Sur les modèles probabilistes de l'arithmétique

Brussels Summer School
of Mathematics 2/8/2013

Gérald Tenenbaum
Institut Élie Cartan
Université de Lorraine
BP 70239
54506 Vandœuvre-lès-Nancy Cedex
France

gerald.tenenbaum@univ-lorraine.fr

1. Une « vraie » probabilité sur $\mathcal{P}(\mathbb{N})$?

1·1. Essai naïf

$\sum_n p_n = 1$: $\quad \mathbb{P}(\mathcal{A}) := \sum_{n\in\mathcal{A}} p_n \quad (\mathcal{A} \subset \mathbb{N})$.

Intuition : $\mathbb{P}(2\mathbb{N}) = \frac{1}{2}$, $\mathbb{P}(3\mathbb{N}) = \frac{1}{3}$, ... , $\mathbb{P}(a\mathbb{N}) = 1/a \quad (a \geqslant 1)$.

Exercice : Si $\mathbb{N}_a := \mathbb{N}^* \setminus a\mathbb{N}^*$ $(a \geqslant 1)$, alors

$\mathbb{P}(a\mathbb{N}^*) = 1/a$ $(a \geqslant 1) \Rightarrow \mathbb{P}(\mathbb{N}_a \cap \mathbb{N}_b) = (1-1/a)(1-1/b) \quad ((a,b)=1)$.

Preuve : $(a,b) = 1 \Rightarrow a\mathbb{N}^* \cap b\mathbb{N}^* = ab\mathbb{N}^* \Rightarrow \mathbb{P}(a\mathbb{N}^* \cap b\mathbb{N}^*) = 1/ab$

donc $\mathbb{P}(\mathbb{N}_a \cap \mathbb{N}_b) = 1 - \mathbb{P}(a\mathbb{N}^* \cup b\mathbb{N}^*) = 1 - \mathbb{P}(a\mathbb{N}^*) - \mathbb{P}(b\mathbb{N}^*) + \mathbb{P}(a\mathbb{N}^* \cap b\mathbb{N}^*)$

$= 1 - 1/a - 1/b + 1/ab = (1-1/a)(1-1/b)$

Corollaire :

$(\forall n) \quad p_n \leqslant \mathbb{P}(\cap_{n<p\leqslant N} \mathbb{N}_p) = \prod_{n<p\leqslant N}(1-1/p) = o(1) \quad (N \to \infty)$

donc $p_n = 0$ $(n = 1, 2, \ldots)$.

1·2. Densités

$N \geqslant 1$, $\Omega_N := [1, N] \cap \mathbb{N}$, $\mathcal{B}_N := \mathcal{P}(\Omega_N)$, ν_N (mesure de comptage).

$\mathbb{P}(\mathcal{A}) \to \mathrm{dens}(\mathcal{A}) := \lim_{N\to\infty} \nu_N(\mathcal{A})$.

Pertes : σ-additivité, mesurabilité universelle.

Gains : accord avec l'intuition, $(\Omega_N, \mathcal{A}_N, \nu_N)$ est un espace probabilisé.

Exemple :

$\mathcal{U} := \{n \in \mathbb{N}^* : \text{premier chiffre de } n = 1 \text{ en base } 10\}$, $\mathcal{U}_N := \big|\mathcal{U} \cap [1, N]\big|$.

$n \in \mathcal{U}_N \Leftrightarrow \exists m \geqslant 0 : 10^m \leqslant n < 10^{m+1}$ et $n \leqslant N$, donc

$|\mathcal{U}_{10^k-1}| = 1 + 10 + 100 + \cdots + 10^{k-1} = \frac{1}{9}(10^k - 1)$,

$|\mathcal{U}_{2\cdot 10^k-1}| = |\mathcal{U}_{10^k-1}| + 10^k = \frac{5}{9}(2 \cdot 10^k - 1) + \frac{4}{9}$.

$\liminf_{N\to\infty} |\mathcal{U}_N|/N = \frac{1}{9} < \frac{5}{9} = \limsup_{N\to\infty} |\mathcal{U}_N|/N$.

Variante : remplacer ν_N par une autre mesure discrète sur Ω_N. Par exemple

$$\lambda_N(\mathcal{A}) := \frac{1}{L_N} \sum_{n\in\mathcal{A},\, 1\leqslant n\leqslant N} \frac{1}{n}, \quad L_N = \sum_{1\leqslant n\leqslant N} \frac{1}{n} \sim \ln N \quad (N \to \infty).$$

Alors $\mathrm{dens}_\lambda(\mathcal{U}) = \dfrac{\ln 2}{\ln 10} \in \left[\frac{1}{9}, \frac{5}{9}\right]$.

2. Modèle de Kubilius

2·1. Indépendance approchée

Les v.a. $\xi_p : \Omega_N \to \{0,1\}$ $(p \in \mathcal{P})$ définies par $\xi_p(n) := \begin{cases} 1 & \text{si } p|n, \\ 0 & \text{si } p \nmid n, \end{cases}$ décrivent la structure multiplicative de Ω_N.

$$E_N(\xi_p) = \nu_N(\xi_p = 1) = \frac{1}{N}\left\lfloor \frac{N}{p} \right\rfloor = \frac{1}{p} + O\Big(\frac{1}{N}\Big).$$

$$(p \neq q) \quad E_N(\xi_p \xi_q) = \frac{1}{pq} + O\Big(\frac{1}{N}\Big) = E_N(\xi_p) E_N(\xi_q) + O\Big(\frac{1}{N}\Big).$$

Approximation pertinente ssi pq est « petit » : $pq > N \Rightarrow E_N(\xi_p \xi_q) = 0$.
Premier modèle pour $\{\xi_p : p \leqslant N\}$: une famille $\{X_p : p \leqslant N\}$ de v.a. de Bernoulli *indépendantes*, définies sur un espace probabilisé $(\Omega, \mathcal{B}, \mathbb{P})$ et telles que $\mathbb{P}(X_p = 1) = 1/p$, $\mathbb{P}(X_p = 0) = 1 - 1/p$.

