Entiers friables : un tour d'horizon

Cécile Dartyge

Entiers friables : un tour d'horizon

Cécile Dartyge

10 octobre 2019

Il sagit d'une version préliminaire à celle parue dans la Gazette des Mathématiciens. Le texte est identique à la version finale mais comporte plus de références bibliographiques.

1 Introduction

Un entier friable est un entier sans grand facteur premier. Plus précisément, notons respectivement $P^+(n)$ et $P^-(n)$ le plus grand et le plus petit facteur premier d'un entier naturel n.[1] Pour $y \geqslant 2$ on dira que n est y-friable si $P^+(n) \leqslant y$ et qu'il est y-criblé si $P^-(n) > y$. Le mot friable reflète la possibilité de fractionner ces entiers en petits diviseurs, les petits facteurs premiers. Lorsque la borne de friabilité y est très petite on peut les écrire comme des produits de diviseurs dont on maîtrise bien la taille. Cette souplesse dans la factorisation des entiers friables est à l'origine de nombreuses percées en théorie analytique des nombres. Un autre aspect fondamental est que tout entier n se décompose de manière unique sous la forme $n = ab$ où a est y-friable et b y-criblé. La partie criblée b possède alors une structure proche de celle d'un nombre premier tandis que la partie friable a se comporte comme un entier standard. Cette idée toute simple s'avère un point de départ souvent très efficace pour étudier des sommes apparaissant dans des problèmes de théorie analytique des nombres, comme par exemple dans le paragraphe 5.1 de cet article.

Les recherches sur les entiers friables ont véritablement commencé il y a un peu moins d'une centaine d'années. Elles se sont considérablement développées à partir des années 80 non seulement en raison de leur intérêt intrinsèque mais aussi pour leurs multiples applications.

Désignons par $S(x, y)$ l'ensemble des entiers y-friables n'excédant pas x et par $\Psi(x, y)$ son cardinal. Dans un premier temps, nous retraçons les différentes méthodes pour évaluer $\Psi(x, y)$ selon les tailles relatives de x et y et rappelons très brièvement quelques résultats multiplicatifs sur les entiers friables. Ensuite, nous décrivons leur utilisation dans des algorithmes de factorisation. Dans la dernière partie nous présentons divers problèmes de théorie des nombres pour lesquels des avancées importantes ont eu lieu grâce aux entiers friables.

1. Avec les conventions $P^+(1) = 1$ et $P^-(1) = \infty$.

Cette présentation est loin d'être exhaustive. On a plutôt voulu donner un aperçu du rôle des entiers friables dans différents domaines de la théorie des nombres. On pourra trouver des exposés bien plus complets dans les superbes articles de synthèse de Hildebrand et Tenenbaum [29], Granville [21], Pomerance [39]. Nous recommandons également le livre de Crandall et Pomerance [9] et celui de Tenenbaum [41] qui sont respectivement des références incontournables en théorie algorithmique et analytique des nombres.

Dans tout ce qui suit, la lettre p avec ou sans indice désigne un nombre premier, et on notera (a, b) le pgcd des entiers a et b. Pour abréger l'écriture, $\ln_k(t)$ sera pour $t > 0$, la k-ième itérée du logarithme népérien de t, en particulier pour $k = 2$, $\ln_2 t = \ln\ln t$.

2 Compter les friables

2.1 La fonction de Dickman

Il existe plusieurs approches pour déterminer $\Psi(x, y)$ selon la taille de y par rapport à x. Ces estimations font intervenir de manière essentielle le rapport

$$u = \frac{\ln x}{\ln y}.$$

Dickman [12] a montré en 1930 que pour tout $u > 0$ fixé, une proportion positive des entiers inférieurs à x est $x^{1/u}$-friable :

$$\lim_{x\to+\infty} \frac{\Psi(x, x^{1/u})}{x} = \varrho(u)$$

où ϱ, appelée fonction de Dickman, est l'unique fonction continue sur $\mathbb{R}^+$, dérivable sur $]1, +\infty[$, solution de l'équation différentielle aux différences

$$u\varrho'(u) = \varrho(u-1)$$

avec la condition initiale $\varrho(u) = 1$ pour $0 \leqslant u \leqslant 1$. Cette fonction $\varrho(u)$ est ainsi la probabilité pour qu'un entier inférieur à x soit $x^{1/u}$-friable. Elle apparaît également dans une situation sans lien évident avec les entiers friables : si $\{U_n\}_{n=1}^{\infty}$ est une suite de variables aléatoires indépendantes de loi uniforme sur $[0, 1]$ alors la série $Y = U_1 + U_1U_2 + U_1U_2U_3 + \cdots$ converge presque sûrement vers une variable aléatoire de densité $\mathrm{e}^{-\gamma}\varrho$, γ étant la constante d'Euler [2].

Ce phénomène d'équations différentielles aux différences n'est pas spécifique aux entiers friables. On le rencontre régulièrement dans des problèmes utilisant des méthodes de crible. Tradionnellement, on note $\Phi(x, y)$ le nombre d'entiers y-criblés inférieurs à x. On démontre alors avec un procédé analogue que la probabilité qu'un entier soit y-criblé est $\omega(u)$ (voir par exemple [41], chapitre III. 6), $\omega(u)$ étant la fonction de Buchstab. Elle est définie par $\omega(u) = 1/u$ pour $1 \leqslant u \leqslant 2$ et $(u\omega(u))' = \omega(u-1)$. On retrouve encore de telles fonctions dans

2. $\gamma = \lim_{N\to\infty} \sum_{n=1}^{N} 1/n - \ln N$.

des méthodes de crible comme par exemple les cribles de Rosser-Iwaniec ou de Jurkat-Richert.

Le lecteur trouvera dans [41] (chapitre III.5) une étude très précise de la fonction de Dickman. Cette fonction décroît très rapidement quand u tend vers $+\infty$, ainsi que le montre l'estimation obtenue par Hildebrand et Tenenbaum ([29] Corollary 2.3) pour $u \geqslant 1$:

$$\varrho(u) = \exp\Big\{ -u\Big(\ln u + \ln_2(u+2) - 1 + O\Big(\frac{\ln_2(u+2)}{\ln(u+2)}\Big)\Big)\Big\}.$$

La fonction ϱ est implantée dans plusieurs logiciels de mathématiques comme par exemple Sage. Les valeurs que nous donnons ci-dessous sont extraites de [21] : $\varrho(2) \approx 3,07 \times 10^{-2}$, $\varrho(5) \approx 3,55 \times 10^{-4}$, $\varrho(10) \approx 2,77 \times 10^{-11}$, $\varrho(20) \approx 2,46 \times 10^{-29}$, $\varrho(50) \approx 6,72 \times 10^{-97}$, etc.

