaire 1.— *Soit $h \geq 3$ un entier. L'ensemble*

$$\mathscr{M} = \left\{\alpha \in \mathbb{R} / \ \forall n \geq 0, \ \left[\alpha^{h^n}\right] \text{ est un nombre premier}\right\}$$

vérifie que pour tout $w > \inf \mathscr{M}$, la partie $\mathscr{M} \cap [2, w]$ est homéomorphe à l'ensemble triadique de Cantor.

Preuve : On choisit ici $\varphi(x) = x^h$ et $A = \mathscr{P}$. La fonction φ satisfait bien aux conditions a,b,c) et à la condition d) pour le choix de $\lambda = h2^{h-1}$.

• L'ensemble $\mathscr{P}$ vérifie la condition (S) car il satisfait en fait à la condition (S'), puisque pour tout a entier, a divise $(a+1)^h - 1$.

• Pour montrer que $\mathscr{P}$ vérifie la condition (T) reprenons le résultat de Ingham qui assure que $p_{n+1} - p_n = O(p_n^{\frac{5}{8}})$. On a aussi $p_{n+2} - p_n = O(p_n^{\frac{5}{8}})$ et l'on peut donc trouver une constante $K > 0$ telle que $p_{n+2} - p_n \leq K p_n^{\frac{5}{8}}$ pour tout entier $n \geq 1$. Considérons alors le réel $M = K^{\frac{8}{3h-8}}$ et prenons un entier $a \geq M$. On note p_n le plus grand premier inférieur à a^h. On a donc

$$p_n \leq a^h < p_{n+1} < p_{n+2} \leq p_n + K p_n^{\frac{5}{8}} \leq a^h + K a^{\frac{5h}{8}} \leq a^h + a^{\frac{3h-8}{8} + \frac{5h}{8}} = a^h + a^{h-1} < (a+1)^h$$

et donc $p_n, p_{n+1} \in [a^h, (a+1)^h[$.

Notons que pour $h = 2$ la preuve ne marche pas. Le fait que $\mathscr{P}$ vérifie la condition (T) quand $h = 2$ est en fait toujours un problème ouvert (voir conjecture de Legendre).

• La longueur maximale des intervalles d'entiers inclus dans $\mathscr{P}$ est 2, ainsi $\mathscr{P}$ satisfait bien la condition (U).

□

Corollaire 2.— *Soit $N \geq 2$ un entier. L'ensemble*

$$\mathscr{M} = \left\{\alpha \in \mathbb{R} / \ [\alpha], [N^\alpha], \left[N^{N^\alpha}\right], \cdots \text{ sont tous des nombres premiers}\right\}$$

vérifie que pour tout $w > \inf \mathscr{M}$, la partie $\mathscr{M} \cap [2, w]$ est homéomorphe à l'ensemble triadique de Cantor.

Preuve : On choisit ici $\varphi(x) = N^x$ et $A = \mathscr{P}$. La fonction φ satisfait bien aux conditions a,b,c) et à la condition d) pour le choix de $\lambda = N^2 \log N$.

• L'ensemble $\mathscr{P}$ vérifie la condition (S) car il satisfait en fait à la condition (S') : si $a \gg 0$ est premier, alors $a+1$ ne l'est pas et donc $N^{a+1}-1$ non plus.

• Pour montrer que $\mathscr{P}$ vérifie la condition (T), le raffinement du théorème de Bertrand-Tchébychev suivant est suffisant : pour $n \geq 6$ il existe au moins deux nombres premiers entre n et $2n$. On prend alors $a \geq 3$, et l'on a $N^a < 2N^a \leq N^{a+1}$ et donc $\sharp\mathscr{P} \cap [N^a, N^{a+1}[\geq 2$.

• $\mathscr{P}$ vérifie la condition (U), comme vu précedemment.

□

Un exemple sans les nombres premiers : On considère deux entiers $a, b \geq 2$ tels que $b > a$ et $a \nmid (b-1)$. L'ensemble

$$\mathscr{M} = \{x \geq a / \ \forall n \geq 0, \ a \text{ divise } [b^n x]\}$$

vérifie que pour tout $w > a$, la partie $\mathscr{M} \cap [a, w]$ est homéomorphe à l'ensemble triadique de Cantor. Pour voir ceci, on choisit $\varphi(x) = bx$ et $A = a\mathbb{N} - \{0\}$.