2·2. Fonctions arithmétiques additives

Somme de v.a.i. ← fonction arithmétique (fortement) additive $f : \Omega_N \to \mathbb{C}$,

$f(n) = \sum_{p \leqslant N} f(p)\xi_p(n) = \sum_{p \mid n} f(p) \leftrightarrow Z_{f,N} := \sum_{p \leqslant N} f(p) X_p.$

$$\mathbb{E}(Z_{f,N}) = \sum_{p \leqslant N} \frac{f(p)}{p}, \quad \mathbb{V}(X_p) = \frac{1}{p}\Big(1 - \frac{1}{p}\Big) \Rightarrow \mathbb{V}(Z_{f,N}) = \sum_{p \leqslant N} \frac{f(p)^2}{p}\Big(1 - \frac{1}{p}\Big).$$

Exemple : $\omega(n) := \sum_{p \mid n} 1$,

$\mathbb{E}(Z_{\omega,N}) = \ln_2 N + O(1), \quad \mathbb{V}(Z_{\omega,N}) = \ln_2 N + O(1) \quad (N \to \infty).$

Premier test : comparaison des variances. On remplace la variance empirique $\nu_N\big(|f - E_N(f)|^2\big)$ par la variance « semi-empirique »

$$V_N(f) := \nu_N\big(|f - \mathbb{E}(Z_{f,N})|^2\big) = \frac{1}{N} \sum_{n \leqslant N} |f(n) - \mathbb{E}(Z_{f,N})|^2 .$$

Turán (1934), Kubilius (1956, 1962), ..., Hildebrand, Kubilius, Stein (1983), La Bretèche-GT (2005) :

$V_N(f) \leqslant C_N \mathbb{V}(Z_{f,N})$: C_N indépendante de f, $\limsup C_N = 2$.

Forme actuelle de l'inégalité de Turán–Kubilius.

Applications :

- Bienaymé-Tchébychev

$$\nu_N\Big(|\omega(n)-\mathbb{E}(Z_{\omega,N})|>\xi\sqrt{\mathbb{V}(Z_{\omega,N})}\Big)\leqslant C/\xi^2\quad(\xi\geqslant 1).$$

$$\mathbb{E}(Z_{\omega,N})=\sum_{p\leqslant N}\frac{1}{p}+O(1)=\ln_2 N+O(1),$$

$$\mathbb{V}(Z_{\omega,N})=\sum_{p\leqslant N}\frac{1}{p}+O(1)=\ln_2 N+O(1).$$

$(\forall \xi_N\to\infty)\quad |\omega(n)-\ln_2 N|\leqslant \xi_N\sqrt{\ln_2 N}$ sauf pour au plus $o(N)$ exceptions.

- Erdős : $n=p_1(n)^{\alpha_1(n)}\cdots p_k(n)^{\alpha_k(n)}$, $k=\omega(n)$.

$$\nu_N\left\{\sup_{H\leqslant j\leqslant\omega(n)}\frac{|\ln_2 p_j(n)-j|}{j^{3/4}}>1\right\}\leqslant\frac{C}{H^{1/4}}\qquad(H\geqslant 1).$$

La taille du j-ième facteur premier d'un entier aléatoire ne dépend que de j !

Plus précisément $\ln_2 p_j(n)\approx j$, ou encore $p_j(n)\approx \exp\exp j$.

Preuve.

On pose $\omega(n,t) := |\{p : p|n,\ p \leqslant t\}$. Noter que $\omega(n, p_j(n)) = j$.

$$\mathbb{E}(Z_{\omega(\cdot,t),N}) = \sum_{p\leqslant t} \frac{1}{p} = \ln_2 t + O(1), \quad \mathbb{V}(Z_{\omega(\cdot,t),N}) = \ln_2 t + O(1) \quad (t > 3).$$

Bienaymé-Tchébychev + Turán-Kubilius :

$$\nu_N\big(|\omega(n,t) - \ln_2 t| > \xi\sqrt{\ln_2 t}\big) \leqslant C/\xi^2.$$

$t = t_k := \exp\exp k^4$, $\quad \xi := k \qquad (k = 1, 2, \cdots)$

$$|\omega(n, t_k) - k^4| \leqslant k^3 \qquad (k > K)$$

sauf pour au plus $C'N/K$ entiers $n \leqslant N$ exceptionnels.

Si $t_k < t \leqslant t_{k+1}$, alors $\omega(n, t_k) = k^4 \leqslant \omega(n, t) \leqslant (k+1)^4 = \omega(n, t_{k+1})$.

donc $\ln_2 t = k^4 + O(k^3) = \ln_2 t_k + O\big((\ln_2 t_k)^{3/4}\big)$.

Donc $(T = \exp\exp K^4)$

$$|\omega(n,t) - \ln_2 t| \leqslant (\ln_2 t)^{3/4} \qquad (t > T)$$

sauf pour au plus $C''N/K = C''N/(\ln_2 T)^{1/4}$ entiers n exceptionnels.

