Qu'est-ce qu'un entier normal ? *

Gérald Tenenbaum
(Institut Élie Cartan, Nancy 1)

7 mai 1997

(version 5/11/2009)

*Leçon rédigée par G. Hanrot

Nombres premiers et entiers au hasard

Historiquement, la première brèche dans la représentation de l'arithmétique sous forme d'un ordre — un *cosmos* —, le premier soupçon de désordre — de *chaos* —, c'est la question des nombres premiers. Ne maintenons pas le suspense plus longtemps : il y en a une infinité. Voici une démonstration, qui, bien que très simple, est en un certain sens optimale. Elle est essentiellement due à Euler. Écrivons d'abord, pour $N \in \mathbb{N}^*$,

$$\log N \leqslant \sum_{n=1}^{N} \int_n^{n+1} \frac{\mathrm{d}t}{t} \leqslant \sum_{n=1}^{N} \frac{1}{n}.$$

Maintenant, faisons intervenir les nombres premiers. Formons le produit, sur tous les nombres premiers p n'excédant pas N, de $(1 + 1/p + 1/p^2 + \dots)$ en remarquant que, dans le développement du produit, on retrouve tous les entiers de 1 à N, plus quelques autres. La somme en n est donc majorée par

$$\prod_{p\leqslant N} \Big(1 + \frac{1}{p} + \frac{1}{p^2} + \dots\Big) = \prod_{p\leqslant N} \Big(1 + \frac{1}{p} + \frac{1}{p(p-1)}\Big),$$

ce que, grâce à l'inégalité bien connue $1 + u \leqslant \mathrm{e}^u$, nous pouvons finalement majorer par :

$$\begin{aligned} \exp\left\{\sum_{p\leqslant N} \frac{1}{p} + \sum_{p\leqslant N} \frac{1}{p(p-1)}\right\} &\leqslant \exp\left\{\sum_{p\leqslant N} \frac{1}{p} + \sum_{n\geqslant 2} \frac{1}{n(n-1)}\right\} \\ &\leqslant \exp\left\{\sum_{p\leqslant N} \frac{1}{p} + 1\right\}. \end{aligned}$$

Nous déduisons donc finalement que[1]

$$\sum_{p\leqslant N} 1/p \geqslant \log_2 N - 1$$

pour tout entier $N \geqslant 2$. Cette estimation facile fournit en fait le bon ordre de grandeur : on peut démontrer que la somme en p est asymptotiquement équivalente à $\log_2 N$.

Le fait que l'ensemble des nombres premiers est infini a été établi par Euclide. La démonstration quantitative d'Euler, que nous venons de donner,

[1] Ici et dans la suite, nous notons $\log_k$ la k-ième itérée de la fonction logarithme lorsque $k \geqslant 2$.

pose immédiatement le problème de la répartition de ces nombres premiers, ces entiers particuliers, dans l'ensemble de tous les nombres entiers. Étudier cette répartition, c'est en réalité appréhender le conflit entre la tendance profonde, lourde — osons : hiératique — à la régularité globale de cette suite, sur laquelle pèse la tâche prégnante d'engendrer celle, ultra-régulière, des nombres entiers, et la tendance non moins profonde, mais d'expression plus contingente — disons : erratique —, à l'irrégularité locale.

Sans répondre à cette vaste question, nous pouvons tirer immédiatement une autre conséquence de la divergence de la série des inverses des nombres premiers, sous la forme suivante : *il n'existe pas de notion probabiliste satisfaisante de l'idée de nombre au hasard.*

Pourquoi cela ? La raison est la suivante : tout choix conforme à l'intuition d'un nombre entier, disons N, au hasard, nécessite par exemple qu'il soit pair avec une probabilité $1/2$, et, plus généralement, qu'il soit divisible par a avec probabilité $1/a$, autrement dit $\mathbb{P}(a\mathbb{Z}) = 1/a$. Mais, si l'on impose cette condition, on obtient immédiatement que, pour chaque entier n fixé, la probabilité $\mathbb{P}(N = n)$ n'excède pas la probabilité que N ne soit divisible par aucun nombre premier plus grand que n. Pour des raisons qui tiennent au calcul des probabilités,[2] cette quantité vaut :

$$\mathbb{P}(p \nmid N,\ \forall p > n) = \prod_{p>n}(1 - 1/p) \geqslant \mathbb{P}(N = n),$$

et, puisque la série des $1/p$ diverge, le membre de gauche vaut 0. Donc $\mathbb{P}(N = n) = 0$ pour tout n. Autrement dit, il n'est pas possible de donner une définition conforme à l'intuition d'un entier au hasard en choisissant un modèle dans la théorie constituée des Probabilités : chaque entier apparaîtrait avec une probabilité nulle.

Densités

Ainsi, l'idée intuitive de nombre entier « normal » se heurte d'emblée à une difficulté conceptuelle. On contourne cet obstacle en introduisant la notion de *densité d'une suite d'entiers*. Que recouvre cette notion ? Étant donnée une partie $\mathcal{A} \subset \mathbb{N}$, nous dirons que la densité de $\mathcal{A}$ est, sous réserve d'existence, égale à la limite

$$\operatorname{dens} \mathcal{A} = \lim_{N\to\infty} \frac{1}{N}\big|\mathcal{A} \cap [1, N]\big|.$$

[2] Si a et b sont premiers entre eux, $ab\mathbb{Z} = a\mathbb{Z} \cap b\mathbb{Z}$, donc $\mathbb{P}(a\mathbb{Z} \cap b\mathbb{Z}) = 1/ab = \mathbb{P}(a\mathbb{Z})\mathbb{P}(b\mathbb{Z})$: en d'autres termes les événements $a\mathbb{Z}$ et $b\mathbb{Z}$ sont indépendants, et, *ipso facto*, leurs complémentaires dans $\mathbb{Z}$ également. Cela fournit la justification du calcul qui suit.

La notion vérifie bien le critère intuitif lié à la divisibilité puisque l'on a $\mathrm{dens}(a\mathbb{Z}) = 1/a$ pour tout entier $a \geqslant 1$, mais ce n'est pas une mesure de probabilité puisqu'à l'évidence elle ne satisfait pas le critère d'additivité dénombrable.

Un nombre normal, c'est un nombre qui appartient à une suite de densité 1. C'est un nombre qui possède une « probabilité » 1 d'être tiré « au hasard » pour la notion de hasard associée à celle de densité. Évidemment, aucun nombre donné n'est normal. Encore une illustration de la fameuse loi des petits nombres, selon laquelle ils sont en quantité trop faible pour satisfaire toutes les contraintes qui pèsent sur eux.

L'idée de nombre normal, c'est donc un concept limite, identifiable à *l'ensemble des propriétés non sélectives*, c'est-à-dire dont l'adjonction ne diminue la densité d'aucun ensemble de densité positive. En fait, on dira, plus concrètement, qu'une propriété $\mathcal{P}$ est normale, ou encore vérifiée presque partout — nous noterons pp pour presque partout — si, pour tout ensemble d'entiers $\mathcal{A}$ de densité d, l'ensemble $\mathcal{A}_{\mathcal{P}}$ des entiers de $\mathcal{A}$ qui vérifient la propriété $\mathcal{P}$ est encore de densité d.

Ainsi, la propriété « n n'est pas un carré » est normale, la propriété « n n'est pas un nombre premier » est normale, la propriété « n possède moins de $\log n$ diviseurs » est normale, la propriété « $2n$ peut s'écrire comme somme de deux nombres premiers » est normale. (Cette assertion est liée au célèbre problème de Goldbach ; on conjecture, avec Goldbach, que la propriété susmentionnée est non seulement normale, mais en fait vérifiée pour tout $n > 1$; on ignore si la conjecture de Goldbach est vraie, mais on sait qu'elle est effectivement satisfaite normalement : pour presque tout n, le nombre $2n$ est somme de deux nombres premiers.) En revanche, les propriétés « n est pair », « n est impair », « n est somme de deux carrés » ne sont pas normales. Erdős a conjecturé pendant plus de quarante ans qu'un nombre normal possède nécessairement, comme le nombre 15, deux diviseurs d et d' dont le rapport est compris entre 1 et 2 — ici par exemple 5 et 3 conviennent. Autrement dit, les nombres, comme 21, qui n'ont pas cette propriété[3] seraient « anormaux », parce que trop rares.

Conflit structural

Parmi les questions relatives à l'étude du concept de nombre normal, celles qui ont trait aux rapports statistiques entre la structure d'ordre et la structure multiplicative de l'ensemble $\mathbb{N}$ des entiers naturels sont parmi les plus complexes.

[3] Le plus petit rapport de deux diviseurs consécutifs de 21 vaut $7/3 > 2$.

La structure d'ordre est celle qui est issue de la notion de taille d'un nombre ; la structure multiplicative est celle qui reflète la décomposition des entiers dans le semi-groupe multiplicatif engendré par les nombres premiers.

Une bonne illustration de cette problématique consiste à comparer, dans l'ensemble des diviseurs d'un entier fixé, l'ordre usuel — issu de la structure additive — et l'ordre lexicographique. Voyons cela de plus près. Considérons un entier générique

$$n = p_1^{\alpha_1} \cdots p_k^{\alpha_k},$$

dont les facteurs premiers sont $p_1 < \cdots < p_k$. Les diviseurs de n sont les entiers de la forme

$$p_1^{\beta_1} \cdots p_k^{\beta_k},$$

avec $0 \leqslant \beta_j \leqslant \alpha_j$ $(1 \leqslant j \leqslant k)$. On peut associer à chaque diviseur le mot $\beta_k \cdots \beta_1$, et ensuite ranger ces mots (donc les diviseurs associés) dans l'ordre lexicographique. On compare ensuite avec l'ordre usuel sur les diviseurs. Les distorsions entre les deux suites obtenues mesurent le conflit entre les deux ordres.