• A vérifie la condition (S') car si $n \in A$, alors $\varphi(n+1) - 1 = bn + (b-1) \notin A$ puisque $a \nmid (b-1)$.

• A vérifie la condition (T) car si $n \in A$, alors $\{bn, bn+a\} \subset A \cap [bn, bn+b[$ puisque $a < b$.

• A vérifie visiblement la condition (U).

En dépit des résultats topologiques établis sur l'ensemble de Mills, il n'est pas facile de prévoir la mesure de $\mathscr{M}_\varphi(A)$. En effet, il existe des parties de $\mathbb{R}$ homéomorphes à l'ensemble triadique de Cantor qui ne sont pas de mesure nulle, par exemple les ensembles de Smith-Volterra-Cantor (voir [P]). Nous allons finir ce texte en montrant que $\mathscr{M}_\varphi(\mathscr{P})$ est bien de mesure nulle lorsque $\varphi(x) = N^x$.

Proposition 1.– *On considère la fonction $\varphi(x) = N^x$ où $N \geq 2$ est un entier. Si l'ensemble A vérifie la condition*

(V) Il existe un entier $n_0 \geq 0$ tel que la série $\displaystyle\sum_{a \in A} \frac{1}{a \log_N a \cdots \log_N^{[n_0]} a}$ converge

alors l'ensemble $\mathscr{M}_\varphi(A)$ est de mesure de Lebesgue nulle.

Preuve : On a $\varphi^{-1}(x) = \log_N x$ et si $n \geq 0$, on notera $\varphi_n^{-1}(x) = \log_N^{[n]} x = \log_N \circ \cdots \circ \log_N(x)$. Pour tout $n \geq 0$ et tout $w \notin A$ entier, on considère l'ensemble

$$\mathscr{M}_n = \{\alpha \in [2, w] / \ \forall k = 0, \cdots, n, \ [\varphi_k(\alpha)] \in A\}$$

La suite d'ensembles $(\mathscr{M}_n)_n$ est visiblement décroissante et comme $\mathscr{M}_\varphi(A) \cap [2, w] = \displaystyle\bigcap_n \mathscr{M}_n$, on voit que $\mu(\mathscr{M}_\varphi(A) \cap [2, w]) = \lim_n \mu(\mathscr{M}_n)$.

Pour $n \geq 1$, on considère l'ensemble $\mathscr{E}_n = \bigcup_{p \in X_n} [p, p+1[$ où

$$X_n = \left\{ p \in A / \ \exists p_0, \cdots, p_n \in A, \ \middle| \ \begin{array}{l} a) \ p_0 \in [1, w], \\ b) \ \forall k \leq n-1, \ N^{p_k} \leq p_{k+1} < N^{p_k+1}, \\ c) \ p = p_n. \end{array} \right\}$$

Pour $\alpha \in \mathscr{M}_n$ et $k = 0, \cdots, n$, on pose $p_k = [\varphi_k(\alpha)] \in A$. On a $p_0 = [\alpha] \in [0, w]$ et, pour tout $k = 0, \cdots, n$, on a $p_k \leq \varphi_k(\alpha) < p_k + 1$. On en déduit que $\varphi_n(\alpha) \in [p_n, p_n + 1[$ et, pour tout $k = 0, \cdots, n-1$, $N^{p_k} \leq N^{\varphi_k(x)} = \varphi_{k+1}(x) < N^{p_k+1}$ et donc $N^{p_k} < p_{k+1} = [\varphi_{k+1}(x)] < N^{p_k+1}$. Ainsi, $\varphi_n(\alpha) \in \mathscr{E}_n$.

Réciproquement, considérons un réel α tel que $\varphi_n(\alpha) \in \mathscr{E}_n$. Il existe donc une suite $p_0, \cdots, p_n \in A$ telle que $p_0 \in [1, w]$, $\forall k = 0, \cdots, n-1$, $N^{p_k} < p_{k+1} < N^{p_k+1}$ et $\varphi_n(\alpha) \in [p_n, p_n + 1[$. On a $[\varphi_n(\alpha)] = p_n \in A$ et comme $p_n \leq \varphi_n(\alpha) < p_n + 1$ on a $\log_N p_n \leq u_{n-1}(x) < \log_N(p_n + 1)$. Puisqu'il n'y a pas d'entier entre $\log_N p_n$ et $\log_N(p_n + 1)$, on en déduit que $p_{n-1} = [u_{n-1}(\alpha)] = [\log_N p_n]$. Par récurrence on montre de la même façon que $p_k = [\varphi_k(\alpha)]$ pour tout $k = 0, \cdots, n$. Puisque $w \notin A$, on a $\alpha < p_0 + 1 \leq w$ et donc $\alpha \in [1, w]$. Ainsi, $\alpha \in \mathscr{M}_n$.