Fin de la preuve : $t := p_j(n)$, $H := \ln_2 T$.

- Loi du logarithme itéré ?

Oui ! (Erdős, 1946) : $\exists \mathcal{A} : \operatorname{dens} \mathcal{A} = 1$ et
$|\ln_2 p_j(n) - j| \leqslant \{1 + o(1)\}\sqrt{2j \ln_2 j} \quad (n \in \mathcal{A},\ j \to \infty)$

- Théorème des trois séries (Kolmogorov) $\leftrightarrow$ th. d'Erdős–Wintner (1939)

CNS pour qu'une fonction arithmétique additive possède une loi limite, i.e. que les f.r. $F_N(z) := \nu_N\{f \leqslant z\}$ convergent faiblement vers une f.r. F :

$$\sum_{|f(p)|\leqslant 1} \frac{f(p)}{p} \text{ cv}, \qquad \sum_{|f(p)|>1} \frac{1}{p} < \infty, \qquad \sum_{|f(p)|\leqslant 1} \frac{f(p)^2}{p} < \infty.$$

Remarque. Les valeurs $f(p^\nu)$ telles que $\nu \geqslant 2$ n'interviennent pas dans le critère.

2·3. Distance en variation totale

Turán–Kubilius :

$$\int_{\mathbb{R}} \{z - \mathbb{E}(Z_{f,N})\}^2 \, \mathrm{d}\nu_N(f \leqslant z) \leqslant C_N \int_{\mathbb{R}} \{z - \mathbb{E}(Z_{f,N})\}^2 \, \mathrm{d}\mathbb{P}(Z_{f,N} \leqslant z)$$

Autre comparaison quantitative des mesures ?

$$\delta(f, Z_{f,N}) := \sup_{A \subset \mathbb{R}} |\nu_N\{f \in A\} - \mathbb{P}(Z_{f,N} \in A)|.$$

$$K_N := \sup_f \delta(f, Z_{f,N}) \to 0 \, ?$$

Non ! À cause du défaut d'indépendance des grands nombres premiers.

$\mathbb{A}_y := \{f \text{ additive} : p > y \Rightarrow f(p) = 0\}$

Jauge de Kubilius : $K(N, y) := \sup_{f \in \mathbb{A}_y} \delta(f, Z_{f,N})$.

Kubilius (1956) : $K(N, y) \ll \mathrm{e}^{-cu}$ $\quad (N =: y^u)$.

Barban & Vinogradov (1964) : $K(N, y) \ll u^{-u/8} + N^{-1/15}$

GT (1999) : $K(N, y) \ll u^{-u} + N^{-1+o(1)}$ [exposants optimaux]

Principe : *Tout théorème concernant une suite finie de variables aléatoires de Bernoulli indépendantes* $\{X_p : p \leqslant N^\varepsilon\}$ ($\mathbb{P}(X_p = 1) = 1/p$) *sera également vrai pour la suite* $\{\xi_p : p \leqslant N^\varepsilon\}$ *sur* Ω_N *avec une erreur acceptable si* $\varepsilon = \varepsilon_N \to 0$ $(N \to \infty)$.

Exemple. Théorème de la limite centrale :

$S_N := \sum_{p \leqslant N^\varepsilon} X_p$.

$$\mathbb{E}\big(S_N\big) = \ln_2 N + O_\varepsilon(1), \quad \mathbb{V}\big(S_N\big) = \ln_2 N + O_\varepsilon(1).$$

$$\lim_{N\to\infty} \mathbb{P}\Big(S_N - \mathbb{E}(S_N) \leqslant z\sqrt{\mathbb{V}(S_N)}\Big) = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{z} \mathrm{e}^{-t^2/2}\,\mathrm{d}t \qquad (z \in \mathbb{R}).$$

Donc (Erdős-Kac, 1940)

$$\lim_{N\to\infty} \nu_N\Big(\omega(n) - \ln_2 N \leqslant z\sqrt{\ln_2 N}\Big) = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{z} \mathrm{e}^{-t^2/2}\,\mathrm{d}t \qquad (z \in \mathbb{R}).$$

Acte de naissance de la théorie probabiliste des nombres.

2·4. Définitions intrinsèques

$P^-(n) := \min_{p|n} p$, $P^+(n) := \max_{p|n} p$, $P^-(1) = \infty$, $P^+(1) = 1$.

$\Phi(N,y) := |\{n \leqslant N : P^-(n) > y\}|$, $\Psi(N,y) := |\{n \leqslant N : P^+(n) \leqslant y\}|$.

$\mathcal{T}_y$ sous-tribu de $\mathcal{P}(\Omega_N)$ engendrée par les

$$E_a := \{m \leqslant n : m = ab,\ P^-(b) > y\} \qquad (P^+(a) \leqslant y).$$

Ainsi $\nu_N(E_a) = \dfrac{1}{N}\Phi\left(\dfrac{N}{a}, y\right)$ $(P^+(a) \leqslant y)$.

Modèle probabiliste de $(\Omega_N, \mathcal{T}_y, \nu_N)$: $(\Omega, \mathcal{T}_y^*, \mathbb{P}_y)$, où

- Ω ensemble abstrait muni de $\pi(y)$ partitions $\Omega = \cup_{j\geqslant 0}\omega_{p,j}$ $(p \leqslant y)$
- $\mathcal{T}_y^*$: tribu engendrée par les intersections finies d'ensembles $\omega_{p,j}$.
- $E_a \leftrightarrow E_a^* := \cap_{p^j \| a}\omega_{p,j}$ $(P^+(a) \leqslant y)$
- $\mathbb{P}_y(\omega_{p,j}) := (1-1/p)p^{-j}$
- $\omega_{p,j} \perp \omega_{q,k}$ $(p \neq q)$.