2.2 $\Psi(x,y)$ pour y grand, avec des équations fonctionnelles

Ce premier résultat de Dickman fut précisé par de Bruijn [6], [7]. L'idée de départ est la suivante : pour $z \geqslant y$, un entier n compté dans $\Psi(x,z)$ est soit y-friable soit de la forme mp avec $P^+(m) \leqslant p$, p étant un nombre premier dans $]y,z]$. On en déduit *l'identité de Buchstab* :

$$\Psi(x,y) = \Psi(x,z) - \sum_{y<p\leqslant z} \Psi\Big(\frac{x}{p}, p\Big) \qquad (1 < y \leqslant z \leqslant x). \tag{1}$$

On initialise l'itération avec la formule évidente $\Psi(x,y) = \lfloor x \rfloor$ pour $y \geqslant x$. En observant que $x/p \leqslant p$ quand $\sqrt{x} \leqslant p \leqslant x$ et ainsi que $\Psi(x/p,p) = \lfloor x/p \rfloor$ puis en reportant cela dans (1) on obtient une formule asymptotique pour $y > x^{1/2}$. En insérant cette nouvelle formule de nouveau dans (1) on trouve une estimation de $\Psi(x,y)$ pour $y > x^{1/3}$ et ainsi de suite. Avec cette approche fonctionnelle on parvient à l'estimation uniforme pour $x \geqslant y \geqslant 2$ (voir par exemple le Théorème III.5.8 de [41]) :

$$\Psi(x,y) = x\varrho(u) + O\Big(\frac{x}{\ln y}\Big).$$

Cette formule devient moins intéressante pour de «grandes» valeurs de u. Par exemple si $u \geq \ln_2 y$, le terme principal $x\varrho(u)$ est dominé par le terme d'erreur $O(x/\ln y)$. La limite de la méthode de de Bruijn est en fait la région

$$y > \exp((\ln x)^{5/8+\varepsilon}), \tag{2}$$

pour $\varepsilon > 0$ fixé. Le résultat de de Bruijn sur l'estimation de $\Psi(x,y)$ qui précède, a été amélioré par Hildebrand [27] qui utilise une autre équation fonctionnelle :

$$\Psi(x,y)\ln x = \int_1^x \Psi(t,y)\frac{\mathrm{d}\,t}{t} + \sum_{\substack{p^k\leqslant x\\ p\leqslant y}} (\ln p)\Psi\Big(\frac{x}{p^k}, y\Big). \tag{3}$$

Cette formule s'obtient en évaluant de deux manières différentes la somme

$$S = \sum_{n \in S(x,y)} \ln n.$$

Tout d'abord, en effectuant une sommation d'Abel, on observe que

$$S = \Psi(x,y) \ln x - \int_1^x \Psi(t,y) \frac{\mathrm{d}\, t}{t},$$

puis en exploitant l'additivité du logarithme sous la forme $\ln n = \sum_{p^k | n} \ln p$, on obtient le deuxième terme du membre de droite de (3). Cette formule a l'avantage de conserver la borne de friabilité y constante de sorte que $\Psi(x,y)$ apparaît comme une moyenne d'elle-même en une seule variable ce qui rend la régularisation issue des itérations plus efficace. Hildebrand montre ainsi que, pour tout $\varepsilon > 0$ fixé, l'estimation

$$\Psi(x,y) = x\varrho(u)\Big\{1 + O\Big(\frac{\ln(u+1)}{\ln y}\Big)\Big\} \tag{4}$$

est valide uniformément dans une région bien plus vaste que (2) :

$$\exp((\ln_2 x)^{5/3+\varepsilon}) \leqslant y \leqslant x. \tag{5}$$

La région (5) est étroitement liée au terme d'erreur du théorème des nombres premiers. Tout progrès sur le terme d'erreur de ce théorème entraîne une amélioration de (5). En fait Hildebrand [26] a montré que l'hypothèse de Riemann [3] est vérifiée si et seulement si la formule (4) est valide dans la région $y \geqslant (\ln x)^{2+\varepsilon}$. Dans cette même région (5), Saias [40] obtient une estimation de $\Psi(x,y)$ plus précise que (4), le terme $x\varrho(u)$ étant remplacé par un terme $\Lambda(x,y)$ qui apparaissait déjà dans l'article de de Bruijn [6]. Il est malgré tout possible d'obtenir des formules asymptotiques pour $\ln(\Psi(x,y)/x)$ valables dans des domaines plus étendus. On trouvera par exemple dans [5], [29] ou [41] des formules très précises. Une conséquence de ces estimations est, pour tout $0 < \varepsilon < 1$ fixé,

$$\Psi(x,y) = xu^{-(1+o(1))u}, \tag{6}$$

quand y et u tendent vers ∞, uniformément pour $u \leqslant y^{1-\varepsilon}$. Cette formule permet d'appréhender l'ordre de grandeur de $\Psi(x,y)$. On en déduit par exemple que pour $\alpha > 1$, $\Psi(x,(\ln x)^\alpha) = x^{1-1/\alpha+o(1)}$.

2.3 Méthode géométrique pour y très petit

Lorsque y est plus petit qu'une puissance de $\ln x$, il faut procéder autrement pour avoir des formules asymptotiques. On remarque que $\Psi(x,y)$ est le nombre

3. La fonction ζ de Riemann est définie par $\zeta(s) = \sum_{n \geq 1} \frac{1}{n^s}$ pour $s \in \mathbb{C}$ de partie réelle strictement supérieure à 1. Elle admet un prolongement analytique noté encore ζ sur $\mathbb{C} \setminus \{1\}$ en une fonction ayant un pôle simple en 1. L'hypothèse de Riemann dit que les zéros non triviaux de ζ ont tous une partie réelle égale à 1/2.

de solutions $(m_p)_{p\leqslant y}$ dans $\mathbb{N}$ de l'inégalité $\prod_{p\leqslant y} p^{m_p} \leqslant x$. En prenant les logarithmes, cette équation devient $\sum_{p\leqslant y} m_p \ln p \leqslant \ln x$. On compte ainsi le nombre points à coordonnées entières d'un polytope de $\mathbb{R}^{\pi(y)}$, où $\pi(y)$ est le nombre de nombres premiers n'excédant pas y. Cette approche est efficace pour de très petites valeurs de y. Ennola [15] montre ainsi pour $2 \leqslant y \leqslant \sqrt{\ln x}$

$$\Psi(x,y) = \frac{1}{\pi(y)!} \prod_{p\leqslant y} \frac{\ln x}{\ln p} \Big\{ 1 + O\Big(\frac{y^2}{(\ln x)(\ln y)} \Big) \Big\}. \tag{7}$$

La Bretèche et Tenenbaum [5] ont apporté des améliorations à ce résultat suivant plusieurs directions (domaine en y, précision du terme d'erreur) en employant la méthode du col qui est l'objet du paragraphe suivant.

2.4 La méthode du col

La formule (4) fournit une approximation de $\Psi(x,y)$ par une fonction régulière ce qui n'est pas le cas de (7) qui dépend de $\pi(y)!$. Que se passe-t-il dans la zone non couverte par ces deux estimations, c'est-à-dire quand $\sqrt{\ln x} \leqslant y \leqslant \exp((\ln\ln x)^{5/3+\varepsilon})$?

Cette question a été résolue par Hildebrand et Tenenbaum [28] qui donnent une estimation de $\Psi(x,y)$ en adoptant une troisième approche : la méthode du col. L'indicatrice des entiers y-friables est une fonction multiplicative. Notons $\zeta(s,y)$ la série de Dirichlet associée :

$$\zeta(s,y) := \sum_{P^+(n)\leqslant y} \frac{1}{n^s} = \prod_{p\leqslant y} \Big(1 - \frac{1}{p^s}\Big)^{-1}.$$

Grâce à la formule de Perron ([41] chapitre II.2), on peut représenter $\Psi(x,y)$ sous la forme suivante pour tout $\alpha > 0$ et $x \notin \mathbb{N}$

$$\Psi(x,y) = \frac{1}{2i\pi} \int_{\alpha - i\infty}^{\alpha + i\infty} \zeta(s,y) x^s \frac{\mathrm{d}\, s}{s}.$$

Le choix optimal de α correspond au point col, c'est-à-dire l'unique solution de l'équation

$$-\frac{\zeta'(\alpha,y)}{\zeta(\alpha,y)} = \ln x, \text{ avec } -\frac{\zeta'(\alpha,y)}{\zeta(\alpha,y)} = \sum_{p\leqslant y} \frac{\ln p}{p^\alpha - 1}. \tag{8}$$

Hildebrand et Tenenbaum [28] obtiennent pour $x \geqslant y \geqslant 2$ la formule

$$\Psi(x,y) = \frac{x^\alpha \zeta(\alpha,y)}{\alpha\sqrt{2\pi\phi_2(\alpha,y)}} \Big(1 + O\Big(\frac{1}{u} + \frac{\ln y}{y}\Big)\Big),$$

où $\phi_2(s,y)$ est la dérivée seconde par rapport à s de $\ln\zeta(s,y)$.