Prenons un exemple. Les diviseurs de 30 sont

$$1,\ 2,\ 3,\ 5,\ 6,\ 10,\ 15,\ 30.$$

Dans l'ordre lexicographique, on a d'abord 1, 2, et 3 mais le diviseur qui succède immédiatement à 3, c'est 6, puisque $6 = 2 \times 3$. Puis viennent 5, 10, 15, 30. On constate donc une interversion de 5 et 6 entre l'ordre usuel et l'ordre lexicographique.

Considérer les rapports entre ces deux ordres, c'est finalement une manière de se demander ce qu'est un nombre normal. On a quelques idées, quelques modèles, d'ailleurs problématiques, pour les nombres normaux. Nous allons essayer de les décrire maintenant.

De Hardy–Ramanujan à Erdős–Kac

La première mention du concept de nombre normal dans la littérature est due à Hardy et Ramanujan, en 1917, dans un article que l'on considère généralement comme le premier acte de naissance de la théorie probabiliste des nombres — le second étant l'article d'Erdős et Kac de 1939 [10], sur lequel nous reviendrons dans la suite. Hardy et Ramanujan montrent la proposition suivante : *si $\omega(n)$ désigne le nombre de facteurs premiers de n, comptés sans multiplicité, alors*

$$\omega(n) \sim \log_2 n \qquad \text{pp.}$$

Autrement dit, un nombre normal n a environ $\log_2 n$ facteurs premiers. Autrement dit encore, pour chaque $\varepsilon > 0$, si l'on retire d'une suite de densité $d > 0$ les nombres n ayant plus de $(1+\varepsilon)\log_2 n$, ou moins de $(1-\varepsilon)\log_2 n$, facteurs premiers, la densité est inchangée.

La démonstration de Hardy et Ramanujan utilise une majoration assez technique pour le nombre $\pi_k(x)$ des entiers $\leqslant x$ ayant exactement k facteurs premiers ; leur estimation n'est pas très performante en toute généralité, mais elle est précise au voisinage, justement, de l'ordre normal, ce qui s'avère suffisant pour montrer que la somme des quantités $\pi_k(x)$ sur les valeurs de k « trop grandes » ou « trop petites » est négligeable en première approximation.[4]

Turán a découvert, dans les années trente, une nouvelle démonstration du théorème de Hardy et Ramanujan. Son approche est beaucoup plus simple et repose essentiellement sur la relation dont nous avons établi la moitié plus haut, soit

$$\sum_{p\leqslant N} 1/p = \log_2 N + O(1) \qquad (N \geqslant 3).$$

Par une simple interversion de sommation, Turán établit que

$$\sum_{n\leqslant N} (\omega(n) - \log_2 N)^2 \leqslant CN \log_2 N \qquad (N \geqslant 3),$$

où C est une constante absolue. Un argument bien connu en théorie des probabilités, l'inégalité de Bienaymé–Tchébychev, fournit alors que l'on a

$$|\omega(n) - \log_2 N| \leqslant \xi\sqrt{\log_2 N}$$

sauf peut-être pour CN/ξ^2 entiers $n \leqslant N$ — ce qui constitue une version quantitative du théorème de Hardy et Ramanujan.

En fait, la démonstration de Hardy et Ramanujan contient une meilleure majoration pour le nombre des exceptions. Donnons-la parce qu'on y voit poindre la loi de Gauss qui décrit plus complètement le phénomène. Un calcul facile permet de déduire des estimations de Hardy et Ramanujan la majoration

$$AN\left(e^{-\xi^2/2} + \frac{1}{(\log N)^a}\right),$$

pour le cardinal de l'ensemble des entiers exceptionnels, où A et a sont des constantes positives. On aperçoit effectivement ici la quantité $\mathrm{e}^{-\xi^2/2}$ évoquant une loi de Gauss que nous allons décrire à présent.

[4] En formule : $\sum_{|k-\log_2 x|>\varepsilon \log_2 x} \pi_k(x) = o(x)$ pour tout $\varepsilon > 0$ fixé et $x \to \infty$, où $\pi_k(x)$ désigne précisément le nombre des entiers $n \leqslant x$ tels que $\omega(n) = k$.

Les résultats de Hardy et Ramanujan ont été étendus dans deux directions. La plus connue, c'est le théorème d'Erdős et Kac, datant de 1939. Il fournit la probabilité asymptotique pour qu'un entier normal ait moins de $\log_2 N + z\sqrt{\log_2 N}$ facteurs premiers : pour tout nombre réel z, on a, lorsque $N \to \infty$,

$$\frac{1}{N}\Big|\Big\{n \leqslant N :\ \omega(n) \leqslant \log_2 N + z\sqrt{\log_2 N}\Big\}\Big| \sim \frac{1}{\sqrt{2\pi}}\int_{-\infty}^{z} e^{-u^2/2}\,\mathrm{d}u.$$

La loi de Gauss apparaît au second membre.

On raconte, et c'est corroboré par plusieurs témoins, que Kac a fait un exposé à Princeton où il conjecturait cette répartition asymptotique et mentionnait qu'il savait démontrer le résultat si l'on y remplaçait la fonction $\omega(n)$ par une fonction tronquée, ne comptant pas tous les facteurs premiers mais seulement les « petits » facteurs, inférieurs à une borne arbitraire mais fixée. Erdős était dans la salle. Il a immédiatement réalisé que si Kac savait conclure dans ce cadre restreint, alors il pouvait prouver la conjecture initiale en utilisant la méthode du crible de Brun — dont il était spécialiste et dont il avait compris les implications profondes avant beaucoup de gens. À la fin de l'exposé, il a levé la main et a dit : « *Je sais démontrer le théorème.* » Il raconte : « *Avec un peu d'impudence, on a pu dire que la théorie probabiliste des nombres était née* », selon ses propres termes. C'était une deuxième naissance — l'idée de nombre normal remonte tout de même à Hardy et Ramanujan.

L'idée sous-jacente, fournissant d'ailleurs l'origine de ce $\log_2 N$ omniprésent en théorie probabiliste des nombres, est très simple : si l'on définit sur $[1, N]$ des variables aléatoires ε_p à valeurs dans $\{0, 1\}$ par

$$\varepsilon_p = \begin{cases} 1 & \text{si } p|n, \\ 0 & \text{si } p \nmid n, \end{cases}$$

alors les ε_p se comportent statistiquement comme des variables indépendantes — deux nombres premiers différents donnent lieu à des conditions de divisibilité indépendantes — qui miment les fréquences empiriques dont rend compte la notion de densité. Autrement dit, ε_p est mimée par une variable aléatoire de Bernoulli Z_p définie sur un ensemble abstrait et dont la loi est donnée par la relation $\mathbb{P}(Z_p = 1) = 1/p$. Si cette approximation est valable en un sens convenable, alors la fonction $\omega(n)$, qui, après tout, n'est autre que

$$\omega(n) = \sum_{p \leqslant n} \varepsilon_p(n),$$

est mimée par $\sum_{p \leqslant n} Z_p$, et l'on obtient non seulement le théorème de Hardy-Ramanujan mais aussi le théorème d'Erdős-Kac, par une simple utilisation du théorème central limite des probabilités.

Le modèle d'Erdős-Kubilius

La seconde direction[5] dans laquelle ce théorème a été généralisé est issue d'une perspective fonctionnelle. Ce n'est plus le nombre total de facteurs premiers qui est étudié, mais la fonction $t \mapsto \omega(n,t) = \sum_{p \leqslant t} \varepsilon_p(n)$ qui décrit totalement la suite des facteurs premiers de n. On se demande alors dans quelle mesure cette quantité peut être approchée, *uniformément en tant que fonction de* $t \leqslant n$, par la fonction correspondante construite sur les variables abstraites Z_p mimant les ε_p.

Une forme possible du résultat — ces approximations fonctionnelles ont été étudiées de beaucoup de manières différentes — est conforme à ce que prévoit la loi du logarithme itéré des probabilités : on a, pour tout $\varepsilon > 0$ et toute fonction $\xi(n) \to \infty$,

$$\sup_{\xi(n) \leqslant t \leqslant n} \frac{|\omega(n,t) - \log_2 t|}{\sqrt{2 \log_2 t \log_4 t}} \leqslant 1 + \varepsilon \qquad \text{pp}, \tag{1}$$

mais aussi, si la croissance de $\xi(n)$ est assez lente,

$$\sup_{\xi(n) \leqslant t \leqslant n} \frac{|\omega(n,t) - \log_2 t|}{\sqrt{2 \log_2 t \log_4 t}} \geqslant 1 - \varepsilon \qquad \text{pp}. \tag{2}$$

Cela signifie que l'on a déterminé les fluctuations de cette fonction par rapport à sa moyenne $\log_2 t$ non seulement avec l'ordre de grandeur exact mais aussi avec la constante multiplicative exacte. Il s'agit ici non plus de la convergence en loi d'une suite de variables aléatoires, mais de la convergence d'un processus pour la norme de la convergence uniforme des fonctions.

Vu sous cette forme, ce théorème n'est peut-être pas très suggestif, cependant on peut lui donner un aspect beaucoup plus spectaculaire. Décomposons le nombre entier générique n en produit de puissances de nombres premiers, soit

$$n = p_1^{\alpha_1} \cdots p_k^{\alpha_k},$$

où les p_j sont rangés dans l'ordre croissant. Comme nous disposons d'estimations uniformes en t pour $\omega(n,t)$, nous pouvons choisir t égal à l'un des p_j — il n'y a, en effet, pas d'objection de principe à prendre t dépendant de n puisque, précisément, l'approximation est uniforme en t. Choisissons donc $t = p_j$, le j-ème facteur premier. Que vaut $\omega(n, p_j)$? Combien y a-t-il de facteurs premiers jusqu'au j-ème ? Il y en a j. Donc $\omega(n, p_j) = j$. C'est assez surprenant, mais on obtient ainsi une approximation du j-ème facteur premier de n en fonction de j seul, toujours presque partout. Autrement dit,

[5] Dont Erdős est également à l'initiative : voir par exemple [7].

on trouve que le logarithme itéré du j-ème facteur premier de n peut s'écrire sous la forme

$$\log_2 p_j(n) = j + \vartheta_j(n)\sqrt{2j\log_2 j}, \tag{3}$$

avec un $\vartheta_j(n)$ tel que $|\vartheta_j(n)| \leqslant 1 + o(1)$ pp, et qui effectivement s'approche *normalement* de 1 ou de -1 pour au moins une valeur de j.