E partie $\mathcal{T}_y$-mesurable $\Omega_N \leftrightarrow E^* \subset \Omega : E^* := \bigcup_{E_a \subset E} E_a^*$.

$$K(N,y) := \sup_{E \in \mathcal{T}_y} |\nu_N(E) - \mathbb{P}_y(E^*)|$$

$$= \tfrac{1}{2} \sum_{P^+(a) \leqslant y} \left| \frac{1}{N} \Phi\Big(\frac{N}{a}, y\Big) - \frac{1}{a} \prod_{p \leqslant y} \Big(1 - \frac{1}{p}\Big) \right|.$$

3. Entiers friables, entiers criblés

3·1. Définitions

$\mathbb{N}^* \ni a$ est dit y-friable $\Leftrightarrow P^+(a) \leqslant y$.

$\mathbb{N}^* \ni b$ est dit y-criblé $\Leftrightarrow P^-(b) > y$.

Décomposition canonique $n = ab$ avec $P^+(a) \leqslant y, P^-(b) > y$.

Heuristique :

$a \approx$ entier ordinaire ;

$b \approx$ nombre premier.

3·2. Entiers criblés

$\Phi(x,y)$ = nombre des entiers restants après application du crible d'Ératosthène.

(GT 1990) $x \geqslant y \geqslant 2$, $x = y^u$: $\Phi(x,y) = x \prod_{p \leqslant y} \left(1 - \frac{1}{p}\right) + O\left(x\mathrm{e}^{-u/2}\right)$.

Remarque. Terme principal probabiliste faux si u est borné !

Pour $y = \sqrt{x}$, $\quad \Phi(x,\sqrt{x}) = \pi(x) - \pi\left(\sqrt{x}\right) + 1 \sim \frac{x}{\ln x}$,

mais (Mertens) : $\quad x \prod_{p \leqslant y} \left(1 - \frac{1}{p}\right) \sim \frac{2\mathrm{e}^{-\gamma} x}{\ln x} \qquad (x \to \infty)$.

Soit ω la fonction de Buchstab, solution de $\{u\omega(u)\}' = \omega(u-1)$ telle que $u\omega(u) = 1$ $(1 \leqslant u \leqslant 2)$. Alors (classique)

$$\Phi(x,y) = \frac{x\omega(u) - y}{\log y} + O\left(\frac{x}{(\log y)^2}\right) \quad (x \geqslant y \geqslant 2)$$

(ce qui implique $\lim_{u\to\infty} \omega(u) = \mathrm{e}^{-\gamma}$).

Meilleure approximation connue (GT, 1995)

$$\Phi(x,y) = \mathrm{e}^{\gamma} \prod_{p\leqslant y} \Big(1-\frac{1}{p}\Big)(x\omega(u)-y)\Big\{1+O\Big(\frac{\mathrm{e}^{-u/3}}{\log y}\Big)\Big\} \qquad (x \geqslant 2y \geqslant 4).$$

3·3. Entiers friables

$\Psi(x,y)$:= nombre des entiers y-friables $\leqslant x$.

Dickman (1930), de Bruijn (1951, 1966), Hildebrand (1986), Hildebrand–Tenenbaum (1986), Saias (1989), Granville, Balog, Maier, Tenenbaum-Wu, La Bretèche-Tenenbaum, Maier–Sankaranarayanan...

Équation fonctionnelle : $\Psi(x,y) = 1 + \sum_{p\leqslant y} \Psi(x/p,p)$.

Dickman (1930) : $\Psi(x,y) \sim x\varrho(u) \qquad (x = y^u,\ u \text{ fixé},\ y \to \infty)$.

ϱ = fonction de Dickman : $\begin{cases} \varrho(u) := 1 & (0 \leqslant u \leqslant 1), \\ u\varrho'(u) + \varrho(u-1) = 0 & (u > 1). \end{cases}$

Si $\{U_j\}_{j=1}^{\infty}$ est une suite de v.a.i. équidistribuées de loi uniforme sur $[0,1]$, $\mathrm{e}^{-\gamma}\varrho(u-1)$ est la densité de probabilités de

$$1 + U_1 + U_1U_2 + U_1U_2U_3 + \cdots$$

- Hildebrand (1984) : la validité de

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

pour $y \geqslant (\ln x)^{2+\varepsilon}$ équivaut à l'hypothèse de Riemann.

- Hildebrand (1986) : on a (1) pour $x = y^u$, et

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

- Hildebrand-GT (1986) : $0 < \varepsilon < \frac{1}{2}$, $y \geqslant (\ln x)^{1+\varepsilon}$, $L_\varepsilon(y) := \mathrm{e}^{(\log y)^{3/5-\varepsilon}}$,

$$\Psi(x,y) = x\varrho(u)\exp\Big\{O\Big(\frac{\ln(u+1)}{\ln y} + \frac{u}{L_\varepsilon(y)}\Big)\Big\}.$$

Méthode du col : $\sum_{P^+(n)\leqslant y} 1/n^s = \prod_{p\leqslant y}(1-p^{-s})^{-1} =: \zeta(s,y)$

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

$$\sum_{p\leqslant y}\frac{\ln p}{p^\alpha-1} = \ln y.$$

$$\alpha \approx \frac{1}{\ln y}\ln\Big(1+\frac{y}{\ln x}\Big).$$

$$\Psi(x,y) \approx \frac{x^\alpha\zeta(\alpha,y)}{\alpha\sqrt{2\pi(\ln x)(\ln y)\ln\{1+(\ln x)/y\}}} \qquad (x\geqslant y\geqslant 2)$$

