Lycée Bascan de Rambouillet
Introduction à l'exposé de Gérald Tenenbaum
Paul Erdös et l'anatomie des nombres entiers à la BNF,
conférences *Un texte, un mathématicien.*
22 février 2017.

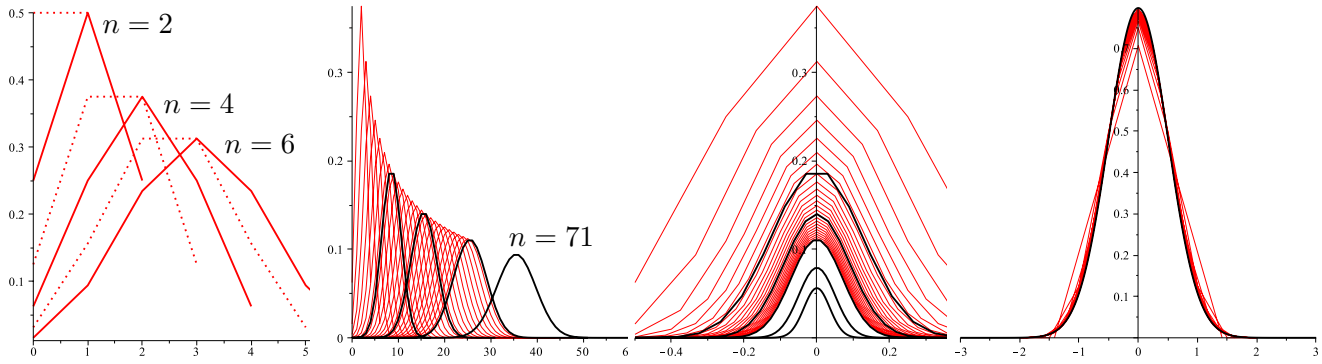
Quelques histoires de nombres, notes d'exposé

1 Résumé

Les nombres sont-ils répartis au hasard ?
D'un côté, pile ou face. Lorsque l'on y joue (très longtemps), on tombe nez à nez avec la célèbre courbe en cloche de F. Gauss, qui est le phare des phénomènes aléatoires. D'un autre côté, les fidèles nombres entiers 1, 2, 3, etc – qui nous sont si familiers – ne semblent rien devoir au hasard.
Et pourtant...
Prenez un nombre au hasard et regardez comment il se décompose en produit de nombres premiers (2, 3, 5, 7, 11 etc). Si l'on regarde attentivement, on peut voir surgir de cette question :
- le nombre pi (mais qu'est-ce que les cercles ont à voir avec les nombres entiers ?)
- une fonction qui croît tellement lentement vers l'infini qu'on la croirait constante
- ou encore, qui l'eût cru, la courbe de Gauss.
Comme si les nombres étaient eux-mêmes fabriqués... au hasard.

2 Pile ou face et Gauss

Pile ou face, gain 0 ou 1. Modèle : jets indépendants et équidistribués $\left(\frac{1}{2}, \frac{1}{2}\right)$. On note S_n la somme des gains après n jets.
Distribution des gains après 1, 2, 3, 4,... jets (triangle de Pascal). Dessins.



$\{(k, \mathbf{Proba}(S_n = k))\}$ $\{(k, \mathbf{Proba}(S_n = k))\}$ $\left\{\left(\frac{k}{n} - \frac{1}{2}, \mathbf{Proba}(S_n = k)\right)\right\}$ $\left\{\left(\frac{k-\frac{n}{2}}{\sqrt{n}}, \sqrt{n}\,\mathbf{Proba}(S_n = k)\right)\right\}$

Le diagramme des probabilités des gains, une fois renormalisé, converge vers une courbe en forme de cloche, qui et ici le graphe (en noir) de la fonction $x \mapsto \sqrt{\frac{2}{\pi}} e^{-2x^2}$ (pour les élèves de terminale). C'est la célèbre courbe de Gauss[1].

[1] Carl Friedrich Gauss, 1777 – 1855

En bref, théorème de la limite centrale, modélisation du hasard, loi binomiale (échec/succès d'expériences répétées), place de l'indépendance stochastique.

3 Nombres premiers et décomposition des nombres entiers

Tout nombre entier naturel se décompose en un produit de nombres (plus petits). Les briques élémentaires de cette décomposition sont les *nombres premiers*. Le début de la liste :

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, \ \textit{etc.}$$

Exemples : $588 = 2^2 \times 3 \times 7^2$, $403 = 13 \times 31$, $139968 = 2^6 \times 3^7$, $25283 = 131 \times 193$. Reconnaître un nombre premier, crible d'Eratosthène[2], difficulté algorithmique, cryptographie RSA (en bref).

Deux entiers naturels sont *premiers entre eux* lorsque 1 est leur unique diviseur commun. Exemples : 588 et 139968 ne sont pas premiers entre eux, 588 et 25283 le sont. Division euclidienne, algorithme d'Euclide[3] pour savoir si deux nombres sont premiers entre eux, simplicité algorithmique.