Pour mettre les choses sous une forme encore plus expressive, quoiqu'un peu moins précise, on peut dire que le j-ème facteur premier ressemble — mais attention au sens que l'on donne ici au mot « ressembler » — à $\exp\exp j$. Autrement dit, le j-ème facteur premier d'un entier normal n a une approximation qui ne dépend que de l'indice j et pas de l'entier n. La dépendance en n n'apparaît finalement que sous une forme débonnaire : un entier normal a d'autant plus de facteurs premiers qu'il est grand, le nombre total de facteurs premiers est $\approx \log_2 n$.

Bien sûr, le terme d'erreur dans l'approximation $p_j(n) \approx \exp(\mathrm{e}^j)$ réside dans le second exposant, donc la qualité de l'approximation est très sensible à l'erreur ; on ne pourra pas en déduire des renseignements trop précis. Mais, tout de même, cela servira de modèle pour la structure normale d'un nombre entier.

Ce modèle probabiliste des entiers normaux, où le j-ème facteur ressemble à $\exp\exp j$, nous l'appelons modèle d'Erdős-Kubilius parce que ce point de vue fonctionnel, dont Erdős est à l'initiative [7], a été développé depuis la fin des années 50 par Kubilius et son école de Vilnius — [21, 22].

On peut montrer que ce modèle permet également de mimer le mouvement brownien à partir de la répartition des facteurs premiers de n. Par quelle mécanique ? Posons

$$\psi_N(n,t) := \frac{\omega\big(n, \exp\{(\log N)^t\}\big) - t\log_2 N}{\sqrt{\log_2 N}}.$$

Considérons l'ensemble de Skorokhod $\mathbf{D}[0,1]$ (bien connu des probabilistes), c'est-à-dire l'ensemble des fonctions $f : [0,1] \to \mathbb{C}$, continues à droite et admettant en tout point une limite à gauche — ce que l'on peut voir comme une normalisation des fonctions réglées définies sur [0,1]. Munissons cet ensemble d'une topologie adéquate (que nous ne préciserons pas plus avant ici) fournissant donc un ensemble $\mathcal{D}$ qui est la tribu des boréliens de $\mathbf{D}[0,1]$.[6] Définissons une mesure sur l'ensemble de ces boréliens de la manière suivante :

$$\mu_N(B) = \frac{1}{N}\,|\{n \leqslant N : t \mapsto \psi_N(n,t) \in B\}| \qquad (B \in \mathcal{D}).$$

[6] Pour une définition précise de la topologie de Skorokhod, voir par exemple Billingsley [2].

On peut alors montrer, comme l'a fait Billingsley dans les années 70, que μ_N converge faiblement vers la mesure de Wiener, autrement dit que μ_N mime le mouvement brownien lorsque N tend vers l'infini.

Ce type de résultat est en un certain sens plus précis que la loi du logarithme itéré précédemment décrite,[7] et fournit un modèle des nombres normaux en accord avec le modèle d'Erdős-Kubilius. Nous verrons que, quoiqu'un peu trop simple, cette représentation permet cependant de démontrer certains résultats sur la structure des entiers normaux.

La première conséquence à tirer de ce modèle d'Erdős-Kubilius, portant sur la structure globale de l'ensemble des facteurs premiers, c'est une description des diviseurs eux-mêmes. Une telle application est naturelle puisque les diviseurs sont obtenus par multiplication des facteurs premiers. Il résulte du calcul que le j-ème diviseur ressemble — avec, comme précédemment, une acception suffisamment vague du mot « ressembler » — à $\exp(j^{1/\log 2})$. Ainsi la suite des logarithmes des diviseurs d'un entier normal croît polynomialement en l'indice.

On retrouve ici, en particulier, un résultat de Hardy et Ramanujan selon lequel le nombre total $\tau(n)$ de diviseurs de n est normalement comparable à $(\log n)^{\log 2}$. Cela permet d'établir rigoureusement l'assertion énoncée plus haut selon laquelle la propriété « n possède moins de $\log n$ diviseurs » est normale : cela découle effectivement de l'inégalité $\log 2 < 1$; « n a plus de $\sqrt{\log n}$ diviseurs » est aussi une propriété normale.

Un objet fractal

On peut aller plus loin dans le sens du modèle d'Erdős-Kubilius, et décrire des phénomènes impliquant les rapports de diviseurs consécutifs. Toutefois, seuls des résultats en moyenne peuvent être obtenus de cette manière. Citons un résultat de 1993, obtenu en collaboration avec Michel Mendès France [25] : si les diviseurs de n, disons $\{d_j\}_{j=1}^{\tau(n)}$, sont rangés dans l'ordre croissant, on a

$$\sum_{1\leqslant j<\tau(n)} \left(\frac{\log d_{j+1}/d_j}{\log n}\right)^{\alpha} = \tau(n)^{\max(0,1-\alpha/\log 2)+o(1)} \qquad \text{pp.} \tag{4}$$

Cette relation est assez curieuse : tant que α dépasse $\log 2$, la somme ne « décolle » pas, et, lorsque α passe en dessous de l'exposant critique $\log 2$, la somme devient brutalement de l'ordre d'une puissance positive fixe de son nombre de termes, révélant ainsi que les distances logarithmiques entre les diviseurs consécutifs sont en moyenne relativement grandes. Si l'on avait

[7] Il permet d'améliorer (1) et (2) pour les grandes valeurs de t, mais fournit un résultat inférieur pour les petites.

une répartition uniforme des $\log(d_{j+1}/d_j)$, le membre de gauche de (4) serait proche de

$$\sum_{1\leqslant j<\tau(n)} \tau(n)^{-\alpha} \approx \tau(n)^{1-\alpha}.$$

Le phénomène observé met donc en évidence une répartition très disparate des distances entre diviseurs consécutifs. Le résultat quantitatif (4) s'apparente à un calcul de dimension de Hausdorff, et l'on peut dire — c'est expliqué beaucoup plus en détail dans notre article avec Michel — que les diviseurs d'un nombre normal ont en réalité une structure d'objet fractal de dimension $\log 2$. Ce qui a fait dire à Michel que les diviseurs d'un entier n bouillent normalement à 1,44 degré — l'inverse de $\log 2$.

Comment aurait-on pu prévoir l'existence d'une telle structure fractale ? Utilisons le modèle d'Erdős-Kubilius ! Considérons les quantités $(\log d)/\log n$, où d parcourt l'ensemble des diviseurs de n. Comment peut-on les écrire ? On a

$$\frac{\log d}{\log n} = \sum_{j=1}^{\omega(n)} \alpha_j \frac{\log p_j}{\log n}, \tag{5}$$

avec des coefficients α_j valant 0 ou 1.[8] Maintenant, remplaçons $\log p_j$ par son approximation. Nous obtenons

$$\frac{\log d}{\log n} \approx \sum_{j=1}^{\omega(n)} \alpha_j \mathrm{e}^{j-\log_2 n}.$$

Mais $\log_2 n$, toujours d'après le modèle d'Erdős-Kubilius, peut être identifié à $\omega(n)$. Réécrivons donc la somme en choisissant $k := j - \omega(n)$ comme variable ; nous avons maintenant des exposants négatifs ou nuls, et, comme $\omega(n)$ tend vers l'infini, nous pouvons étendre la somme jusqu'à l'infini sans altérer la nature de l'approximation : nous obtenons une série

$$\sum_{k=0}^{\infty} \alpha_k \mathrm{e}^{-k}.$$

Qu'avons-nous trouvé ? Un ensemble de Cantor, de paramètre non pas 3, mais e (compris entre 2 et 3), dont la dimension est égale à $\log 2$ — puisque la dimension d'un ensemble de Cantor de paramètre ϑ vaut $\log 2/\log \vartheta$.

On retrouve donc ainsi, très simplement à partir du modèle d'Erdős-Kubilius, cette structure fractale de l'ensemble des diviseurs d'un entier. Il est

[8] Pour simplifier l'exposition, nous supposons ici que n est sans facteur carré.

remarquable que, bien que ce modèle soit assez grossier (puisque le terme d'erreur est dans le dernier exposant), il soit cependant suffisamment précis en moyenne pour prédire la formule asymptotique (4).

Les limites du modèle d'Erdős–Kubilius

Certains des renseignements relativement fins dont on dispose sur la structure normale des diviseurs d'un nombre ne sont pas déduits du modèle d'Erdős-Kubilius. Plus grave : une notable proportion de ces informations sont en fait en complète contradiction avec lui. Voyons cela. Considérons les nombres de la forme

$$\sum_{1\leqslant j\leqslant\omega(n)} \alpha_j \mathrm{e}^j \qquad (\alpha_j = 0 \text{ ou } 1).$$

Comme $\mathrm{e} > 2$, ces sommes sont « dominées » par leur plus grand terme et un calcul simple montre que les différences de valeurs consécutives sont minorées par e. Autrement dit, si l'on en croit le modèle d'Erdős-Kubilius simple, le rapport de deux diviseurs consécutifs ne devrait jamais s'approcher de 1. Nous verrons cependant que non seulement il s'approche de 1 mais il s'en approche beaucoup, avec d'ailleurs un résultat précisément quantifiable — cf. formule (7) *infra*. Cela signifie que ce sont finalement les *termes d'erreur* du modèle d'Erdős-Kubilius qui permettent l'approximation : la structure fine de la suite des diviseurs est gouvernée par les termes d'erreur, alors que, comme l'atteste par exemple le résultat (4), la structure globale et la structure en moyenne sont essentiellement tributaires des termes principaux.