Sous-produits : comportement local

$$\Psi(2x,y)\sim\Psi(x,y)\Leftrightarrow y\leqslant(\ln x)^{1+o(1)},$$

$$\Psi(2x,y)\sim 2\Psi(x,y)\ \Leftrightarrow\ (\ln y)/\ln_2 x\to\infty.$$

4. Applications de la théorie des entiers friables

4·1. Preuve élementaire du théorème des nombres premiers

Fonction de Möbius :

$$\mu(n) := \begin{cases} (-1)^r & \text{si } n = p_1 p_2 \cdots p_r \text{ et } p_i \neq p_j \ (i \neq j) \\ 0 & \text{si } \exists p^2 | n. \end{cases}$$

Daboussi a montré que le théorème des nombres premiers équivaut élémentairement à

$$\lim_{y \to \infty} \prod_{p \leqslant y} \left(1 - \frac{1}{p}\right) \int_1^\infty \frac{|M(x,y)|}{x^2} \, \mathrm{d}x = 0$$

où $M(x,y) := \sum_{n \leqslant x,\, P^+(n) \leqslant y} \mu(n)$.

Cela revient à montrer le théorème des nombres premiers en considérant un modèle des entiers constitué à partir d'un nombre fini de nombres premiers. Un traitement ingénieux reposant sur des équations fonctionnelles canoniques lui a permis d'aboutir.

4·2. Applications en cryptologie

Systèmes à clefs publiques (RSA) :

$(p, q) \to n = pq$ facile, $n = pq \to (p, q)$ difficile.

Décryptage = méthode de factorisation. Friable = facile à factoriser.

n composé impair $\Leftrightarrow n = a^2 - b^2$.

Problème : trouver des carrés dans la suite $a^2 - n$ $(a > \sqrt{n})$.

On peut aussi chercher $a_1, \ldots, a_k$ tels que :

$$\prod_{1 \leqslant j \leqslant k} (a_j^2 - n) \in \mathbb{Z}^2$$

Ce travail est plus simple si les $a_j^2 - n$ sont friables.

On en déduit a et $b = \prod a_j$ tels que $a^2 \equiv b^2 \pmod{n}$ et $a \not\equiv \pm b \pmod{n}$.

On conclut en calculant $\operatorname{pgcd}(a - b, n)$ par l'algorithme d'Eulide.

4·3. Applications en algorithmique

Problème du logarithme discret.

- $n \in \mathbb{Z}$, $p \nmid n$, g générateur de $(\mathbb{Z}/p\mathbb{Z})^*$,

trouver ν tel que $g^\nu \equiv n \pmod p$.

- Solution *prouvée* en temps $T(p) \approx \mathrm{e}^{\sqrt{2 \ln_2 p \ln_3 p}}$.

Idée.

1. Calculer de nombreux $u_j := g^{\nu_j} \pmod p$ et garder les y-friables.
2. Déduire (algèbre linéaire) ν_q tels que $q \equiv g^{\nu_q} \pmod p$ ($\forall q$ premier $\leqslant y$).
3. Calculer $u \equiv n g^{-k} \pmod p$ pour k aléatoire.
4. Dès que $P^+(u) \leqslant y$, on a fini !

4·4. Théorie de la sommabilité : sommation friable

Fouvry-GT (1991) : posons $m(\vartheta) := \begin{cases} 0 & \text{si } \vartheta \in \mathbb{R} \smallsetminus \mathbb{Q}, \\ \Lambda(q)/\varphi(q) & \text{si } \vartheta = a/q,\ (a,q) = 1. \end{cases}$

Fonction de Mangoldt : $\Lambda(q) := \begin{cases} \ln p & \text{si } q = p^\nu, \\ 0 & \text{sinon.} \end{cases}$

Notant $\mathrm{e}(x) := \mathrm{e}^{2\pi i x}$ $(x \in \mathbb{R})$, on a

$$(2) \qquad \lim_{y\to\infty} \sum_{P(n)\leqslant y} \frac{\mathrm{e}(n\vartheta)}{n} = \log\Big(\frac{1}{1-\mathrm{e}(\vartheta)}\Big) + m(\vartheta) \qquad (\vartheta \in \mathbb{R} \smallsetminus \mathbb{Z}).$$

Définition. *On dit qu'une série* $\sum_n f(n)$ *a pour somme friable* s *si*

$$\mathfrak{S}(f) := \lim_{y\to\infty} \sum_{P(n)\leqslant y} f(n) = s.$$

Remarque. Les sommes partielles friables sont bien définies si $f(n) \ll 1/n^c$ avec $c > 0$.

La relation (2) montre que la sommation friable n'est pas un procédé régulier. Si une série $\sum_n a_n$ est sommable et si sa somme friable est égale à sa somme ordinaire, on dit qu'elle est régulière (pour la sommation friable).

Exemple.
La régularité friable de $\sum_n \mu(n)/n$ est classiquement équivalente au théorème des nombres premiers.
Ici, la convergence friable vers 0 est banale (Euler) : $\lim_{y\to\infty} \prod_{p\leqslant y}(1-1/p) = 0$.