On vient donc de montrer que $\alpha \in \mathscr{M}_n \Longleftrightarrow \varphi_n(\alpha) \in \mathscr{E}_n$, et l'on en déduit que

$$\begin{aligned} \mu(\mathscr{M}_n) &= \sum_{1 \leq p_0 \leq w} \ \sum_{N^{p_0} < p_1 < N^{p_0+1}} \cdots \sum_{N^{p_{n-1}} < p_n < N^{p_{n-1}+1}} \left(\log_N^{[n]}(p_n + 1) - \log_N^{[n]}(p_n) \right) \\ &= \sum_{p \in X_n} \left(\log_N^{[n]}(p + 1) - \log_N^{[n]}(p) \right) \end{aligned}$$

Puisque $X_n \subset [\varphi_n(1), \varphi_n(w)]$, on a donc

$$\mu(\mathscr{M}_n) \leq \sum_{p \in [\varphi_n(1), \varphi_n(w)] \cap A} \left(\log_N^{[n]}(p + 1) - \log_N^{[n]}(p) \right)$$

Pour $n \geq 2$ et $x \in [\varphi_n(1), \varphi_n(w)]$, on a

$$(\log_N^{[n]})'(x) = \frac{1}{(\log N)^n x \log_N(x) \cdots \log_N^{[n-1]}(x)}$$

et le théorème des accroissements finis montre alors que

$$\begin{aligned} \mu(\mathscr{M}_n) &\leq \sum_{p \in [\varphi_n(1), \varphi_n(w)] \cap A} \left(\log_N^{[n]}(p + 1) - \log_N^{[n]}(p) \right) \\ &\leq \frac{1}{(\log(N))^n} \sum_{p \in [\varphi_n(1), \varphi_n(w)] \cap A} \frac{1}{p \log_N(p) \cdots \log_N^{[n-1]}(p)} \end{aligned}$$

Ainsi, pour $n \geq n_0 + 1$, on a

$$\mu(\mathscr{M}_n) \leq \frac{1}{(\log N)^n} \sum_{p \in A, \ \ p \geq \varphi_n(1)} \frac{1}{p \log_N(p) \cdots \log_N^{[n_0]}(p)} \underset{n \to +\infty}{\longrightarrow} 0$$

ce qui achève la preuve de la proposition.

□

L'ensemble $A = \mathscr{P}$ des nombres premiers vérifie bien la condition (V), puisque si l'on note $(p_n)_n$ la suite des nombres premiers, alors le théorème des nombres premiers assure que $p_n \simeq n \log n$ et l'on a donc l'équivalent $p_n \log p_n \simeq n(\log n)^2$. La série $\sum_{p \in \mathscr{P}} \dfrac{1}{p \log p}$ est donc convergente par application du critère de Bertrand sur les séries.

Connaître la mesure de $\mathscr{M}_\varphi(\mathscr{P})$ est une chose, évaluer son entropie en est une autre, bien plus délicate. Nous ouvrons cette question à la sagacité du lecteur !

Nous avons fait figurer ci-après une petite annexe sur une autre question relative aux nombres premiers et à l'entropie. Bien que les considérations qui y sont développées sont dans le même thème que ce dont nous venons de parler, il n'y a pas de lien direct. Il nous a néanmoins semblé intéressant de faire figurer quelques part ces résultats.

Annexe : sur l'entropie de la suite des inverses des nombres premiers.

Si A désigne une partie du segment $[0, 1]$, alors pour tout $\varepsilon > 0$, on considère

$$N(\varepsilon) = \sharp\{k = 0, \cdots, [1/\varepsilon] /\ A \cap [k\varepsilon, (k+1)\varepsilon[\neq \emptyset\}$$

le nombre de "cases" du réseau de longueur ε qui rencontrent la partie A. On définit alors l'entropie de la partie A comme étant le réel

$$\mathrm{ent}(A) = \limsup_{\varepsilon \to 0} \frac{\log N(\varepsilon)}{\log 1/\varepsilon} \in [0, 1]$$