Dans le même ordre d'idées, on peut montrer[9] que, posant

$$\Delta(n) := \sup_{u\in\mathbb{R}} \sum_{\substack{d\mid n\\ \mathrm{e}^u < d \leqslant \mathrm{e}^{u+1}}} 1,$$

on a

$$(\log_2 n)^{c+o(1)} < \Delta(n) < \xi(n)\log_2 n \qquad \text{pp}$$

dès que $\xi(n)\to\infty$, avec $c = \log 2/\log\{\log 3/(\log 3 - 1)\} \approx 0,28754$. Il s'agit essentiellement ici d'évaluer la concentration des nombres

$$\sum_{1\leqslant j\leqslant\omega(n)} \alpha_j \log p_j(n)$$

[9] cf. Maier–Tenenbaum [23, 24].

avec $\alpha_j = 0$ ou 1.[10] Les $\log p_j(n)$ valent en moyenne e^j, mais les fluctuations stochastiques sont assez grandes pour que $\Delta(n)$ tende normalement vers l'infini. La majoration, que l'on peut donc aussi exprimer sous la forme $\Delta(n) < \xi(n)\omega(n)$ pp, est également surprenante : l'inégalité générale de Kolmogorov–Rogozin ne fournit qu'une borne exponentiellement plus grande, soit $\ll 2^{\omega(n)}/\sqrt{\omega(n)}$. Le modèle d'Erdős–Kubilius (i.e. $\log p_j(n) \approx \mathrm{e}^j$) prévoit que $\Delta(n)$ est borné pp.

Ce même modèle laisse également augurer que les diviseurs d'un entier normal sont rangés dans l'ordre lexicographique.[11] Pourtant, il est possible d'évaluer asymptotiquement le nombre $L(x)$ des entiers lexicographiques — définis comme les entiers pour lesquels tous les diviseurs sont rangés dans l'ordre lexicographique — plus petits que x, soit

$$L(x) = |\{\ell \leqslant x : \ell \text{ lexicographique}\}|.$$

On peut établir (voir le travail en commun avec André Stef [27]) que ce nombre est asymptotiquement équivalent à $Cx/(\log x)^\delta$, pour une certaine constante C — dont on n'a d'ailleurs aucune évaluation numérique, on sait simplement qu'elle est positive — et où δ est un exposant approximativement égal à $0,228$, et précisément défini comme la solution de l'équation

$$\int_0^{1/2} \frac{dv}{v^\delta(1-v)} = 1.$$

La valeur de l'exposant laisse supposer, à juste titre, que la démonstration n'est pas complètement évidente. En tout état de cause, les entiers lexicographiques sont relativement rares, ce qui est en contradiction manifeste avec le modèle.

Le modèle d'Erdős–Kubilius doit donc être vu comme une tendance générale, sur laquelle se greffent des fluctuations aléatoires,[12] et qui, par conséquent, ne doit pas être exploité sans précaution particulière.

Dans d'autres types de problèmes, le modèle est en défaut, mais moins gravement. Notant toujours $\{p_j(n)\}_{j=1}^{\omega(n)}$ la suite croissante des facteurs premiers distincts d'un entier n, écrivons par exemple,

$$p_j(n)^{\gamma_j(n)} = p_1(n)p_2(n)\cdots p_{j-1}(n) \qquad (1 \leqslant j \leqslant \omega(n)),$$

[10] En réalité, on a bien sûr $\alpha_j \in \{1, \dots, v_j(n)\}$ où $v_j(n)$ est l'exposant de $p_j(n)$ dans la décomposition canonique de n. Cependant, comme la densité des entiers n divisibles par le carré d'un nombre premier $> y$ est $O(1/y)$, on peut supposer que $v_j(n) = 1$ dès que $j \to \infty$.

[11] L'ordre lexicographique sur les diviseurs a été défini page 4.

[12] Ces fluctuations sont en partie décrites par la formule (6) *infra.*

ce qui constitue une définition des $\gamma_j(n)$. Si l'ordre lexicographique prévalait, cela signifierait que les $\gamma_j(n)$ sont toujours plus petits que 1. Or Erdős a montré en 1969 (voir [8]) que

$$\max_j \gamma_j(n) \sim (\log_3 n)/\log_4 n \qquad \text{pp},$$

autrement dit $\max_j \gamma_j(n)$ tend normalement vers l'infini — donc le modèle est faux — mais cette quantité tend très lentement vers l'infini — donc le modèle n'est pas aberrant, sa « philosophie » demeure, à bien des égards, pertinente.

Voyons maintenant comment on peut affiner la description.

Un modèle plus précis

L'approximation essentielle (3), relative à $\log_2 p_j(n)$, du modèle d'Erdős Kubilius est issue de la loi du logarithme itéré. Cette relation-là suggère que les $\log_2 p_j$ se comportent statistiquement comme des sommes de variables indépendantes relevant du théorème central limite. Que pourraient être les variables élémentaires associées ? Les $\log_2 p_{\ell+1} - \log_2 p_\ell$ constituent une option naturelle. On peut en effet démontrer, comme l'a fait Galambos [14], que, pour la plupart des indices ℓ,

$$\log_2 p_{\ell+1}(n) - \log_2 p_\ell(n)$$

se comporte normalement — c'est-à-dire pour un entier normal — comme une variable aléatoire X qui suit une loi exponentielle d'espérance 1,[13] autrement dit

$$\mathbb{P}(X \leqslant z) = 1 - \mathrm{e}^{-z} \qquad (z \geqslant 0).$$

Les rapports $(\log p_{\ell+1})/\log p_\ell$, dont les produits partiels forment les $\log p_j$, étant modélisés par des variables de même loi que $\exp X$, on peut finalement modéliser un diviseur générique d d'un entier n normal par la relation

$$\log d \approx \sum_{j=1}^{\omega(n)} \alpha_j X_1 \cdots X_j, \tag{6}$$

où les α_j sont des variables de Bernoulli indépendantes sur $\{0,1\}$, et où les X_j sont des variables mutuellement indépendantes et indépendantes des α_j, plus grandes que 1 et telles que $\mathbb{P}(1 \leqslant X_j \leqslant t) = 1 - 1/t$. Voilà un modèle probabiliste plus précis pour la structure des diviseurs de n.[14]

[13] Si la loi est indépendante de j, il faut bien que l'espérance soit 1 puisque la somme est, pour tout j, d'espérance j.

[14] Ce modèle, toutefois, ne tient pas compte de la répartition spécifique des très grands facteurs premiers. Voir également Billingsley [4], et, pour des études plus récentes, Donnelly et Grimmett [6], Arratia [1], Tenenbaum [32].

> *M. Mendès France :* Une petite remarque. Dans (5) et ici, tu prends des *quadratfrei* ?
>
> *G. Tenenbaum :* On suppose en effet les entiers sans facteur carré, pour simplifier l'exposé. Ça n'induit pas de difficulté. S'il y a des facteurs carrés ou des puissances plus grandes, les α_j ne sont plus à valeurs 0 ou 1, mais relèvent d'une répartition un peu plus compliquée. Cependant, les valeurs prises sont, avec une forte probabilité, relativement petites, et cela ne modifie pas le modèle de manière sensible.

Ce modèle assez sophistiqué de la structure des diviseurs d'un nombre pourrait être développé plus avant dans la théorie des probabilités, mais, pour l'instant, il semble difficile à exploiter directement pour démontrer, voire même pour conjecturer, des résultats sur les nombres normaux. En effet, bien que les variables en cause ne soient pas particulièrement difficiles à appréhender, une telle représentation ne conduit pas, en pratique, à une réelle simplification du problème. Les rapports de diviseurs, par exemple, sont modélisés par des différences de sommes de produits — donc des sommes pondérées à coefficients 0, ± 1, de produits de variables aléatoires indépendantes. Les descriptions probabilistes disponibles pour de telles quantités ne sont pas satisfaisantes.

Quoique complexe et délicat à utiliser, le modèle est cependant bien défini et possède une structure limpide : tous les espoirs sont permis.

Exploitation heuristique du nouveau modèle

S'il ne fournit pas encore de technique effective pour résoudre des problèmes liés à la structure des nombres normaux, le modèle modifié constitue déjà un précieux guide conjectural : l'hypothèse que la somme de variables aléatoires (6) se comporte de manière statistique,[15] et qu'elle se conforme finalement à une certaine équirépartition est en effet riche de conséquences.

Revenons sur la conjecture d'Erdős mentionnée précédemment et qui concerne les petits rapports de deux diviseurs consécutifs. Un raisonnement heuristique relativement simple permet d'en formuler un énoncé précis. Considérons les $\log(d'/d)$, qui sont des nombres réels compris entre $-\log n$ et $\log n$. En supposant toujours le nombre n sans facteur carré, combien y a-t-il de telles quantités ? Il faut garder à l'esprit qu'il n'y a pas unicité de

[15] Ainsi qu'il faut s'y attendre lorsque l'on ajoute des variables aléatoires présentant un certain degré d'indépendance. Ici, évidemment, les produits ne sont pas indépendants, mais le fait que des produits dont les nombres de termes sont très différents possèdent beaucoup de facteurs indépendants rend tout de même plausible un effet de moyenne stochastique.

représentation — chaque d'/d peut être obtenu de beaucoup de façons différentes. Cependant, un rapport d'/d est toujours représenté de manière unique sous la forme d'un produit

$$\prod_{j=1}^{\omega(n)} p_j^{\beta_j},$$

où, cette fois, les β_j valent 0, +1 ou −1. Pour chaque facteur premier p_j, il y a donc trois choix possibles de β_j. Cela fournit $3^{\omega(n)}$ rapports d'/d, ou encore, comme $\omega(n)$ est proche de $\log_2 n$, environ $(\log n)^{\log 3}$ rapports distincts d'/d. Si l'on suppose que les logarithmes de ces $(\log n)^{\log 3}$ rapports sont équirépartis dans l'intervalle $[-\log n, \log n]$, on s'attend à ce que chaque sous-intervalle contienne un quota de rapports proportionnel à sa longueur, et en particulier, à ce que le plus rapport positif soit très proche de 0 — en fait que $\min \log(d'/d)$ soit à peu près de l'ordre de $1/(\log n)^c$, avec $c := \log 3 - 1 > 0$.