Théorème (La Bretèche-GT, 2004). *La sommation friable des séries de Fourier conserve le théorème de Jordan en évitant le phénomène de Gibbs :*

Pour toute fonction F à variation bornée normalisée sur le tore $\mathbb{T} := \mathbb{R}/\mathbb{Z}$,

$$F_y(\vartheta) := \sum_{P^+(n)\leqslant y} c_n(F)\mathrm{e}^{2\pi i n\vartheta} \underset{y\to\infty}{\longrightarrow} F(\vartheta) \quad (\vartheta\in\mathbb{T})$$

et $\sup_\vartheta F_y(\vartheta) \to \sup_\vartheta F(\vartheta)$.

4·5. Méthode du cercle, problèmes additifs

Problèmes additifs $n = a_1 + a_2 + \cdots + a_s$, $a_j \in \mathcal{A}_j$ $(1 \leqslant j \leqslant s)$.

Goldbach (1742) $\mathcal{A}_j = \mathcal{P}$, Waring (1770) $\mathcal{A}_j := \mathbb{Z}^k$ $(k \geqslant 2)$.

Hardy–Littlewood (1920+) : $\mathcal{A}_j = \mathcal{A}$ $(1 \leqslant j \leqslant s)$, $\mathrm{e}(t) := \mathrm{e}^{2\pi i t}$,

$$R_s(n) := \int_0^1 \mathrm{e}(-n\vartheta)\Big\{\sum_{a\in\mathcal{A}} \mathrm{e}(a\vartheta)\Big\}^s \mathrm{d}\vartheta$$

Bonne factorisation des entiers friables ⇒ bonnes estimations des sommes d'exponentielles.

Exemple (Fouvry-GT 1991) :

si $3 \leqslant y \leqslant x^{1/3}$, $1 \leqslant q \leqslant \sqrt{x}$, $(a,q) = 1$, $|\vartheta - a/q| \leqslant 1/x$, on a $\sum_{n\leqslant x,\, P^+(n)\leqslant y} \mathrm{e}(n\vartheta) \ll x(\ln x)^3\{q^{-1/2} + x^{-1/12}\}$.

Pb de Waring : $G(k) := \inf\{s : \exists N : n > N \Rightarrow n = a_1^k + \ldots + a_s^k\}$

Vinogradov (1959) : $G(k) \leqslant \{2 + o(1)\}k \ln k$,

Wooley (1995) : $G(k) \leqslant \{1 + o(1)\}k \ln k$.

Vaughan (1989) : $R_7(n) \gg n^{4/3}$ pour $\mathcal{A} := \mathbb{Z}^3$.

5. Modèle de Billingsley

Billingsley (1972) : si l'on désigne par $P_1(m) > P_2(m) > \cdots > P_{\omega(m)}$ la suite décroissante des facteurs premiers de m, alors

$$\Big(\frac{\ln P_1(m)}{\ln n}, \ldots, \frac{\ln P_{\omega(m)}(m)}{\ln n}\Big),$$

considéré comme un vecteur aléatoire sur $\Omega_n := \{m : 1 \leqslant m \leqslant n\}$ muni de la probabilité uniforme ν_n, converge faiblement vers un processus réparti selon une loi de Poisson-Dirichlet (LPD) de paramètre 1.

L'une des constructions de LPD(1) est obtenue en considérant

$$X_1 = U_1, \quad X_2 := (1-U_1)U_2, \quad X_3 := (1-U_1)(1-U_2)U_3, \ldots$$

où les U_j sont des v.a.i. de loi uniforme sur $[0,1]$, de sorte que

$$\sum_{j\geqslant 1} X_j = 1 \qquad \text{ps.}$$

Le réarrangement décroissant $(X_{\sigma(1)}, X_{\sigma(2)}, \ldots)$ suit la loi $LPD(1)$.

Si $(V_1, V_2, \ldots)$ est un processus de loi LPD(1), alors

$$\mathbb{P}(V_1 > \alpha_1, \ldots, V_k > \alpha_k) = \int_{\substack{v_k < \cdots < v_1 \\ v_j > \alpha_j \ (1 \leqslant j \leqslant k)}} \varrho\Big(\frac{1 - \sum_j v_j}{v_k}\Big) \prod_{1 \leqslant j \leqslant k} \frac{\mathrm{d}v_j}{v_j}.$$

Version effective du théorème de Billingsely (GT, 2000) :

$$\nu_n\Big\{m : P_j(m) > n^{\alpha_j} \ (1 \leqslant j \leqslant k)\Big\} = \mathbb{P}\Big(V_j > \alpha_j \ (1 \leqslant j \leqslant k)\Big) + O\Big(\frac{(\ln 1/\alpha_k)^{k-2}}{\ln n}\Big)$$

uniformément pour $\alpha = (\alpha_1, \ldots, \alpha_k) \in]0, 1]^k$, $n \geqslant 2$.

[Sous certaines conditions, développement asymptotique du membre de gauche du type

$$\sum_{0 \leqslant h \leqslant H} \frac{\varphi_h(\alpha)}{(\ln n)^h} + O\Big(\frac{1}{(\alpha_k \ln n)^{H+1}}\Big).]$$

Application. Loi du k-ième plus grand facteur premier.

$$r_k(v) := 1 - \varphi_0(0, 0, \dots, 0, 1/v) = \mathbb{P}(V_k \leqslant v).$$

Pour $k \geqslant 2$ fixé,

$$r_k(v) \asymp \frac{(1+\log v)^{k-2}}{v} \ (v \geqslant 1), \qquad r_2(u) = \mathrm{e}^\gamma/u + O(1/u^2)$$

$$\nu_n\big\{P_k(m) \leqslant y\big\} = r_k(u)\Big\{1 + O\Big(\frac{1}{\log y}\Big)\Big\} \qquad \Big(2 \leqslant y \leqslant n,\ u := \frac{\log n}{\log y}\Big).$$

Pour $(\log n)^{K_H} < y \leqslant n$,

$$\nu_n\big\{P_k(m) \leqslant y\big\} = r_k(u) + \sum_{1 \leqslant j \leqslant H} \frac{r_{kj}(u)}{(\log y)^j} + O\Big(\frac{1}{(\log y)^{H+1}}\Big).$$

6. Inégalité de Turán–Kubilius friable

Notons $S(n,y) := \{m \leqslant n : P^+(m) \leqslant y\}$.