A priori cette formule n'apporte pas d'information directement exploitable car l'expression de α donnée par (8) semble assez mystérieuse. Cependant, Hildebrand et Tenenbaum obtiennent à partir du théorème des nombres premiers

des estimations asymptotiques de $\alpha = \alpha(x, y)$. Cela leur permet de retrouver par cette voie les résultats de Hildebrand évoqués précédemment. Ils déterminent en outre des estimations très précises du comportement local de $\Psi(x, y)$. Par exemple, ils montrent lorsque y tend vers $+\infty$, que $\alpha(x, y) = o(1)$ si et seulement si $y \leqslant (\ln x)^{1+o(1)}$ où cette fois-ci, le "$o(1)$" se rapporte à x. Une conséquence est que l'équivalence $\Psi(2x, y) \sim \Psi(x, y)$ a lieu si et seulement si $y \leqslant (\ln x)^{1+o(1)}$.

Très récemment, La Bretèche et Tenenbaum [5] ont obtenu des estimations de $\Psi(x, y)$ dans la zone critique $1 \leqslant y \leqslant (\ln x)^{1+o(1)}$ élucidant complètement le comportement de cette fonction dans cette région. Leurs résultats mettent notamment en évidence des discontinuités importantes de $\Psi(x, y)$ lorsque y est un nombre premier de taille $o((\ln x)^{2/3}(\ln_2 x)^{1/3})$. Les entiers très friables ne sont pas lisses...

3 Quelques propriétés des entiers friables

Avant d'exposer les applications en cryptographie et dans d'autres problèmes de théorie analytique des nombres essayons de répondre à la question suivante : dans quelle mesure les entiers friables sont-ils des entiers comme les autres ?

Pour cela, on peut se baser sur plusieurs critères fréquemment utilisés en théorie analytique des nombres, la répartition de ces entiers dans les petits intervalles, ainsi que dans les progressions arithmétiques, ou encore étudier les moyennes friables de fonctions multiplicatives. La fin de cette partie est consacrée à un thème de la théorie probabiliste des nombres : l'inégalité de Turán-Kubilius.

3.1 Répartition dans les petits intervalles

On s'attend à ce que la répartition des entiers friables dans les petits intervalles soit harmonieuse, c'est-à-dire

$$\frac{\Psi(x + z, y) - \Psi(x, y)}{z} \sim \frac{\Psi(x, y)}{x}, \tag{9}$$

dans une grande région en x, y, z. Hildebrand [27] obtient une estimation de la forme (9) dans le même domaine (5) et pour des intervalles de taille $xy^{-5/12} \leqslant z \leqslant x$. Hildebrand et Tenenbaum [28] trouvent des estimations asymptotiques dans des domaines plus vastes en y mais en contrepartie avec des intervalles de longueur z d'un ordre de grandeur plus élevé.

Pour des intervalles plus courts, Friedlander et Lagarias [18] montrent qu'il existe une constante $c > 0$ telle que pour tous $\alpha > 0$ et $\beta > 1 - \alpha - c\alpha(1 - \alpha)$ fixés, l'intervalle $[x, x+x^\beta]$ contient une proportion positive d'entiers x^α-friables. On trouvera dans [29] et [21] d'autres résultats sur les entiers friables dans les petits intervalles. Très récemment Matomäki et Radzwiłł [36] ont réalisé une avancée spectaculaire : ils ont montré que pour tout $\varepsilon > 0$, il existait $C(\varepsilon) > 0$ tel que, pour tout x assez grand, l'intervalle $[x, x + C(\varepsilon)\sqrt{x}]$ contienne au moins

$\sqrt{x}/(\ln x)^4$ entiers x^ε-friables. On verra au paragraphe 5 que la recherche d'entiers friables dans de tels petits intervalles est un point important de plusieurs algorithmes de factorisation. C'est le cas par exemple du crible quadratique.

3.2 Entiers friables dans les progressions arithmétiques

Désignons par $\Psi(x, y; a, q)$ le nombre d'entiers y-friables congrus à a modulo q et $\Psi_q(x, y)$ le cardinal des entiers y-friables premiers à q. Lorsque $(a, q) \neq 1$ et est y-friable, ce cardinal vaut $\Psi(x/d, y; a/d, q/d)$ si on note $d = (a, q)$. On peut donc se limiter au cas où a et q sont premiers entre eux. Dans l'hypothèse d'une bonne répartition dans les classes inversibles modulo q, on attend pour $(a, q) = 1$,

$$\Psi(x, y; a, q) \sim \frac{\Psi_q(x, y)}{\varphi(q)}, \tag{10}$$

où φ est l'indicatrice d'Euler : $\varphi(n) = \sharp(\mathbb{Z}/n\mathbb{Z})^*$. Ici encore l'enjeu est double : obtenir des estimations dans des domaines les plus grands possibles à la fois par rapport à q et à y. En fait, l'estimation du terme principal $\Psi_q(x, y)$ est déjà un problème difficile.

De très beaux résultats dans ce sens existent dans la littérature tels les travaux de Fouvry et Tenenbaum [16], [17], Granville [19], [20] et tout récemment les articles de Harper [25], [24] et de Drappeau [13]. Harper [25] a montré que (10) a lieu dès que le rapport $\ln x/\ln q \to \infty$ et $q \leqslant y^{4\sqrt{e}-\varepsilon}$, $y \geqslant y_0(\varepsilon)$.

Cependant la condition $\ln x/\ln q \to \infty$ est très contraignante, elle ne couvre pas des zones où $q \approx x^\alpha$ même pour des réels $\alpha > 0$ très petits. Cet obstacle est résolu quand on s'intéresse à la répartition en moyenne sur q. Harper [24] montre ainsi qu'il existe $c > 0$ tel que pour $(\ln x)^c \leqslant y \leqslant x$, (10) est vérifié pour presque tout $q \leqslant \sqrt{\Psi(x, y)}(\ln x)^{-7/2}$ puis Drappeau [13] obtient un résultat de ce type en moyenne pour $q < x^{3/5-\varepsilon}$ mais avec une uniformité moins bonne sur les classes a modulo q et pour une zone de friabilité du type $(\ln x)^c \leqslant y \leqslant x^{c'}$ où $c' > 0$ est une constante très petite.