C'est la motivation de la conjecture d'Erdős, et c'est maintenant un théorème : on a bien

$$\min_{\substack{dd'|n \\ d<d'}} \log(d'/d) = 1/(\log n)^{\log 3 - 1 + o(1)} \qquad \text{pp.} \tag{7}$$

Ce résultat a été démontré en collaboration avec Maier,[16] en 1983, [23] sans invoquer directement un modèle probabiliste, mais en l'utilisant comme support heuristique essentiel et en faisant appel à des techniques, sur lesquelles nous reviendrons plus loin, qui font partie de l'arsenal usuel des probabilistes.

Pour donner une idée du type de renseignements que l'on peut obtenir dans cette direction, mentionnons un résultat très récent concernant la structure fine des petits rapports de diviseurs consécutifs. L'énoncé lui-même atteste que la démonstration ne peut pas être trop simple.

On sait que le logarithme du rapport de deux diviseurs consécutifs est normalement au moins égal à $1/(\log n)^{\log 3 - 1}$ — en négligeant, pour simplifier, l'erreur $o(1)$ sur l'exposant. Il est alors naturel de se demander combien de rapports consécutifs sont plus petits, logarithmiquement, que $1/(\log n)^\alpha$ lorsque α est un paramètre vérifiant $0 \leqslant \alpha < \log 3 - 1$. On formalise la question en définissant

$$D(n, \alpha) := |\{d_j \ : \log(d_{j+1}/d_j) \leqslant 1/(\log n)^\alpha\}| \qquad (0 \leqslant \alpha < \log 3 - 1).$$

Cette fonction ne possède pas forcément un ordre normal, et il se pourrait fort bien qu'une telle quantité présente des fluctuations très violentes sur

[16] En fait, c'est uniquement la majoration de $E(n)$ contenue dans cette formule qui fait l'objet du travail cité. La minoration, techniquement beaucoup plus simple, avait été établie par Erdős et Hall en 1979 [13].

une suite de densité 1. Cependant, il s'avère que l'on peut normalement approcher $D(n,\alpha)$ par une puissance fixe (c'est-à-dire ne dépendant que de α) du nombre de diviseurs de n. Pour une fonction convenable

$$G\colon [0,\log 3-1[\to[0,2/3[,$$

on a

$$D(n,\alpha)=\tau(n)^{1-G(\alpha)+o(1)}\qquad(0<\alpha<\log 3-1)\qquad\text{pp.}$$

Juste pour détendre un peu l'atmosphère, explicitons la fonction $G(\alpha)$; elle est définie à partir d'une autre fonction, soit

$$F(u)=\begin{cases} u\log(2/u)-(1-u)\log(1-u)-1 & (1-1/\mathrm{e}\leqslant u<2/3),\\[2ex] u\log\left(\dfrac{2}{\mathrm{e}-1}\right) & (0\leqslant u<1-1/\mathrm{e}).\end{cases}$$

On peut vérifier que F est strictement croissante et qu'elle est en fait de classe $\mathcal{C}^1$ sur $[0,2/3[$. On définit alors G comme la fonction inverse de F.

On constate donc que $G([0,\log 3-1[)=[0,2/3[$. Ce $2/3$ est très surprenant : il signifie que si l'on prend α à peine inférieur à $\log 3-1$, il y a à peu près $\tau(n)^{1/3}$ rapports de diviseurs consécutifs d_{j+1}/d_j n'excédant pas $1+(\log n)^{-\alpha}$, c'est-à-dire pratiquement aussi petits qu'il est possible. Et dès que l'on franchit le seuil critique $\alpha=\log 3-1$, cet exposant $1/3$ devient $0-$, ou $-\infty$, comme l'on veut, puisqu'il n'y a plus aucun rapport de diviseurs consécutifs aussi petit. On a donc mis en évidence une « énorme » discontinuité.

On peut s'interroger sur l'origine de ce curieux phénomène. Il y a en fait une explication très simple.

Comment obtenir des rapports d_{j+1}/d_j petits ? Soit $t:=\mathrm{pgcd}(d_j,d_{j+1})$. Si le rapport d_{j+1}/d_j est voisin de 1, il existe des diviseurs proches et premiers entre eux, d, d', tels que

$$d_j=td,\quad d_{j+1}=td'. \tag{8}$$

Réciproquement, lorsque d et d' sont donnés, proches et premiers entre eux, il est vraisemblable que la plupart des $\tau(n/dd')$ valeurs de t possibles fournissent une solution. En effet, si d et d' sont très voisins, il est peu probable qu'un autre diviseur de n vienne s'intercaler entre td et td', ce qui signifie que le système (8) aura beaucoup de solutions en (t,j). En fait, sous l'hypothèse heuristique précédente, il en aura autant que de choix admissibles pour t, c'est-à-dire à peu près $\tau(n/dd')$. Ainsi, dès qu'il existe un seul couple (d,d') avec un rapport d'/d petit, il y a présomption d'existence de nombreux rapports d_{j+1}/d_j proches de 1. Combien exactement ? Nous avons vu

que d et d' sont premiers entre eux. Plus le nombre de choix possibles pour le couple (d, d') est grand, plus la taille attendue de $\min(d'/d)$ est petite. Or, le nombre maximal de couples (d, d') premiers entre eux est obtenu lorsque d et d' ont chacun approximativement un tiers du nombre total de facteurs premiers : cela résulte d'un calcul facile de coefficients binomiaux. Il reste donc (au moins) $\omega(n)/3$ facteurs premiers pour constituer les diviseurs t. En résumé, le nombre maximal de rapports d'/d (parmi lesquels il est raisonnable de trouver le plus petit de tous les rapports de ce type) est obtenu lorsque $\omega(dd') = \frac{2}{3}\omega(n)$, et il reste approximativement $2^{\omega(n)/3} \approx \tau(n)^{1/3}$ choix possibles pour t — d'où l'explication de la formule $G(\log 3 - 1 - 0) = \frac{2}{3}$ alors que $G(\log 3 - 1 + 0) = +\infty$.

Un point de vue « extérieur » sur la normalité : les suites de Behrend

Un autre type de propriété attendue pour un entier normal est que l'ensemble de ses diviseurs contienne un élément de chaque suite suffisamment dense et suffisamment aléatoire, en un sens à définir. C'est une notion qui a été considérée de manière implicite par Erdős depuis longtemps,[17] et Hall [16] en a plus récemment donné une définition formelle. *On dit qu'une suite d'entiers $\mathcal{A}$ est une* suite de Behrend *si tout entier normal possède un diviseur dans $\mathcal{A}$.* En d'autres termes, $\mathcal{A}$ est une suite de Behrend si la suite des multiples de $\mathcal{A}$,

$$\mathcal{M}(\mathcal{A}) := \{ma : m \geqslant 1,\, a \in \mathcal{A}\},$$

est de densité 1.[18] Les nombres pairs ne constituent pas une suite de Behrend, parce qu'un nombre normal sur deux est impair. Les nombres impairs ou les nombres premiers forment bien sûr des suites de Behrend.

On touche là des questions qui ont intrigué Erdős pendant de nombreuses années : que faut-il imposer à une suite pour qu'elle soit de Behrend ? Comment reconnaître une suite de Behrend ?

Voici un problème qui s'apparente à une recherche de suite de Behrend.

Nous savons qu'un nombre normal n a $\tau(n) = (\log n)^{\log 2 + o(1)}$ diviseurs. Considérons les nombres $\log d$, lorsque d parcourt les diviseurs de n ; ce sont des nombres réels et un seul est rationnel, c'est $\log 1 = 0$. Il n'y a pas de

[17] L'idée est sous-jacente dans les travaux d'Erdős depuis la fin des années trente. Voir, par exemple, [9] pour un énoncé précis du problème.

[18] Pour des exposés modernes de la théorie des ensembles de multiples, et de nombreux renseignements sur les suites de Behrend, voir le récent livre de Hall [18] et, parmi d'autres, l'article de synthèse [31].

raison structurelle pour supposer que ces quantités $\log d$ sont réparties modulo 1 de manière particulière. Un raisonnement standard reposant sur une hypothèse d'équirépartition conduit donc à conjecturer que, définissant la « norme modulo un » $u \mapsto \|u\|$ comme la fonction distance à l'ensemble des entiers, on a

$$\min_{d|n,\, d>1} \|\log d\| = 1/\tau(n)^{1+o(1)} \qquad \text{pp}, \tag{9}$$

c'est-à-dire normalement. Cela étant, l'observation des nombres $\log d$ fait tout de même apparaître cette tendance lourde, décrite plus haut, à une répartition globale de type fractal ; or, même si la structure fractale est liée à la taille des nombres, et non à leur reste modulo un, il pourrait se produire des interférences entre les deux tendances. Il se trouve que, dans le cas de la fonction $\log d$, ces interférences n'ont pas d'effet notable. Cependant, lorsque l'on considère plus généralement la fonction $(\log d)^\alpha$, un raisonnement heuristique suggère que l'exposant de $\tau(n)$ dans la formule conjecturale analogue à (9) n'est pas constamment égal à 1. On peut établir que l'exposant est le minimum — on retrouve justement ici le côté fractal — de 1 et de $\alpha/(1-\log 2)$: on a

$$\min_{d|n,\, d>1} \|(\log d)^\alpha\| = 1/\tau(n)^{\min(1,\alpha/(1-\log 2))+o(1)} \qquad \text{pp}, \tag{10}$$

lorsque le nombre positif α vérifie la condition (trivialement nécessaire)

$$\big\{(\log d)^\alpha : d > 1\big\} \cap \mathbb{N} = \varnothing.$$

Ainsi, tant que α excède $1 - \log 2$, le raisonnement heuristique fondé sur l'équirépartition fournit la valeur exacte, mais lorsque α est inférieur au seuil critique, il est nécessaire de tenir compte du modèle fractal pour déterminer le bon exposant. Il est à noter que la preuve de (10) relève effectivement des deux points de vue : la minoration repose sur un lemme apparaissant dans l'article cité plus haut en collaboration avec Michel Mendès France [25],[19] et la majoration est issue d'une très légère altération de l'argument principal d'un travail relatif aux suites de Behrend, [30].[20]

Il n'est pas absolument évident, de prime abord, de lier ce problème à celui des suites de Behrend. Voici une explication succincte. Considérons pour simplifier le cas $\alpha = 1$. On a $\|\log d\| = \min\big(\{\log d\}, 1 - \{\log d\}\big)$ où $\{u\}$ désigne la partie fractionnaire du réel u. En nous bornant, par exemple, à l'étude des variations de la fonction $\{\log d\}$, il s'agit donc de montrer que, pour ε_n assez

[19] Voir le lemme 6.3 de ce travail.