Dans la formule $K(n,y) = \sup_f \sup_{A\subset\mathbb{R}} |\nu_n(f \in A) - \mathbb{P}(Z_f \in A)|$,

nous avons : $\nu_n(f \in A) = \mu_n\big(f^{-1}(A) \cap S(n,y)\big)$ $(A \subset \mathbb{R})$

où l'on a posé $\mu_n(B) := \displaystyle\sum_{m\in B} \frac{1}{n}\Phi\Big(\frac{n}{m}, y\Big)$ $\big(B \subset S(x,y)\big)$.

Cette mesure μ_n privilégie les petites valeurs des entiers m.

Approfondir la connaissance de la structure probabiliste de Ω_n : remplacer μ_n par $\mu_{n,y}$, mesure uniforme sur $S(n,y)$.

Cela nécessite de construire, pour chaque fonction additive f un modèle probabiliste $Z_f^* := Z_{f,n,y}$ de la restriction de f à $S(n,y)$ et d'estimer

$C(n,y) := \sup_f \dfrac{V_{n,y}(f)}{\mathbb{V}(Z_f^*)}$, avec $V_{n,y}(f) := \dfrac{1}{\Psi(n,y)} \displaystyle\sum_{m\in S(n,y)} \big|f(m) - \mathbb{E}(Z_f^*)\big|^2$.

On sait que $C(n,n) = 2 + o(1)$, mais a-t-on $\sup_{n\geqslant y\geqslant 2} C(n,y) < \infty$?

Construction du modèle Z_f^*.

On a $f|_{S(n,y)} = \sum_{p\leqslant y} f_p$ et

$$\mu_{n,y}\big(f_p = f(p^\nu)\big) = \frac{\Psi(n/p^\nu, y) - \Psi(n/p^{\nu+1}, y)}{\Psi(n,y)} \approx \frac{1-p^{-\alpha}}{p^{\alpha\nu}} \quad (\alpha = \alpha(n,y))$$

d'après l'étude du comportement local de $\Psi(n,y)$ par la méthode du col.

D'où $Z_f^* := \sum_{p\leqslant y} \xi_p^*$ avec $\mathbb{P}\big(\xi_p^* = f(p^\nu)\big) = (1-p^{-\alpha})p^{-\alpha\nu}$ et $\alpha = \alpha(n,y)$.

- La Bretèche–GT (2003, 2012, 2013) :

(i) $(\forall \varepsilon > 0) \quad \sup_{n\geqslant y\geqslant (\log n)^\varepsilon} C(n,y) < \infty$.

(ii) $C(n,y) = 1 + o(1)$ si $(\log n)/y + (\log y)/\log n \to 0$.

- Martin-GT (2009) : $\sup_{n^{1/u}\leqslant y\leqslant n} C(n,y) = G(u) + o(1)$ $(n\to\infty)$, où G est une fonction explicite (calculable à partir du spectre d'un opérateur hermitien non compact) telle que $G(1) = 2$, $G(\infty) = 1$.

- Hanrot–Martin–GT (2009) : Calcul numérique et tabulation de G, qui n'*est pas* décroissante.

Applications.

Théorème de type Erdős–Wintner.

Analogue du théorème des trois séries de Kolmogorov.

Soit f une fonction additive. Supposons que n, y tendent vers l'infini de façon que $\alpha = \alpha(n,y) \to \alpha_0$.

On obtient une CS (trois séries) pour que la v.a. f sur $\big(S(n,y), \mu_{n,y}\big)$ converge en loi lorsque n et y tendent vers l'infini,

c'est-à-dire pour qu'il existe une fonction de répartition $z \mapsto D(z)$ telle que

$$\frac{1}{\Psi(n,y)} \sum_{\substack{m \in S(n,y) \\ f(m) \leqslant z}} 1 = D(z) + o(1)$$

en tout point z où D est continue.

Théorème d'Erdős–Wintner classique correspond à $\alpha = 1$. L'existence de la loi limite ne dépend alors que des $f(p)$ et pas des $f(p^\nu)$ avec $\nu \geqslant 2$.

Ici, l'existence de la loi limite dépend des $f(p^\nu)$ avec $\nu \leqslant 1/\alpha$.
On a toujours

$$\alpha(n,y) \sim \frac{\log(1+y/\log n)}{\log y},$$

donc, si par exemple, $y = (\log n)^{5/3}$ seuls les $f(p)$ et $f(p^2)$ ont une influence sur l'existence d'une loi limite.

Structure des facteurs premiers d'un entier friable.
Notons $\{p_j(m)\}_{j=1}^{\omega(n)}$ la suite croissante des facteurs premiers d'un entier m.
Erdős : $\log_2 p_j(m) \sim j$ pour presque tout m dès que $j \to \infty$.
Méthode :

$$\omega(m,t) := \sum_{p|m,\, p\leqslant t} 1$$

et inégalité classique de Turán–Kubilius.