3.3 Fonctions multiplicatives et entiers friables

En théorie analytique des nombres, on est souvent confronté à l'estimation de sommes de la forme

$$\Psi_f(x, y) := \sum_{n \in S(x,y)} f(n)$$

où f est une fonction multiplicative c'est-à-dire telle que $f(mn) = f(m)f(n)$ si $(m, n) = 1$. Des exemples typiques sont la fonction τ qui donne le nombre de diviseurs, les caractères de Dirichlet, la fonction de Möbius qui sera définie au paragraphe 5.1, le nombre $r(n)$ de représentations de n comme somme de deux carrés, le nombre $\varrho_P(n)$ de racines de P modulo n pour un polynôme $P \in \mathbb{Z}[X]$ donné, etc. Lorsque f est une fonction oscillante telle que $\sum_{n \leqslant x} f(n) = o(x)$ comme c'est le cas par exemple de la fonction de Möbius ou des caractères

de Dirichlet, l'enjeu est d'obtenir la plus grande région possible en y telle que $\Psi_f(x,y) = o(\Psi(x,y))$. Quand f est à valeurs positives, on espère obtenir des formules asymptotiques. Il est fréquent dans les applications que les $f(p)$ soient proches en moyenne d'un réel κ : $\kappa = 2$ pour la fonction τ, $\kappa = 1$ pour ϱ_P si P est irréductible, etc. Tenenbaum et Wu [42] montrent sous de telles hypothèses des formules du type

$$\Psi_f(x,y) = C_\kappa(f) x \varrho_\kappa(u) \ln(y)^{\kappa-1}(1 + E(x,y)),$$

où ϱ_κ est la puissance fractionnaire de convolution d'ordre κ de la fonction de Dickman [4], $C_\kappa(f)$ est un produit eulérien convergent dépendant de f et de κ et $E(x,y)$ un terme d'erreur très explicite qu'il serait trop long de définir ici. Dans des circonstances très générales, nous avons $E(x,y) = o(1)$ pour des régions analogues à la zone (5) de Hildebrand pour $\Psi(x,y)$.

3.4 Inégalité de Turán-Kubilius

Un problème que l'on rencontre fréquemment en théorie analytique des nombres consiste à comprendre le comportement «presque partout» d'une fonction arithmétique f donnée. On cherche s'il existe une fonction *régulière* g telle que $|f(n) - g(n)|$ soit très petit pour presque tout entier n, c'est-à-dire pour n appartenant à un ensemble de densité naturelle 1 [5]. On dit alors que g est un ordre normal de f. Un exemple célèbre est le théorème de Hardy et Ramanujan [23] énonçant que $g(n) = \ln_2 n$ est un ordre normal de la fonction $\omega(n)$, le nombre de facteurs premiers de n ainsi que de la fonction $\Omega(n)$, le nombre de facteurs premiers comptés avec multiplicité.

Un candidat naturel en général pour g est la valeur moyenne de f, c'est-à-dire

$$g(N) = E_N(f) = \frac{1}{N} \sum_{n \leqslant N} f(n).$$

On entre dans le domaine de la théorie probabiliste des nombres. Une méthode souvent très efficace est d'évaluer la variance $V_N(f) = E_N(|f(n) - E_N(f)|^2)$ puis d'appliquer l'inégalité de Bienaymé-Tchébychev. Il faut malgré tout être en mesure d'évaluer cette variance, ou les moments d'ordre 1 et 2. L'inégalité de Turán-Kubilius fournit une telle majoration de la variance, pour les fonctions additives. Une fonction additive est une fonction h telle que $h(mn) = h(m) + h(n)$ dès que $(m,n) = 1$. Les fonctions $\ln n$, $\omega(n)$, $\Omega(n)$ sont des prototypes de fonctions additives. Ces fonctions sont déterminées par leurs valeurs sur les puissances de nombres premiers. Le lecteur trouvera dans [41] une construction détaillée du modèle probabiliste que l'on peut associer aux fonctions additives.

4. ϱ_κ est la fonction continue sur $]0,\infty[$, dérivable sur $[1,\infty[$ telle que $\varrho_\kappa(u) = u^{\kappa-1}/\Gamma(\kappa)$ si $0 < u \leqslant 1$ et $u\varrho_k'(u) + (1-\kappa)\varrho_\kappa(u) + \kappa\varrho_k(u-1) = 0$ pour $u > 1$.

5. Une partie A de $\mathbb{N}$ est de densité naturelle 1 si

$$\lim_{N\to\infty} \frac{1}{N} \sharp\{n \leq N : n \in A\} = 1.$$

En considérant que la probabilité qu'un entier n soit divisible exactement par p^k est égale à $1/p^k - 1/p^{k+1} = (1-1/p)p^{-k}$, il est naturel de penser que, si f est additive, $E_N(f)$ soit proche de $E_N^*(f) := \sum_{p^\nu \leqslant N} \frac{f(p^\nu)}{p^\nu}\Big(1-1/p\Big)$. La variance associée devient

$$V_N^*(f) = \frac{1}{N}\sum_{1\leqslant n\leqslant N} |f(n) - E_N^*(f)|^2.$$

L'inégalité de Turán-Kubilius énonce que pour toute fonction additive f à valeurs complexes, on a

$$V_N^*(f) \leqslant \Big\{4 + O\Big(\sqrt{\frac{\ln\ln N}{\ln N}}\Big)\Big\}B_N(f)^2,$$

où $B_N(f)^2$ est le moment d'ordre 2 correspondant :

$$B_N(f)^2 = \sum_{p^\nu\leqslant N} \frac{|f(p^\nu)|^2}{p^\nu}\Big(1-\frac{1}{p}\Big).$$

Une application immédiate est de retrouver une version quantitative du théorème de Hardy-Ramanujan évoqué précédemment. La Bretèche et Tenenbaum [4] (voir également Martin et Tenenbaum [35]) ont obtenu une telle inégalité pour les entiers friables. Pour $p \leqslant y$, la probabilité qu'un entier friable soit exactement divisible par p^k est proche de $(1-1/p^\alpha)p^{-k\alpha}$ où α est le point col défini par (8). Les espérances, variances et moments d'ordre 2 associés à ce modèle probabiliste pour les entiers friables, sont :

$$E_N^*(f,y) = \sum_{p^\nu\in S(N,y)} \frac{f(p^\nu)}{p^{\alpha\nu}}\Big(1-\frac{1}{p^\alpha}\Big),\ V_N^*(f,y) = \frac{1}{\Psi(N,y)}\sum_{n\in S(N,y)} |f(n)-E_N^*(f,y)|^2$$

$$\text{et } B_N(f,y)^2 = \sum_{p^\nu\in S(N,y)} \frac{|f(p^\nu)|^2}{p^{\alpha\nu}}\Big(1-\frac{1}{p^\alpha}\Big).$$

La Bretèche et Tenenbaum montrent alors qu'il existe une constante absolue $C>0$ telle que pour tous $2\leqslant y\leqslant N$, on ait

$$V_N^*(f,y) \leqslant CB_N(f,y)^2.$$

La Bretèche et Tenenbaum obtiennent en outre l'inégalité plus fine $V_N^*(f,y) \ll V(Z_f)$, où $V(Z_f)$ est la variance du modèle probabiliste friable Z_f associé à la fonction additive f. Ce théorème a de très belles applications sur les propriétés des entiers friables. Ici nous n'en évoquerons qu'une seule mais le lecteur en trouvera d'autres tout aussi spectaculaires dans [4]. Notons $p_j(n)$ la suite croissante des facteurs premiers de n. Un fait très surprenant est que pour presque tout entier n l'ordre de grandeur de $p_j(n)$ ne dépend que de j : pour presque tout $n\leq x$, $\ln_2(p_j(n)) \sim j$ pour $J_x \leq j \leq \omega(n)$, J_x étant une fonction positive tendant vers l'infini avec x (voir par exemple [22]).