[20] Le cas α=1 a été établi par Erdős et Hall dans [12].

petit,[21] l'un au moins des intervalles $[k, k+\varepsilon_n[$ $(k \in \mathbb{N}^*)$ contient normalement une valeur de $\log d$ avec $d|n$, ce qui signifie que n possède un diviseur dans

$$\mathcal{A}_n := \cup_{k\in\mathbb{N}^*}]\mathrm{e}^k, \mathrm{e}^{k+\varepsilon_n}].$$

Or, sous l'hypothèse d'une équirépartition, et puisque, d'après le modèle simple, un entier normal n possède environ $k^{\log 2+o(1)}$ diviseurs d tels que $\log d \leqslant k+1$, il est vraisemblable que, pour $\varepsilon > 0$ arbitrairement petit, l'un au moins des intervalles $]k, k+1/k^{\log 2-\varepsilon}]$ contienne une valeur de $\log d$. Autrement dit, la suite

$$\mathcal{A} = \cup_k[\mathrm{e}^k, \mathrm{e}^k(1+1/k^{\log 2-\varepsilon})] \cap \mathbb{N} \tag{11}$$

doit être une suite de Behrend : on peut effectivement établir cela et en déduire (10) dans le cas $\alpha = 1$.[22]

Voilà un exemple tout à fait non trivial de suite de Behrend. L'exposant $\log 2$ est critique, c'est-à-dire que, lorsqu'on le remplace par un nombre strictement plus grand, on obtient une suite qui n'est pas de Behrend, alors que, bien entendu, la suite demeure de Behrend pour tout exposant plus petit.

> Pour les lecteurs les plus curieux, nous développons ici l'argument heuristique en faveur de (10). Il est fondé à la fois sur le modèle simple d'Erdős–Kubilius et sur l'équirépartition les valeurs $(\log d)^\alpha$ pour un certain sous-ensemble de valeurs de d. Considérons $\alpha < 1 - \log 2$ et définissons la discrépance
>
> $$\delta(n) := \sup_{0\leqslant u<v\leqslant 1/2} \Bigg| \sum_{\substack{d|n \\ u<\|(\log d)^\alpha\|\leqslant v}} 1 - (v-u)\tau(n) \Bigg|.$$
>
> Il est alors naturel de conjecturer que l'inégalité
>
> $$\min_{d|n,\, d>1} \|(\log d)^\alpha\| \leqslant 2\delta(n)/\tau(n)$$
>
> est optimale pp à un facteur $\tau(n)^{o(1)}$ près.[23] Cependant, si l'on choisit

[21] Ici, « assez petit » signifie : au plus de l'ordre de $1/\tau(n)^{1-\varepsilon}$ avec $\varepsilon > 0$ arbitraire.

[22] C'est exactement le résultat fourni par le théorème principal de [30] lorsque l'on y spécialise les paramètres de façon que la suite « par blocs » générale de l'hypothèse soit la suite $\mathcal{A}$ de (11). Au prix de quelques modifications techniques, d'ailleurs évidentes, la preuve fournit également que, si l'on note $\mathcal{A}_x := \cup_k[\mathrm{e}^k, \mathrm{e}^k(1+1/(\log x)^{\log 2-\varepsilon})]$, alors $\mathcal{M}(A_x)$ contient tous les entiers $n \leqslant x$ sauf au plus $o(x)$ — ce qui établit (10) dans le cas $\alpha = 1$. Le cas général résulte de considérations similaires.

[23] Cette inégalité est obtenue en choisissant $u = 0$, $v = 2\delta(n)/\tau(n)$: on a alors

$$\sum_{\substack{d|n,\, d>1 \\ \|(\log d)^\alpha\|\leqslant 2\delta(n)/\tau(n)}} 1 \geqslant \delta(n) > 0.$$

un paramètre $\varrho \in]0,1[$ et si l'on écrit $n = abp$ où tous les facteurs premiers de a sont $\leqslant \exp\{(\log n)^\varrho\}$ et p est le plus grand facteur premier de n, le modèle d'Erdős–Kubilius permet de montrer que

$$\log a = (\log n)^{\varrho+o(1)}, \qquad \log p = (\log n)^{1+o(1)} \qquad \text{pp.}$$

Cela implique, pp, que les $\tau(a)$ diviseurs d de n de la forme $d = a_1 p$ avec $a_1 | a$ vérifient

$$(\log d)^\alpha = (\log p)^\alpha + O\big((\log n)^{\varrho+\alpha-1+o(1)}\big).$$

Si $\varrho < 1-\alpha$, les nombres $\|(\log d)^\alpha\|$ occupent donc un sous-ensemble de $\big[0, \frac{1}{2}\big]$ de mesure totale

$$\lambda \leqslant (\log n)^{\varrho+\alpha-1+o(1)}.$$

On en déduit que

$$\delta(n) \geqslant \tau(a) - \lambda\tau(n) > \tfrac{1}{2}\tau(a) = \tau(n)^{\varrho+o(1)}$$

dès que $\varrho + \alpha - 1 + \log 2 < \varrho \log 2$, c'est-à-dire $\varrho < 1 - \alpha/(1-\log 2)$. Cela fournit bien l'optimalité de la majoration heuristique

$$\begin{aligned} \min_{d|n,\, d>1} \|(\log d)^\alpha\| \leqslant \delta(n)/\tau(n) &= \tau(n)^{\varrho-1+o(1)} \\ &= \tau(n)^{-\alpha/(1-\log 2)+o(1)} \qquad \text{pp.} \end{aligned}$$

Transformées de Fourier de fonctions arithmétiques

En l'absence d'une exploitation directe du modèle probabiliste précis, les techniques disponibles pour appréhender la structure normale des entiers restent dans le cadre de la théorie des fonctions arithmétiques. L'une des méthodes les plus efficaces consiste à introduire la transformée de Fourier de la mesure de répartition des diviseurs. Conformément à ce que nous avons décrit jusqu'ici, il est plus pertinent de repérer les diviseurs par leurs logarithmes : nous considérons donc la transformée de Fourier–Stieltjes de la fonction croissante $z \mapsto \varphi_n(z) := \sum_{d|n,\, \log d \leqslant z} 1$, soit

$$\tau(n,\vartheta) := \sum_{d|n} \mathrm{e}^{i\vartheta \log d} = \sum_{d|n} d^{i\vartheta}.$$

Cette fonction possède la remarquable propriété de dépendre multiplicativement de n. Ainsi, alors que, pour chaque n, ses variations en ϑ décrivent complètement le problème étudié,[24] ses variations en n à ϑ fixé relèvent de la théorie assez avancée des fonctions multiplicatives à croissance modérée. Pour un entier n sans facteur carré, par exemple, le nombre $\tau(n,\vartheta)$ s'exprime simplement comme un produit, soit

$$\tau(n,\vartheta) = \prod_{p|n}(1+p^{i\vartheta}).$$

Une des approches utilisées consiste alors à estimer $\tau(n,\vartheta)$ en moyenne (souvent pondérée) sur n, en considérant momentanément ϑ comme un paramètre, pour en déduire ensuite, par transformée de Fourier inverse, des résultats sur la répartition des diviseurs.

Cela dit, cette fonction $\tau(n,\vartheta)$ demeure tout de même assez mystérieuse. Hall, par exemple, a démontré en 1975 [15] que

$$|\tau(n,\vartheta)| \leqslant \mathrm{e}^{\xi(n)\sqrt{\log_2 n}} \qquad \text{pp},$$

pour tout $\vartheta \neq 0$ fixé,[25] et toute fonction $\xi(n)$ tendant vers l'infini. Autrement dit, les valeurs individuelles sont normalement beaucoup beaucoup plus petites que l'ordre maximal. Mais que se passe-t-il lorsque l'on prend le supremum du module sur un intervalle en ϑ ne contenant pas l'origine, comme $[1,2]$? Est-il vrai que, pour presque tout n, la fonction $\sup_{1\leqslant\vartheta\leqslant 2}|\tau(n,\vartheta)|$ prend de grandes valeurs ? Cette question est encore ouverte. Un résultat récent de Hall [17] montre que

$$\inf_{a\in\mathbb{R}} \sup_{a\leqslant\vartheta\leqslant a+(\log n)^{\varepsilon}} |\tau(n,\vartheta)| \geqslant \tau(n)^{1/2+o(1)} \qquad \text{pp.}^{(26)}$$

Il est à noter, ici encore, que les résultats précédemment mentionnés d'équirépartition modulo un des $\log d$ sous-tendraient paradoxalement l'hypothèse d'un changement radical de comportement pour $\varepsilon = 0$, i.e. , pour $a > 0$ fixé,

$$\sup_{a\leqslant\vartheta\leqslant a+1} |\tau(n,\vartheta)| = \tau(n)^{o(1)} \qquad \text{pp.}^{(27)}$$

[24] C'est-à-dire la fonction $\varphi_n(z)$.

[25] $\tau(n,0)$, c'est $\tau(n)$, c'est-à-dire à peu près $(\log n)^{\log 2}$ pp.