On considère une suite numérique $(u_n)_n$ strictement décroissante vers 0 et vérifiant $u_0 = 1$, et l'on considère la partie $A = \{u_n /\ n \in \mathbb{N}\}$. Pour $n \geq 0$, on pose $\varphi_n = u_n - u_{n+1}$, de sorte que la série $\sum \varphi_n$ est convergente vers 1. On voit alors que

$$N(\varepsilon) = [1/\varepsilon] - \sum_{n/\ \varphi_n > \varepsilon} ([u_n/\varepsilon] - [u_{n+1}/\varepsilon] - 1)$$

Ainsi, si l'on considère la suite $u_n = 1/n$ alors on a $\varphi_n = \dfrac{1}{n} - \dfrac{1}{(n+1)} = \dfrac{1}{n(n+1)}$. Si pour $\varepsilon > 0$ fixé on note $n_0(\varepsilon) = \left[\dfrac{1}{2\sqrt{\varepsilon}}\left(-\sqrt{\varepsilon} + \sqrt{\varepsilon + 4}\right)\right]$, on a alors

$$N(\varepsilon) = [1/\varepsilon] - \sum_{n=0}^{n_0(\varepsilon)} ([u_n/\varepsilon] - [u_{n+1}/\varepsilon] - 1) = [u_{n_0(\varepsilon)}/\varepsilon] - n_0(\varepsilon) \simeq_{\varepsilon \to 0} \frac{K}{\sqrt{\varepsilon}}$$

et l'on en déduit que $\mathrm{ent}(A) = 1/2$.

On s'intéresse dans cette annexe, à l'entropie de la suite $u_n = 1/p_n$ où $p_0 = 1$ et $(p_n)_{n\geq 1}$ désigne la suite strictement croissante des nombres premiers. Cette question est reliée au fait que le calcul de l'entropie est dépend intimement lié des variations de la fontion $\varphi_n = 1/p_n - 1/p_{n+1}$ et donc des variations de $p_{n+1} - p_n$, fonction pour le comportement de laquelle il existe bon nombre de conjectures. Rappelons, par exemple, que l'hypothèse de Riemann implique que $p_{n+1} - p_n = O(\sqrt{p_n}\log p_n)$ (ce dernier résultat étant toujours une conjecture). Cette implication a été démontrée par H. Cramér, qui conjectura par la suite quelque chose de beaucoup plus fort : $p_{n+1} - p_n = O(\log^2 p_n)$. Chacune de ces conjectures n'a pas la même conséquence entropique pour la suite $(1/p_n)_n$.

Un petit calcul machine montre, pour les premières valeurs de la suite $(p_n)_n$, que la fonction $\frac{\log N(\varepsilon)}{\log 1/\varepsilon}$ semble tendre vers $1/2$, c'est-à-dire que l'ensemble des inverses des nombres premiers serait d'entropie maximale (ce que prévoit bien la conjecture de Cramér). Le résultat général suivant montre que cette propriété entropique reste vraie sous une conjecture beaucoup plus faible :

Proposition 2.– *Pour tout $n \geq 0$, on considère $u_n = 1/p_n$ où $p_0 = 1$ et $(p_n)_{n\geq 1}$ désigne une suite strictement croissante d'entiers. On note alors $A = \{u_n /\ n \in \mathbb{N}\}$. Si $(p_{n+1} - p_n) = p_n^{o(1)}$ alors $\mathrm{ent}(A) = 1/2$.*

Preuve : Puisque la suite $(u_n)_n$ est une sous-suite de la suite $(1/n)_n$, on a immédiatement $\mathrm{ent}(A) \leq 1/2$. Supposons maintenant que $p_{n+1} - p_n = p_n^{o(1)}$, on a alors $p_n \simeq p_{n+1}$ et donc

$$\varphi_n = \frac{p_{n+1} - p_n}{p_n p_{n+1}} = p_n^{-2+o(1)}$$

Notons $\omega(n)$ le $o(1)$ apparaissant dans cette inégalité. Pour $\varepsilon > 0$ fixé, on considère le plus grand entier $n_0(\varepsilon)$ tel que

$$\varepsilon < p_{n_0(\varepsilon)-1}^{-2+\omega(n_0(\varepsilon)-1)}$$

Cet entier existe bien puisque la suite $(p_n^{-2+\omega(n)})_n$ tend vers 0 et il est clair que $\lim_{\varepsilon\to 0} n_0(\varepsilon) = +\infty$. On choisit dans la suite un ε suffisamment petit pour que $-2 + \omega(n_0(\varepsilon) - 1) < 0$. On a alors, pour tout $n \geq n_0(\varepsilon)$, $\varphi_n \leq \varepsilon$ et donc

$$N(\varepsilon) \geq [1/\varepsilon] - \sum_{n=0}^{n_0(\varepsilon)-1} ([1/\varepsilon p_n] - [1/\varepsilon p_{n+1}]) = \left[\frac{1}{\varepsilon p_{n_0(\varepsilon)}}\right]$$