L'inégalité de Turán-Kubilius sur les friables fournit un ordre normal de ces fonctions $p_j(n)$ quand n est friable. La Bretèche et Tenenbaum montrent que les petits facteurs premiers des entiers friables ont un comportement similaire aux entiers naturels mais que passé un certain seuil, il y a un phénomène de tassement de plus en plus important. Notamment pour $y \leqslant (\ln x)^{1+o(1)}$ et J_x comme précédemment, $p_j(n) = p_j^{1+o(1)}$ pour $J_x \leq j \leq \omega(n)$, pour presque tout $n \in S(x,y)$, où p_j est le j ième nombre premier. D'après le théorème des nombres premiers, $p_j \sim j \ln j$, la situation est donc très différentes de celle des entiers génériques.

4 Applications en théorie algorithmique des nombres et en cryptographie

La sécurité de divers systèmes de cryptographie à clé publique repose sur la difficulté de factoriser des entiers produits d'un petit nombre de grands facteurs premiers. Par exemple, la clé publique du système RSA est un entier N produit de deux «grands» facteurs premiers, soit $N = pq$. On décrypte le code si on réussit à déterminer les facteurs premiers p et q.

Les entiers friables ont une place très importante dans plusieurs algorithmes de factorisation et donc entre autres dans la détermination des facteurs p et q ci-dessus. Ils interviennent également dans le problème du logarithme discret et dans certains tests de primalité. Dans ce paragraphe, nous donnons un aperçu de leur rôle dans quelques-uns de ces algorithmes. Nous avons choisi des situations dont la présentation nécessitait assez peu de bagage mathématique. Nous laissons ainsi notamment de côté les algorithmes de factorisation ou les tests de primalité construits à partir des lois de groupes sur les courbes elliptiques et qui sont pourtant parmi les plus couramment utilisés.

La place des entiers friables dans ces algorithmes y est analogue à ce que nous décrivons ici, même si le contexte est différent. On pourra consulter par exemple l'exposé de Pomerance au congrès international des Mathématiques à Zurich en 1994 [39] ainsi que le livre de Crandall et Pomerance [9] qui nous ont beaucoup servi dans cette partie.

4.1 Le crible quadratique

Le crible quadratique a été inventé par Pomerance [38] au début des années 80. On cherche à factoriser un entier n que l'on sait composé. L'idée de départ est que si a et b sont deux entiers tels que $a \not\equiv \pm b \mod n$ et $a^2 \equiv b^2 \mod n$ alors $(a-b, n)$ sera un diviseur non trivial de n. Il s'agit maintenant de construire de tels entiers a et b.

La première étape du crible quadratique consiste à considérer les valeurs y-friables prises par le polynôme $Q(t) = t^2 - n$ lorsque t est proche de $\sqrt{n}$, disons $|t - \sqrt{n}| < n^\varepsilon$ avec $\varepsilon > 0$ petit. Pour de tels t, $Q(t)$ sera petit : $|Q(t)| \leqslant (2 + n^{-1/2+\varepsilon})n^{1/2+\varepsilon} < 3n^{1/2+\varepsilon}$. Il est naturel d'escompter que ces

valeurs ont des propriétés multiplicatives similaires à celles des entiers dans l'intervalle $]-3n^{1/2+\varepsilon}, 3n^{1/2+\varepsilon}[$. Pourquoi construire autant de valeurs de $Q(t)$ friables ? Notons $(t_1, Q(t_1)), \ldots, (t_N, Q(t_N))$ les couples de t_i avec $Q(t_i)$ friables ainsi obtenus. La deuxième idée de Pomerance est que si nous disposons d'au moins $N \geqslant \pi(y) + 1$ entiers y friables alors on pourra former un carré à partir de ces valeurs de $Q(t_i)$. Cela découle d'un raisonnement d'algèbre linéaire. Chaque $Q(t_i)$ se factorise sous la forme $Q(t_i) = \prod_{p \leqslant y} p^{v_p(Q(t_i))}$ où $v_p(a)$ désigne la valuation p-adique de a. On peut associer à chaque $Q(t_i)$ un vecteur de $\mathbb{F}_2^{\pi(y)}$ dont les coordonnées sont les $v_p(Q(t_i)) \mod 2$, $p \leqslant y$. Comme $N > \pi(y)$, on a construit plus de vecteurs que la dimension. Ces vecteurs ne sont donc pas indépendants, il existe $J \subset \{1, \ldots, N\}$ tel que $\sum_{j \in J} v_p(Q(t_j)) \equiv 0 \mod 2$ pour tout $p \leqslant y$, autrement dit tel que $\prod_{j \in J} \prod_{p \leqslant y} p^{v_p(Q(t_j))}$ soit un carré, que l'on note v^2. On aura ainsi

$$\begin{aligned}\Big(\prod_{j \in J} t_j\Big)^2 &\equiv \prod_{j \in J} (t_j^2 - n) \mod n \\ &\equiv v^2 \mod n.\end{aligned}$$

Si $\prod_{j \in J} t_j \not\equiv \pm v \pmod n$, $(v - \prod_{j \in J} t_j, n)$ sera un diviseur non trivial de n détecté à l'aide des entiers friables. En reprenant l'hypothèse que les valeurs des polynômes considérés se comportent comme des entiers naturels pris au hasard dans l'intervalle $]-3n^{1/2+\varepsilon}, 3n^{1/2+\varepsilon}[$ et en utilisant (6), Pomerance montre que la complexité du crible quadratique vaut $L(n)^{1+o(1)}$ avec $L(n) = \exp(\sqrt{\ln n \ln_2 n})$, $L(n)^{\sqrt{2}/2}$ étant la borne de friabilité optimale de l'algorithme.

4.2 Le crible algébrique

Le crible quadratique est en pratique utilisé pour factoriser des entiers avec moins d'une centaine de chiffres. Pour les entiers plus grands, on passe au crible algébrique qui est l'objet de ce paragraphe. On commence par construire un polynôme f de degré $d \geqslant 2$ tel que $f(m) \equiv 0 \mod n$ pour un entier m proche de $n^{1/d}$ où n est l'entier à factoriser. Par exemple, pour $m = \lfloor n^{1/d} \rfloor$, on peut former le polynôme f à partir du développement de n en base m : $n = m^d + c_{d-1}m^{d-1} + \cdots + c_1 m + c_0$, où les entiers c_j sont compris entre 0 et $m - 1$. On considère ensuite le polynôme $f(X) = X^d + c_{d-1}X^{d-1} + \cdots + c_1 X + c_0$. Si ce polynôme est réductible, on a tout de suite une factorisation de n. On peut donc supposer désormais le contraire. Soit $\theta \in \mathbb{C}$ une racine de $f(X)$. On cherche alors un ensemble S de couples d'entiers premiers entre eux (a, b) tels que l'on ait

$$\prod_{(a,b) \in S} (a - b\theta) = \gamma^2, \quad \prod_{(a,b) \in S} (a - bm) = v^2, \tag{11}$$

pour des $\gamma \in \mathbb{Z}[\theta]$, $v \in \mathbb{Z}$. La construction de tels carrés suit un procédé d'algèbre linéaire analogue à celui du crible quadratique. La première étape consiste ainsi à trouver des couples (a, b) tels que $(a - bm)$ et $N(a - b\theta)$ soient friables où N est la norme sur $\mathbb{Q}(\theta)$.