La Bretèche-GT : Soient $b > 1$, $J_x \to \infty$.

Pour $m \in S(x,y)$ et $J_x \leqslant j \leqslant \omega(m)$,

$$\begin{cases} |\log_2 p_j(m) - j| \leqslant j^{2/3}(\log j)^{b/3} & \text{si } j \leqslant H_{x,y}, \\ \log p_j(m) = \dfrac{\log j_{x,y} + \log_2 j_{x,y} + O(1)}{1-\alpha} & \text{si } j > H^*_{x,y}, \end{cases}$$

où

$$H_{x,y} \approx \ln\Big(\frac{1}{1-\alpha}\Big) \approx \ln\Big(1 + \frac{\log y}{\log 2u}\Big).$$

Conclusion qualitative :

- les petits facteurs premiers se comportent comme ceux d'un entier « normal ».
- Les grands facteurs premiers sont « compressés ».

Par exemple, si $y \leqslant (\log n)^{1+o(1)}$, on a $p_j(m) = p_j^{1+o(1)} \quad (J_x \leqslant j \leqslant \omega(m))$, où p_j désigne le j-ème nombre premier.

7. Autres modèles probabilistes

- Forme optimale du théorème d'Erdős–Kac (1940) : Rényi & Turán (1958)

$$\nu_N\big(\omega(n) \leqslant \log_2 N + u\sqrt{\log_2 N}\big) = \int_{-\infty}^{u} \mathrm{e}^{-x^2/2}\frac{\mathrm{d}x}{\sqrt{2\pi}} + O\Big(\frac{1}{\sqrt{\log N}}\Big)$$

- Lois locales (Sathe–Selberg, 1954)

$$\nu_N\big(\omega(n) = k\big) \sim F\Big(\frac{k}{\log_2 N}\Big)\frac{(\log_2 N)^{k-1}}{(k-1)!\log N} \qquad (k \leqslant A\log_2 N)$$

Erdős : la répartition est poissonnienne dans tout intervalle assez long.

- Loi de l'arcsinus (Dress-Deshouillers-GT, 1979).

Soit D_n une v.a. telle que $\mathbb{P}(D_n = \log d) = 1/\tau(n)$ $(d|n)$, alors

$$E_N(\mathbb{P}(D_n \leqslant u)) = \frac{2}{\pi}\arcsin\sqrt{u} + O\Big(\frac{1}{\sqrt{\log N}}\Big) \qquad (0 \leqslant u \leqslant 1,\ N \to \infty)$$

mais nous avons le principe d'incertitude (GT 1980) :

$(\forall F)\quad \lim_{n\to\infty,\, n\in\mathcal{A}} \mathbb{P}(D_n \leqslant u) = F(u)$ $\mathrm{d}F$-pp $\Rightarrow \operatorname{dens}\mathcal{A} = 0$.

- Structure fractale des diviseurs (Mendès France-GT, 1994)

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

Justification heuristique :

$\ln p_j(n) \approx \mathrm{e}^j$

$$\frac{\ln d}{\ln n} = \sum_{1\leqslant j\leqslant k} \varepsilon_j \frac{\ln p_j}{\ln n} \quad (k=\omega(n),\, \varepsilon_1,\dots,\varepsilon_n)\in\{0,1\}^k,\ n \text{ sans facteur carré})$$

$$\frac{\ln d}{\ln n} \approx \sum_{1\leqslant j\leqslant k} \varepsilon_j \mathrm{e}^{j-k} \approx \sum_{h\geqslant 0} \varepsilon'_h \mathrm{e}^{-h}$$

donc $\{(\ln d)/\ln n : d|n\} \approx$ un ensemble de Cantor de dimension $\ln 2$.

- Limites du modèle :

Le modèle fractal prévoit que $E(n) := \min_j d_{j+1}(n)/d_j(n) > 1 + c$ pour une suite de densité positive.

Or (Erdős–Hall 1979, Maier-GT 1984) :

$$E(n) = 1 + 1/(\ln n)^{\ln 3 - 1 + o(1)} \text{ pp.}$$

Galambos (1976) :

$\ln_2 p_{j+1}(n) - \ln_2 p_j(n)$ sont asymptotiquement répartis comme des v.a.i. de même loi : $\mathbb{P}(X \leqslant z) = 1 - \mathrm{e}^{-z}$ $(z > 0)$.

Modèle plus précis :

$$\frac{\ln d}{\ln n} \approx \sum_{j \geqslant 1} \varepsilon_j X_1 \cdots X_j$$ où toutes les variables sont indépendantes.

Mais cela n'est pas en accord avec le modèle de Billingsley : cette modélisation ne fonctionne pas pour les grands diviseurs.

- Un problème ouvert (Erdős–Hooley) :

Concentration des diviseurs

$\Delta(n) := \sup_u \big|\{d : d|n,\, \mathrm{e}^u \leqslant d \leqslant \mathrm{e}^{u+1}\}\big|$.

On sait (Maier-GT 1985-2009) que

$$(\ln_2 n)^{c_1+o(1)} < \Delta(n) < (\ln_2 n)^{c_2+o(1)} \text{ pp}$$

avec $c_1 := (\ln 2)/\ln\left(\frac{1-1/\ln 27}{1-1/\ln 3}\right) \approx 0.33827$, $c_2 = \ln 2 \approx 0,69315$.

$$\Delta(n) = (\ln_2 n)^{c+o1)} \quad \text{pp ?}$$

Modèle probabiliste pour prévoir la valeur de c ?