[26] Depuis cet exposé, l'auteur a établi des résultats légèrement plus précis dans cette direction ; par exemple, pour tout $b \geqslant 1$, on a

$$\inf_{a\in\mathbb{R}} \sup_{a\leqslant\vartheta\leqslant a+b} |\tau(n,\vartheta)| \geqslant \big(1-1/\sqrt{b}\,\big)\sqrt{\tau(n)}$$

sur une suite de densité tendant vers 1 lorsque $b\to\infty$.

[27] Un tel comportement doit être considéré comme hautement improbable au vu du résultat cité dans la note précédente.

Cela pose un problème très intéressant, motivé non par la fonction $\tau(n,\vartheta)$ elle-même, mais par les applications à la répartition des diviseurs et à la structure multiplicative normale d'un nombre. Actuellement, aucune des techniques disponibles ne semble assez fine pour l'aborder.

Sommes d'exponentielles

On dit qu'une fonction arithmétique réelle f est équirépartie modulo un si l'on a pour tout $\alpha \in [0,1]$

$$\lim_{N\to\infty} \frac{1}{N} \sum_{\substack{d\leqslant N\\ \{f(d)\}\leqslant\alpha}} 1 = \alpha,$$

avec la notation $\{u\}$ pour la partie fractionnaire. Le critère classique de Weyl énonce qu'une condition nécessaire et suffisante d'équirépartition est que l'on ait, pour tout entier relatif non nul ν,

$$\sum_{d\leqslant N} \mathrm{e}^{2\pi i\nu f(d)} = o(N) \qquad (N\to\infty).$$

Ainsi, le problème de l'équirépartition équivaut en toute généralité à un problème d'estimation de sommes d'exponentielles.

On dit qu'une fonction arithmétique réelle f est équirépartie modulo un sur les diviseurs si l'on a, pour toute suite $\mathcal{A}$ de densité 1,

$$\lim_{\substack{N\to\infty\\ N\in\mathcal{A}}} \frac{1}{\tau(N)} \sum_{\substack{d\mid N\\ \{f(d)\}\leqslant\alpha}} 1 = \alpha.$$

Il existe un analogue du critère de Weyl pour l'équirépartition sur les diviseurs, établi par l'auteur [29] (voir aussi [31]), à savoir

$$\lim_{N\to\infty} \frac{1}{\sqrt{\log N}} \sum_{k\leqslant N} \left| \sum_{\substack{d\leqslant N\\ d\equiv 0 \,(\mathrm{mod}\, k)}} \frac{e^{2\pi i\nu f(d)}}{d4^{\Omega(d)}} \right| = 0 \qquad (\nu\in\mathbb{Z}^*), \tag{12}$$

où $\Omega(d)$ désigne le nombre total des facteurs premiers de d, comptés avec leurs ordres de multiplicité. Il s'avère donc que les problèmes d'équirépartition sur les diviseurs peuvent également être interprétés en termes de majorations de sommes d'exponentielles. La différence essentielle avec le cas classique est qu'il s'agit à présent de sommes pondérées par des coefficients de nature arithmétique.

Or, comme on l'a vu précédemment, établir qu'une fonction arithmétique est équirépartie modulo un sur les diviseurs d'un entier normal équivaut essentiellement à construire une suite de Behrend. De plus, une évaluation effective de la discrépance (i.e. l'écart à l'équirépartition) fournit des estimations quantitatives sur les nombres normaux. Nous voyons donc que les estimations de sommes d'exponentielles à coefficients arithmétiques sont un moyen d'étude des suites de Behrend, et par conséquent des entiers normaux.

À ce stade, une remarque méthodologique peut éclairer la situation. Considérons la suite $\{(\log d)^\alpha : d|n\}$, c'est-à-dire

$$\big\{(\log d_j)^\alpha\big\}_{j=1}^{\tau(n)}.$$

Le modèle simple prédit que cette suite « ressemble » à

$$\big\{j^{\alpha/\log 2}\big\}_{j=1}^{\tau(n)}.$$

L'existence de résultats comme (10) sur la répartition modulo un de ces quantités est donc en accord avec l'état actuel de la théorie de l'équirépartition modulo un des suites de nombres réels, qui possède des outils performants pour traiter les suites à croissance polynomiale. Cependant, notre problème est ici deux fois probabilisé : on considère en premier lieu une question relative aux entiers normaux — ce qui constitue un premier degré de probabilisation —, et l'on observe, dans un second temps, la répartition des diviseurs — d'où une seconde réduction probabiliste. Il est donc naturel d'espérer un champ d'investigation plus large que celui auquel on est astreint dans le cadre usuel de la théorie de l'équirépartition.

Il est effectivement possible d'appréhender dans ce nouveau cadre des fonctions à croissance beaucoup plus rapide que polynomiale. Par exemple, pour chaque nombre irrationnel ϑ, on peut considérer la répartition des nombres ϑd, dont la croissance, comparable à celle de $j \mapsto \vartheta \exp(j^{1/\log 2})$, est exponentielle. Ce problème pourrait *a priori* être de nature semblable à celui de l'équirépartition modulo un de $(3/2)^n$, sur lequel les spécialistes s'accordent à penser qu'aucune méthode actuelle ne fournit même un espoir d'approche. Cependant, la double probabilisation mise en évidence dans le remplacement du critère de Weyl par (12) permet de répondre *aussi* à des question de cette nature — bien que les techniques touchent ici leurs limites. Par exemple, il est établi dans [31] (corollaire 9), que, lorsque ϑ est irrationnel algébrique, on a Par exemple, la technique conduisant au corollaire 9 de [31] permet également d'établir que, lorsque ϑ est irrationnel algébrique, on a

$$1/\tau(n)^{1+o(1)} \leqslant \min_{d|n} \|\vartheta d\| \leqslant 1/\tau(n)^c \qquad \text{pp}$$

dès que $c < 1 - \log 3/\log 4$.[28] Ici, l'exposant c n'est pas optimal — on attendrait $1 + o(1)$. Le fait que les techniques employées, qui reposent en particulier sur la méthode très sophistiquée de Vinogradov pour majorer certaines sommes d'exponentielles, permettent tout de même de parvenir à un exposant positif traduit leur degré de pertinence.

Un autre exemple intéressant est constitué par le problème de la distance à l'entier le plus proche de d^α. On obtient alors, pour chaque α positif non entier,

$$\min_{d|n,\, d>1} \|d^\alpha\| \leqslant 1/\tau(n)^\delta \qquad \text{pp},$$

dès que $\delta < \log(\frac{12}{11})/\log 4$.[29] Ici encore, l'optimalité est loin, mais la garantie d'un exposant positif indique qu'en mesure logarithmique une proportion positive du chemin a été franchie : un tel résultat est en lui-même assez surprenant.

La voie des sommes d'exponentielles pondérées représente un angle d'attaque prometteur pour l'étude des entiers normaux. Elle repose sur la mise en œuvre de méthodes compliquées d'analyse, reposant sur des théorèmes très difficiles, mais ne fait pas un usage concret du modèle probabiliste de nombre normal.

Limitation théorique : un principe d'incertitude

Pour achever cette présentation, citons un curieux théorème négatif [28], qui montre qu'un nombre normal ne peut pas être décrit de manière trop précise. Considérons la répartition des logarithmes des diviseurs et définissons à cette fin la quantité

$$F_n(u) := \frac{1}{\tau(n)} \sum_{d|n,\, d\leqslant n^u} 1 \qquad (0 \leqslant u \leqslant 1).$$

Pour chaque n, F_n est une honnête fonction de répartition, qui croît de 0 à 1 lorsque u croît de 0 à 1. Or, on peut montrer que, *si μ est une mesure de probabilité, et $\mathcal{A}$ est une suite d'entiers telle que* $\mathrm{d}F_n$ *converge faiblement vers μ lorsque n tend vers l'infini en restant dans $\mathcal{A}$, alors la densité naturelle de $\mathcal{A}$ est nulle*. Dès que l'on sait, avec une certaine précision, comment les diviseurs sont répartis, on le sait sur un ensemble négligeable !

Finalement, un nombre normal, c'est comme un électron, à peine connaît-on quelque chose sur lui, il se transforme en nuage...

[28] La minoration résulte de la remarque qui suit l'énoncé du corollaire 9 de [31].
[29] Voir le théorème 11 de [31].

En guise de conclusion

J'ai tenté, dans cet exposé, de décrire certaines avancées sur la notion intuitive de nombre « au hasard ». Avant de nous quitter, je voudrais vous faire brièvement partager quelques réflexions sur les motivations subjectives qui peuvent attirer un mathématicien vers la théorie des nombres.

Le nombre entier exerce, en effet, sur les amateurs comme sur les professionnels, une formidable fascination. Peut-être parce qu'il est si profondément ancré en nous que nous en venons facilement — si naturellement — à le concevoir comme une part de nous. Du même fait, surgit un sentiment d'inquiétante étrangeté lorsque nous expérimentons son opacité.

Le nombre répond à un besoin fondamental de repérage, d'action sur le monde. Il est en ce sens une notion qu'on pourrait qualifier « d'équipement conceptuel de base », plus primordiale que primitive. Je compte mes moutons — ça, c'est pour Michel Mendès France —, mes ennemis, mes années parce que je veux préserver mon cheptel, m'imposer à mes adversaires, connaître mon destin.

Mais ce lieu privilégié de l'idéation, de la pensée en formation, qu'est l'arithmétique élémentaire n'est pas un havre de paix. Le nombre porte en lui l'idée de mesure, la mesure induit l'ordre, et l'ordre la discorde. On ne saurait impunément placer l'homme dans l'univers sans refléter, dans le même mouvement, nos propres contradictions entre l'interrogation sur les choses de la nature et le désir de comprendre la nature des choses : reconnaître la source et cependant l'altérer jusqu'à, si le cœur, la raison ou la passion m'en disent, la transformer entièrement — au sens propre la dé-naturer — voilà bien une tâche qui ne va pas de soi.