En supposant de nouveau que les valeurs des polynômes considérés se comportent comme des entiers naturels pris au hasard, Buhler, H. Lenstra et Pomerance [8] et [33] montrent que la complexité du crible algébrique est de l'ordre de $\exp(c(\ln n)^{1/3}(\ln_2 n)^{2/3})$ et serait atteinte pour des polynômes de degré $d \sim \left(\frac{3\ln n}{\ln_2 n}\right)^{1/3}$. Ces résultats sont basés entre autres sur des conjectures relatives à la répartition des entiers friables dans les petits intervalles et dans des suites polynomiales, qui sont actuellement hors d'atteinte notamment pour le crible algébrique où le degré du polynôme optimal est très élevé. Ces dernières années, plusieurs travaux ont porté sur ce sujet. Dans le cadre du crible algébrique, on vient de voir que les formes binaires de la forme $F(a,b) = (a - bm)N(a - b\theta)$ ont une place importante. Balog, Blomer, Tenenbaum et l'auteur [1] ont donné dans un cadre général pour des formes binaires $F \in \mathbb{Z}[X_1, X_2]$ des minorations de $\Psi_F(x,y) = |\{1 \leqslant a, b \leqslant x : P^+(F(a,b)) \leqslant y\}|$ pour $y \geqslant x^{\alpha_F + \varepsilon}$ où α_F dépend de la structure de F. Dans le cas où F est une forme binaire irréductible, la valeur $\alpha_F = \deg F - 2$ est admissible. Lachand [31], [32], [30] obtient des formules asymptotiques valables dans des régions où $y = x^{o(1)}$ dans le cas où f est une forme cubique ou un produit de formes affines (avec pour les formes cubiques des expressions explicites du "$o(1)$" de l'exposant de y ci-dessus).

4.3 Le problème du logarithme discret sur les entiers

Le problème du logarithme discret intervient dans plusieurs protocoles de cryptographie. Soient p un grand nombre premier, g un générateur de $\mathbb{F}_p^*$ et $t \in \mathbb{F}_p^*$. Le problème du logarithme discret [6] consiste à trouver ℓ tel que $g^\ell = t$. On écrit alors $\ell = \log_g t$. On commence par sélectionner les puissances g^m qui admettent un représentant y-friable. Si on en trouve suffisamment, on pourra déterminer par un raisonnement d'algèbre linéaire les logarithmes discrets des nombres premiers q inférieurs à y. Après cette étape, on considère les produits $g^m t$ où m est un entier choisi au hasard. Si l'un des $g^m t$ est y-friable, donc de la forme $g^m t = \prod_{i=1}^r q_i^{a_i}$, on pourra en déduire que $\log_g t = -m + \sum_{i=1}^r a_i \log_g(q_i)$.

5 Applications des entiers friables en analyse et en théorie des nombres

Les entiers friables ont à de nombreuses reprises ouvert des brèches dans des problèmes restés inattaquables durant des décennies. Dans cette partie nous décrivons très brièvement leur apport sur des sujets très différents.

5.1 Théorème des nombres premiers, théorème de Daboussi sur les fonctions multiplicatives

Dans la première moitié du siècle dernier, de nombreux mathématiciens étaient persuadés qu'il n'existait pas de preuve élémentaire du théorème des

6. On peut le formuler dans un cadre plus général en remplaçant $\mathbb{F}_p^*$ par un groupe cyclique.

nombres premiers, élémentaire signifiant uniquement avec les outils standard de l'analyse réelle, notamment sans faire appel à l'analyse complexe. Ce fut une énorme surprise lorsque Erdős et Selberg fournirent en 1949 une preuve élémentaire mais très difficile. En 1984, Daboussi [10] donne une preuve très élégante en utilisant les entiers friables. Désignons par μ la fonction de Möbius. Cette fonction est définie de la manière suivante : $\mu(n) = 0$ si n est divisible par le carré d'un nombre premier, sinon elle vaut $(-1)^{\omega(n)}$, $\omega(n)$ étant le nombre de facteurs premiers distincts de n. Un résultat classique de théorie des nombres énonce que le théorème des nombres premiers est équivalent à la formule

$$M(x) := \sum_{n \leqslant x} \mu(n) = o(x). \tag{12}$$

Une des idées de Daboussi est d'exprimer $M(x)$ en fonction de sommes de Möbius sur les friables $M(x,y) = \sum_{n \in S(x,y)} \mu(n)$. En écrivant $n = ab$ avec a y-friable et b y-criblé, on parvient en effet à la formule :

$$M(x) = \sum_{P^-(b) > y} \mu(b) M(x/b, y).$$

Les étapes suivantes suivent un déroulement plus naturel que la preuve élémentaire initiale d'Erdős et Selberg. Elles utilisent des estimations très simples sur les entiers criblés ainsi que sur les entiers friables, le passage clé étant la majoration d'une sorte de moyenne en y des quantités $M(x,y)$.

Ce procédé limpide de factorisation criblé-friable, combiné avec des méthodes de convolution [7] permet également de retrouver le théorème de Daboussi [11] suivant : si f est une fonction multiplicative (i.e. $f(mn) = f(m)f(n)$ si m et n sont premiers entre eux) de module n'excédant pas 1 alors pour tout α irrationnel, on a :

$$\lim_{x \to \infty} \frac{1}{x} \sum_{n \leqslant x} f(n) \exp(2i\pi n\alpha) = 0.$$

5.2 Les entiers friables dans le problème de Waring

Le problème de Waring consiste à trouver pour chaque entier $k \geqslant 2$, le plus petit entier s tel que tout entier naturel s'écrive comme la somme de s puissances k ièmes. Une version légèrement affaiblie est d'imposer seulement que tout entier *assez grand* soit somme de s puissances k ièmes. Cet entier s pour cette deuxième version est souvent noté $G(k)$. Par exemple $G(3) \leqslant 7$ d'après Linnik, $G(4) = 16$ d'après Davenport. La méthode du cercle consiste à écrire le nombre de telles représentations sous la forme d'une intégrale de Cauchy ou de Fourier. Si on note $R(n)$ le nombre de représentations de n comme sommes de s puissances k-ièmes, on a alors

$$R(n) = \int_0^1 F(\alpha)^s \exp(-2i\pi n\alpha)\, \mathrm{d}\alpha, \text{ avec } F(\alpha) = \sum_{m \leqslant n^{1/k}} \exp(2i\pi m^k \alpha).$$

7. Le produit de convolution de deux fonction arithmétiques est défini dans le paragraphe 5.3.

La contribution principale à cette intégrale provient des *arcs majeurs* qui correspondent aux α proches d'un rationnel de petit dénominateur. On note traditionnellement $\mathcal{M}$ l'ensemble de ces α, puis $\mathfrak{m} =]0,1[\setminus \mathcal{M}$ les *arcs mineurs*. Une part importante du travail consiste alors à montrer que la contribution des arcs mineurs est négligeable. On peut partir de majorations de la forme

$$\int_{\mathfrak{m}} |F(\alpha)|^s \, \mathrm{d}\alpha \leqslant \max_{\alpha \in \mathfrak{m}} |F(\alpha)|^{s-2\ell} \int_0^1 |F(\alpha)|^{2\ell} \, \mathrm{d}\alpha,$$

avec $2\ell \leqslant s$. L'intégrale du membre de droite ci-dessus correspond au nombre de solutions de l'équation diophantienne

$$x_1^k + \cdots + x_\ell^k = y_1^k + \cdots + y_\ell^k, \quad (1 \leqslant x_i, y_i \leqslant n^{1/k}).$$

En restreignant à des variables friables, Wooley ([43], [44]), parvient à établir des inégalités fonctionnelles entre les solutions d'une équation diophantienne faisant intervenir ℓ variables x_i, y_i friables et les solutions d'une équation pour $\ell - 1$ variables. Le procédé est très compliqué et ne peut être expliqué en quelques lignes, mais a permis à Wooley de montrer notamment que $G(k) \leq k \ln k + k \ln \ln k + O(k)$ quand $k \to \infty$, les majorations précédentes étant $\leq (2 + o(1))k \ln k$.