Puisque $p_{n-1} \simeq p_n$, il existe une constate $c > 0$ telle que $cp_n \leq p_{n-1}$ pour tout n, si bien que l'on a

$$(cp_{n_0(\varepsilon)})^{-2+\omega(n_0(\varepsilon)-1)} \geq p_{n_0(\varepsilon)-1}^{-2+\omega(n_0(\varepsilon)-1)} > \varepsilon$$

On en déduit que

$$\frac{1}{p_{n_0(\varepsilon)}} > c\varepsilon^{\frac{1}{2-\omega(n_0(\varepsilon)-1)}}$$

Comme $\lim\limits_{\varepsilon\to 0} n_0(\varepsilon) = +\infty$, en la variable ε, on a $\omega(n_0(\varepsilon)-1) = o(1)$. Ainsi,

$$N(\varepsilon) \geq \frac{1}{\varepsilon p_{n_0(\varepsilon)}} - 1 \geq c\varepsilon^{-1/2+o(1)} - 1 = \varepsilon^{-1/2+o(1)}$$

ce qui prouve finalement que $\mathrm{ent}(A) \geq 1/2$.

□

Quelques conjectures et liens entropiques.– On note $(p_n)_n$ la suite des nombres premiers et $1/\mathscr{P}$ l'ensemble des inverses des nombres premiers.

Conjecture de Firoozbakht[1]
La suite $(p_n^{1/n})_n$ est décroissante

$\Downarrow$

Conjecture de Cramér[2]
$\boxed{p_{n+1} - p_n = O((\log p_n)^2)}$

$\Downarrow$

Conjecture intermédiaire
$\boxed{p_{n+1} - p_n = p_n^{o(1)}} \Longrightarrow \mathrm{ent}\,(1/\mathscr{P}) = 1/2$

$\Downarrow$

Conjecture de Legendre
$\forall n \geq 0$, $\exists p$ premier tel que $n^2 < p < (n+1)^2$ $\Longrightarrow$

Conjecture d'Andrica[3]
$\forall n \geq 0,\ \sqrt{p_{n+1}} - \sqrt{p_n} < 1$ $\Longrightarrow$

$\boxed{p_{n+1} - p_n = O(\sqrt{p_n})}$

$\Downarrow$

Hypothèse de Riemann $\Longrightarrow$ $\boxed{p_{n+1} - p_n = O(\sqrt{p_n}\log p_n)} \Longrightarrow 1/3 \leq \mathrm{ent}\,(1/\mathscr{P}) \leq 1/2$ [4]

---

[1] Voir [R] p. 185.

[2] Voir [C].

[3] Voir [A].

[4] L'implication $p_{n+1} - p_n = O(\sqrt{p_n}\log p_n) \Longrightarrow \mathrm{ent}\,(1/\mathscr{P}) \geq 1/3$ se démontre avec les même idées que celles de la preuve de la proposition 2 et sa démonstration est laissée en exercice.

Bibliographie

[A] D. Andrica, *On a conjecture in prime number theory* , Studia Univ. Babes-Bolyai Math., 31-4, 44-48 (1986).

[C] H. Cramér, *On the order of magnitude of the difference between consecutive prime numbers*, Acta Arithmetica, 2, 23-46 (1936).

[I] A. Ingham, *On the difference between consecutive primes*, Quart. J. Math. Oxford 8, 255-266 (1937).

[M] W. Mills, *A prime-representing function*, Bull. Amer. Math. Soc., p. 604 (1947).

[P] A. Poelstra, *Homeomorphims Between Cantor Sets*, préprint, (2011).

[R] P. Ribenboim, *The Little Book of Bigger Primes* Second Edition. Springer-Verlag (2004).

Bruno Deschamps

Département de Mathématiques — Université du Maine
Avenue Olivier Messiaen, 72085 Le Mans cedex 9 - France

Laboratoire de Mathématiques Nicolas Oresme
CNRS UMR 6139

E-mail : Bruno.Deschamps@univ-lemans.fr