Pour l'homme de la rue comme pour le mathématicien, le rapport au nombre est empreint d'ambivalence. Nous sommes friands de sondages, de statistiques, de mesures en tous genres à partir desquelles nous nous déterminons tout en en déplorant les effets réducteurs, dont nous prenons parfois conscience avec une souffrance sincère.

Le monde des nombres est, par sa proximité même, le siège de conflits sauvages. Que d'angoisses ne s'y trouvent-elles pas actualisées ? Toute angoisse est angoisse de mort, mais la mort a bien des visages, et l'imagination sait décliner à l'envi ses représentations. La mort, c'est d'abord la non-vie, c'est-à-dire l'impossibilité d'agir, et nous voici devant le vertige de l'infini : « *Maman, les nombres, ça ne s'arrête jamais ?* », avons-nous tous un jour demandé, espérant secrètement peut-être une rassurante dénégation parentale. La mort, c'est aussi l'absence, le manque, le retrait de ce que j'ai et que l'on va me prendre — ce que les psychanalystes désignent du vocable peut-être exigu de castration. Et les nombres sont encore là pour remuer le couteau

dans la plaie. « *Que se passe-t-il si de cent on ôte deux cent cinquante ?* », se demandait à quatre ans l'enfant prodige Paul Erdős, avant de fondre en larmes, parce qu'il avait compris qu'il allait mourir.

Et parmi ces conflits engendrés par une pensée qui se réfléchit, qui se reflète sur elle-même, il y a celui des deux ordres, des deux structures issues des deux opérations dont nous nous servons pour conjuguer ces entiers qui, pour autant, ne se laissent pas subjuguer. Ajouter, accumuler, appliquer puis échafauder, construire ; multiplier, dupliquer, répliquer, reproduire, voire produire. Ces deux ordres naturels, si tant est que compter soit naturel, entretiennent d'étranges rapports de filiation et d'indépendance. S'y retrouver, c'est-à-dire *se* retrouver, dans un tel imbroglio, c'est en quelque sorte tutoyer l'irréductible énigme que chacun porte au plus profond de lui-même — interroger le « comment ça fonctionne » pour sonder le « comment je fonctionne ». Je suppose qu'à l'instar de toute quête d'absolu les mathématiques ne parlent au fond que de ça.

Questions

M. Balazard : Qu'est-ce qu'on sait sur les suites de Behrend, dans le sens d'une caractérisation ?

G. Tenenbaum : Dans la voie d'une caractérisation, on dispose d'un théorème assez satisfaisant lorsque la suite est constituée de blocs d'entiers consécutifs suffisamment longs. Une telle suite $\mathcal{A}$ s'écrit comme une réunion d'intervalles $\mathcal{A}_j = [T_j, H_jT_j]$ assez longs pour que les ensembles de multiples $\mathcal{M}(\mathcal{A}_j)$ correspondants soient représentatifs de la structure probabiliste des nombres de $\mathcal{A}_j$, et non de leur structure locale — on exclut l'éventualité d'intervalles trop courts, par exemple de longueur 1, qui pourraient contenir « trop » de nombres dont la structure multiplicative est aberrante. Une condition suffisante est, par exemple, $H_jT_j > T_j + T_j^\alpha$ avec $\alpha > 0$ fixé. On a alors ce curieux résultat[30] qui ressemble au théorème de Borel–Cantelli en probabilités, sauf que, dans le cas de Borel–Cantelli, le critère est relatif à la convergence d'une série de probabilités, tandis qu'ici on a les mêmes probabilités, mais élevées à un certaine puissance. Sous forme condensée, on peut dire que, selon que la série

$$\sum_j \{\mathrm{dens}\,\mathcal{M}(\mathcal{A}_j)\}^{\beta_j + o(1)}$$

[30] Voir [19], théorème 1 et [30], théorème 1.

converge ou diverge, où l'on peut expliciter simplement les β_j, la suite est de Behrend ou ne l'est pas.

Tel quel, ce n'est pas tout à fait vrai... En fait, c'est ce que j'appelle un « pseudo-critère » : si vous remplacez le $o(1)$ par ε, la divergence est une condition suffisante, alors que si vous le remplacez par $-\varepsilon$, elle devient une condition nécessaire. Il est très surprenant que les exposants critiques ne soient pas égaux à 1. Si je prends $H_j = 2$ pour tout $j \geqslant 1$, ce qui est un cas particulier très intéressant, l'exposant critique est le même pour tout les $\mathcal{A}_j$, et vaut

$$\beta = \frac{(1 - \log 2)\log 2}{\log 2 - 1 - \log_2 2} \approx 3,56509.$$

Enfin, on peut retenir que l'on dispose d'un pseudo-critère simple dans le cas d'une suite composée d'intervalles suffisamment longs pour se comporter de manière statistique. Pour être tout à fait honnête, il faut mentionner que la condition suffisante est soumise à quelques hypothèses techniques supplémentaires, toujours réalisées en pratique. Comme résultat général, je pense que c'est le seul. Il concerne donc les suites par blocs, qui ont été introduites par Erdős. Tous les autres critères sont relatifs à des suites de structure très particulière.

Bibliographie

[1] Arratia, R., Independence of small prime factors of a uniformly distributed integer : total variation and Wasserstein metrics. Manuscrit, 1996.

[2] P. Billingsley, *Convergence of probability measures*, Wiley & sons, New York (1968).

[3] P. Billingsley, Additive functions and Brownian motion, *Notices Amer. math. Soc.* **17** (1970), 1050, abstract no.681-A9.

[4] P. Billingsley, The distribution of large prime factors, *Period. Math. Hungar.* **2** (1972), 283–289.

[5] P. Billingsley, The probability theory of additive functions, *The Annals of Probability* **2** (1974), no. 5, 749–791.

[6] P. Donnelly and G. Grimmett, On the asymptotic distribution of large prime factors. J. London Math. Soc. (2) **47** (1993), 395-404.

[7] P. Erdős, On the distribution function of additive functions, *Ann. of Math.* **47** (1946), 1–20.

[8] P. Erdős, On the distribution of prime divisors, *Aequationes Math.* **2** (1969), 177–183.

[9] P. Erdős, Some unconventional problems in number theory, *Astérisque* **61** (1979), 73–82.

[10] P. Erdős & M. Kac, On the Gaussian law of errors in the theory of additive functions, *Proc. Nat. Acad. Sci. U.S.A.* **25** (1939), 206–207.

[11] P. Erdős and M. Kac, The Gaussian law of errors in the theory of additive number-theoretic functions, *Amer. J. Math***62** (1940), 738–742.

[12] P. Erdős & R.R. Hall, Some distribution problems concerning the divisors of integers, *Acta Arith.* **26** (1974), 175–188.

[13] P. Erdős & R. R. Hall, The propinquity of divisors, *Bull. London Math. Soc.* **11** (1979), 304–307.

[14] J. Galambos, The sequences of prime divisors of integers, *Acta Arith.* **31** (1976), 213–218.

[15] R. R. Hall, Sums of imaginary powers of the divisors of integers, *J. London Math Soc.* (2) **9** (1975), 571–580.

[16] R.R. Hall, Sets of multiples and Behrend sequences, in : *A tribute to Paul Erdős* (editors A. Baker, B. Bollobás, A. Hajnal), Cambridge University Press, 1990, pp. 249–258.

[17] R.R. Hall, Ω theorems for the complex divisor function, *Math. Proc. Camb. Philos. Soc.* **115**, (1994), 145–177.

[18] R.R. Hall, *Sets of multiples*, Cambridge tracts in mathematics 118, Cambridge University Press, 1996.

[19] R.R. Hall & G.Tenenbaum, On Behrend sequences, *Math. Proc. Camb. Philos. Soc.* **112** (1992), 467–482.

[20] G.H. Hardy and S. Ramanujan, The normal number of prime factors of a number n, *Quart. J. Math.* **48** (1917), 76–92.

[21] J. Kubilius, Méthodes probabilistes en théorie des nombres (en russe), *Uspehi Mat. Nauk* **11** no. 2 (1956), 31–66 = *Amer. Math. Soc. Transl.* **19** (1962), 47–85.

[22] J. Kubilius, *Probabilistic methods in the theory of numbers*, Amer. Math. Soc. Translations of Math. Monographs, no. 11 (1964), Providence ; troisième impression corrigée, 1978.

[23] H. Maier & G.Tenenbaum, On the set of divisors of an integer, *Invent. Math.* **76** (1984), 121–128.

[24] H. Maier & G.Tenenbaum, On the normal concentration of divisors, *J. London Math. Soc.* (2) **31** (1985), 393–400.

[25] M. Mendès France & G. Tenenbaum, Systèmes de points, diviseurs et structure fractale, *Bull. Soc. Math. France* **121** (1993), 197–225.

[26] A. Raouj & G. Tenenbaum, Sur l'écart quadratique moyen des diviseurs d'un entier normal, *Math. Proc. Camb. Phil. Soc.* **126** (1999), 399–415.

[27] A. Stef & G. Tenenbaum, Entiers lexicographiques, *Ramanujan J.* **2** (1998), 167–184.

[28] G. Tenenbaum, Lois de répartition des diviseurs, 2, *Acta Arith.* **38** (1980), 1–36.

[29] G. Tenenbaum, Sur la densité divisorielle d'une suite d'entiers, *J. Number Theory* **15**, n° 3 (1982), 331-346.

[30] G. Tenenbaum, On block Behrend sequences, *Math. Proc. Camb. Philos. Soc.* **120** (1996), 355–367.

[31] G. Tenenbaum, Uniform distribution on divisors and Behrend sequences, *L'Enseignement Mathématique* **42** (1996), 153–197.

[32] A rate estimate in Billingsley's theorem for the size distribution of large prime factors, *Quart. J. Math. (Oxford)* **51** (2000), 385–403.

[33] P. Turán, On a Theorem of Hardy and Ramanujan, *J. London Math. Soc.* **9** (1934), 274–276.

Gérald Tenenbaum
Institut Élie Cartan
Université Henri Poincaré–Nancy 1
BP 239
54506 Vandœuvre Cedex
France