5.3 Sommation friable et identités de Davenport

Duffin [14] puis Fouvry et Tenenbaum [16] ont introduit un procédé de sommation pour les séries, la sommation friable ou P-sommation. Il s'agit de considérer les séries restreintes aux entiers friables puis d'étudier la convergence quand la borne de friabilité tend vers l'infini. Cela conduit à la définition de convergence friable suivante : on dit que la série $\sum \alpha_n$ est convergente au sens friable (ou P-convergente) vers α si

$$\sum_{P^+(n) \leqslant y} \alpha_n = \alpha + o(1) \quad (y \to +\infty).$$

La série sera dite *régulière* si sa somme friable α est égale à sa somme usuelle :

$$\lim_{y \to +\infty} \sum_{P^+(n) \leqslant y} \alpha_n = \alpha = \lim_{N \to +\infty} \sum_{n=1}^{N} \alpha_n.$$

Il peut arriver que la somme friable ne coïncide pas avec la somme usuelle. Le théorème 11 de [16] fournit une infinité d'exemples. Alors que pour $\theta \in \mathbb{R} \setminus \mathbb{Z}$ la série $\sum_{n \geqslant 1} \frac{\exp(2i\pi n\theta)}{n}$ converge au sens usuel et vaut $\log\Big(\frac{1}{1-\exp(2i\pi\theta)}\Big)$, où ici log désigne la détermination principale du logarithme, Fouvry et Tenenbaum montrent que pour tout rationnel de $]0,1[$, $\theta = a/q$ avec $(a,q) = 1$, $1 \leqslant a < q$ la somme friable vaut :

$$\lim_{y \to \infty} \sum_{P(n) \leqslant y} \frac{\exp(2i\pi na/q)}{n} = \log\Big(\frac{1}{1 - \exp(2i\pi a/q)}\Big) + \frac{\Lambda(q)}{\varphi(q)},$$

où Λ est la fonction de Von Mangoldt, elle est définie par $\Lambda(q) = \ln p$ si $q = p^k$, $\Lambda(q) = 0$ si q n'est pas une puissance de nombre premier.

La sommation friable permet de contourner le phénomène de Gibbs et ainsi de résoudre des questions ardues d'analyse comme celles relatives à l'identité de Davenport que nous exposons maintenant.

Le produit de convolution de Dirichlet de deux fonctions arithmétiques u, v est donné par

$$u * v(n) = \sum_{d|n} u(d)v(n/d) \qquad (n \geqslant 1).$$

L'élément neutre pour cette loi de groupe sur les fonctions arithmétiques est souvent noté δ. On a alors $\delta(n) = 1$ pour $n = 1$ et $\delta(n) = 0$ pour $n \geqslant 2$. Notons aussi $\mathbf{1}$ la fonction qui vaut 1 pour tous les entiers supérieurs à 1. On a alors la formule fondamentale $\delta = \mu * \mathbf{1}$.

Soit $B_1(t)$ la première fonction de Bernoulli, elle est définie par $B_1(t) = \{t\} - 1/2$ si $t \notin \mathbb{Z}$ et $B_1(t) = 0$ pour t entier, $\{t\}$ étant la partie fractionnaire de t. Elle coïncide partout avec sa série de Fourier :

$$B_1(\theta) = -\sum_{k\geqslant 1} \frac{\sin(2\pi k\theta)}{\pi k}.$$

À partir de cela, on obtient formellement pour deux fonctions arithmétiques f et g reliées par $f = g * \mathbf{1}$ la belle identité

$$\sum_{m\geqslant 1} \frac{f(m)}{\pi m} \sin(2\pi m\theta) + \sum_{n\geqslant 1} \frac{g(n)}{n} B_1(n\theta) = 0. \tag{13}$$

Cela amène Davenport à formuler le problème suivant : pour quels nombres réels θ la relation (13) est-elle valide ? C'est une question très difficile que l'on ne sait pas résoudre en général. Davenport a montré que si $(f, g) = (\delta, \mu)$ alors (13) est vérifiée pour tout $\theta \in \mathbb{R}$. Cependant, son argument ne s'étend pas aux cas emblématiques $(f, g) = (\ln, \Lambda)$, $(\tau, \mathbf{1})$, τ étant la fonction nombre de diviseurs. C'est seulement soixante années plus tard que ces cas sont résolus par La Bretèche et Tenenbaum [3]. Un des ingrédients fondamentaux de leur travail est l'emploi de la sommation friable qui est remarquablement bien adaptée à ce problème. Ils montrent ainsi que pour $(f, g) = (\ln, \Lambda)$, (13) a lieu pour tout θ réel, par contre pour $(f, g) = (\tau, \mathbf{1})$ ils obtiennent un critère sur le développement en fraction continue des θ irrationnels selon lequel (13) ait lieu ou non. Mentionnons également l'article de Martin [34] qui résout entre autres le problème de Davenport pour les puissances de convolution de $\mathbf{1}$.

5.4 Petits écarts entre nombres premiers

On termine cet article par une avancée retentissante obtenue grâce aux entiers friables : les travaux de Zhang [45] puis de Maynard [37] sur les petits écarts entre les nombres premiers. Zhang a fait sensation en 2013 [8] en montrant qu'il

8. l'article correspondant est paru en 2014.

existait une infinité de nombres premiers $p \neq p'$ tels que $|p - p'| < 70000000$. Suite à ce travail cette borne fut réduite à plusieurs reprises notamment dans le cadre de projets collaboratifs Polymath. À la fin de cette même année se produisit un nouveau coup de théâtre : Maynard annonce que cette borne peut être réduite à 600. Actuellement cette borne a été ramenée à 246. La conjecture des nombres premiers jumeaux qui correspond à une infinité d'écarts égaux à 2 ne semble plus aussi hors d'atteinte qu'il y a à peine dix ans.

Un ingrédient clé de la preuve de Zhang est un résultat de répartition en moyenne des nombres premiers dans des progressions arithmétiques de raisons friables. Cette structure friable permet de considérer des ensembles d'entiers inférieurs à x vérifiant des conditions de congruences modulo des entiers supérieurs à $x^{1/2}$ ce qui était crucial pour montrer un écart borné entre une infinité de nombres premiers. Très récemment Régis de la Bretèche [2] a rédigé un article passionnant pour la Gazette sur les projets collaboratifs Polymath autour des percées de Zhang [45] puis de Maynard [37] sur ce sujet. On renvoie le lecteur à [2] pour plus de détails sur cette magnifique avancée. Indéniablement de très belles mathématiques restent encore à découvrir grâce aux entiers friables.

Remerciements. Je tiens à remercier chaleureusement Pierrick Gaudry, Martine et Hervé Queffélec, Anne de Roton, Gérald Tenenbaum et les deux rapporteurs anonymes pour leurs relectures minutieuses et pour les nombreuses remarques et suggestions qu'ils ont proposées.

Références

[1] A. Balog, V. Blomer, C. Dartyge & G. Tenenbaum – « Friable values of binary forms », *Comment. Math. Helv.* **87** (2012), no. 3, p. 639–667.

[2] R. d. l. Bretèche – « Petits écarts entre les nombres premiers et polymath : une nouvelle manière de faire de la recherche en mathématiques ? », *SMF Gaz. des Math.* **140** (2014), p. 19–31.

[3] R. d. l. Bretèche & G. Tenenbaum – « Séries trigonométriques à coefficients arithmétiques », *J. Anal. Math. 92* **92** (2004), p. 1–79.

[4] — , « Entiers friables : inégalité de Turán-Kubilius et applications », *Invent. Math.* **159** (2005), p. 531–588.

[5] — , « Une nouvelle approche dans la théorie des entiers friables », *Compos. Math.* **153** (2017), p. 453–473.

[6] N. G. d. Bruijn – « On the number of positive integers $\leq x$ and free of prime factors $> y$ », *Nederl. Akad. Wetensch. Proc. Ser. A* **54** (1951), p. 50–60.

[7] — , « On the number of positive integers $\leq x$ and free of prime factors $> y$, II », *Nederl. Akad. Wetensch. Proc. Ser. A* **69** (1966), p. 239–247.

[8] J. Buhler, H. L. Jr. & C. Pomerance – « Factoring integers with the number field sieve », *In The development of the number field sieve, A.K. Lenstra and H.W. Lenstra Jr. (eds), Lecture Notes in Math.* **1554** (1993), p. 50–94.

[9] R. Crandall & C. Pomerance – *Prime numbers, a computational perspective*, vol. 4ème édition, Springer, 546 pp., 2001.

[10] H. Daboussi – « Sur le théorème des nombres premiers », *C. R. Acad. Sc. Paris, Série I* **298** (1984), no. 8, p. 161–164.

[11] — , « On a convolution method », *in : E. Aparicio, C. CalderónJ.C. Peral (eds), Congreso de Teoria de los Números (Universitad del País Vasco)* (1989), p. 110–137.

[12] K. Dickman – « On the frequency of numbers containing prime facors of a certain relative magnitude », *Ark. Mat. Astr. Fys.* **22** (1930), p. 1–14.

[13] S. Drappeau – « Théorèmes de type Fouvry-Iwaniec pour les entiers friables », *Compos. Math.* **151** (2015), p. 828–862.

[14] R. Duffin – « Representation of Fourier integrals as sums iii », *Proc. Amer. Math. Soc.* **8** (1957), p. 272–277.

[15] V. Ennola – « On numbers with small prime divisors », *Ann. Acad. Sci. Fenn. Ser. AI* **440** (1969), p. 16pp.

[16] E. Fouvry & G. Tenenbaum – « Entiers sans grand facteur premier en progressions arithmétiques », *Proc. London Math. Soc. (3)* **63** (1991), p. 449–494.

[17] — , « Répartition statistique des entiers sans grand facteur premier dans les progressions arithmétiques », *Proc. London Math. Soc. (3)* **72** (1996), p. 481–514.

[18] J. Friedlander & J. Lagarias – « On the distribution in short intervals of integers having no large prime factor », *J. Number Theory* **25** (1987), p. 249–273.

[19] A. Granville – « Integers, without large prime factors, in arithmetic progressions. I », *Acta Math.* **170** (1993), p. 255–273.

[20] — , « Integers, without large prime factors, in arithmetic progressions. II », *Philos. Trans. Roy. Soc. London Ser. A* **345** (1993), no. 1676, p. 349–362.

[21] — , « Smooth numbers : computational number theory and beyond », *Algorithmic number theory, MSRI Proceedings* **44** (2008), p. 267–323.

[22] R. R. Hall & G. Tenenbaum – *Divisors*, vol. 90, Cambridge University Press, 1988.

[23] G. Hardy & R. S. – « The normal number of prime factors of a number n », *Quart. J. Math.* **48** (1917), p. 76–92.

[24] A. J. Harper – « Bombieri-Vinogradov and Barban-Davenport-Halberstam type theorems for smooth numbers », *arXiv :1208.5992* . (2012).

[25] — , « On a paper of K. Soundararajan on smooth numbers in arithmetic progressions », *J. Number Theory* **132** (2012), no. 1, p. 182–199.

[26] A. Hildebrand – « Integers free of large prime factors and the Riemann Hypothesis », *Mathematika* **31** (1984), p. 258–271.

[27] — , « On the number of positive integers $\leq x$ and free of prime factors $> y$ », *J. Number Theory* **22** (1986), p. 289–307.

[28] A. Hildebrand & G. Tenenbaum – « On integers free of large prime factors », *Trans. of the Amer. Math. Soc.* **296** (1986), no. 1, p. 265–290.

[29] — , « Integers without large prime factors », *Journal de Théorie des Nombres de Bordeaux* **5** (1993), no. 2, p. 411–484.

[30] A. Lachand – « On the representation of friable integers by linear forms », *Acta Arith., à paraître.*

[31] — , *Entiers friables et formes binaires*, Thèse, Université de Lorraine, 2014.

[32] — , « Valeurs friables d'une forme quadratique et d'une forme linéaire », *Q. J. Math.* **66** (2015), no. 1, p. 225–244.

[33] A. K. Lenstra & H. W. L. J. (eds) – *The development of the number field sieve*, vol. 1554, Lecture Notes in Math. Springer, 546 pp., 1993.

[34] B. Martin – « Nouvelles identités de Davenport », *Funct. Approx. Comment. Math.* **37** (2007), no. 2, p. 293–328.

[35] B. Martin & G. Tenenbaum – « Sur l'inégalité de Turán-Kubilius friable », *J. Reine Angew. Math.* **647** (2010), p. 175–234.

[36] K. Matomäki & M. Radziwiłł – « Multiplicative functions in short intervals », *Ann. of Math. (2)* **183** (2016), no. 3, p. 1015–1056.

[37] J. Maynard – « Small gaps between primes », *Ann. of Math. (2)* **183** (2015), no. 1, p. 383–413.

[38] C. Pomerance – « Analysis and comparison of some integer factoring algorithms », in *Computational Methods in Number Theory (H. W. Lenstra, Jr and R. Tijdeman, eds. Math. Centre Tracts 154/155, Mathematish Centrum, Amsterdam*, 1982, p. 89–139.

[39] — , « The role of smooth sumbers in number theoretic algorithms », *Proceedings of the international comgress of mathematiciens, Zurich Switzerland 1994* **5** (1995), no. 2, p. 411–422.

[40] E. Saias – « Sur le nombre des entiers sans grand facteur premier », *J. Number Theory* **32** (1989), p. 78–99.

[41] G. Tenenbaum – *Introduction à la théorie analytique et probabiliste des nombres*, vol. 4ème édition, coll. Échelles, Belin, 592 pp., 2015.

[42] G. Tenenbaum & J. Wu – « Moyennes de certaines fonctions multiplicatives sur les entiers friables », *J. Reine Angew. Math.* **564** (2003), p. 119–166.

[43] R. C. Vaughan – *The hardy littlewood method*, vol. Second edition, Cambridge University Press, 248 pp., 1997.

[44] T. D. Wooley – « Large improvements in Waring's problem », *Ann. of Maths.* **135** (1992), p. 131–164.

[45] Y. Zhang – « Bounded gaps between primes », *Ann. of Math. (2)* **179** (2014), no. 3, p. 1121–1174.