4 Tirer deux nombres au hasard

Quel sens mathématique donner à l'idée: *prendre un nombre entier naturel au hasard* ? Exigence de l'uniformité. Le choix : on tire uniformément dans $\{1, \ldots, n\}$ et on fait tendre n vers l'infini. Par exemple, la probabilité de tirer un nombre pair est $1/2$, de tirer un multiple de d est $1/d$.

On tire indépendamment *deux* entiers naturels au hasard (par exemple, la probabilité que l'un soit pair et l'autre multiple de 5 est $1/10$). La question :

quelle est la probabilité que ces deux nombres soient premiers entre eux ?

Le calcul : on prend un couple de nombres dans $\{1, \ldots, n\}^2$. Le nombre de ces couples : n^2.
Pour trouver les couples premiers entre eux, on enlève les couples de nombres pairs, de multiples de 3, de multiples de 5 etc. Le nombre de ces couples : $\left\lfloor \frac{n}{2} \right\rfloor^2 + \left\lfloor \frac{n}{3} \right\rfloor^2 + \cdots$.
On en a enlevé trop : il faut ajouter les couples de multiples de 2×3, de 2×5, de 3×5, etc.
Un résumé sans parole du raisonnement, la notation $\lfloor x \rfloor$ désignant la partie entière du réel x :

$$n^2 - \left(\left\lfloor \frac{n}{2} \right\rfloor^2 + \left\lfloor \frac{n}{3} \right\rfloor^2 + \cdots \right) + \left(\left\lfloor \frac{n}{2 \times 3} \right\rfloor^2 + \left\lfloor \frac{n}{2 \times 5} \right\rfloor^2 + \cdots \right) - \left(\left\lfloor \frac{n}{2 \times 3 \times 5} \right\rfloor^2 + \left\lfloor \frac{n}{2 \times 3 \times 7} \right\rfloor^2 + \cdots \right) + \cdots$$

$$\approx n^2 \left(1 - \left(\frac{1}{2^2} + \frac{1}{3^2} + \cdots \right) + \left(\frac{1}{2^2 \times 3^2} + \frac{1}{2^2 \times 5^2} + \cdots \right) - \left(\frac{1}{2^2 \times 3^2 \times 5^2} \right) + \cdots \right)$$

$$\approx n^2 \left(1 - \frac{1}{2^2} \right) \left(1 - \frac{1}{3^2} \right) \left(1 - \frac{1}{5^2} \right) \left(1 - \frac{1}{7^2} \right) \left(1 - \frac{1}{11^2} \right) \cdots$$

L'approximation est légitime lorsque n tend vers l'infini. Au bout du compte, la probabilité que deux nombres entiers pris au hasard soient premiers entre eux s'écrit comme le produit (infini !)

$$P_{\text{premiers entre eux}} = \left(1 - \frac{1}{2^2} \right) \left(1 - \frac{1}{3^2} \right) \left(1 - \frac{1}{5^2} \right) \left(1 - \frac{1}{7^2} \right) \left(1 - \frac{1}{11^2} \right) \cdots \tag{1}$$

[2] *Ερατοσθένης*, -276 – -194.
[3] *Εὐκλειδης*, *ca.* -300

Petite digression sur les sommes infinies
Exemple des sommes géométriques : si $|x|<1$, alors $\frac{1}{1-x}=1+x+x^2+x^3+\dots$, la somme infinie a le sens d'une limite.
La série harmonique $1+\frac{1}{2}+\frac{1}{3}+\frac{1}{4}+\cdots$ diverge (limite infinie, preuve *via* $\frac{1}{3}+\frac{1}{4}>\frac{1}{2}$, $\frac{1}{5}+\frac{1}{6}+\frac{1}{7}+\frac{1}{8}>\frac{1}{2},\dots$).
Sommer les $\frac{1}{n(n-1)}=\frac{1}{n-1}-\frac{1}{n}$, télescopage, $\frac{1}{1\times 2}+\frac{1}{2\times 3}+\frac{1}{3\times 4}+\cdots=1$.
Sommer les $\frac{1}{n^2}\leq\frac{1}{n(n-1)}$, suite des sommes partielles croissante et majorée, $1+\frac{1}{2^2}+\frac{1}{3^2}+\frac{1}{4^2}+\cdots$ définit bien un nombre. *Idem* si on somme les $1/m^2$ pour les m dans un sous-ensemble de $\mathbb{N}^*$.

On reconsidère la formule (1) sous l'éclairage des sommes géométriques :
$1-\frac{1}{2^2}=1+\frac{1}{2^2}+\frac{1}{2^4}+\frac{1}{2^6}+\frac{1}{2^8}+\cdots$, *idem* avec $3,5,7,11\dots$. On obtient

$$P_{\text{premiers entre eux}}=\left(\frac{1}{1+\frac{1}{2^2}+\frac{1}{2^4}+\cdots}\right)\left(\frac{1}{1+\frac{1}{3^2}+\frac{1}{3^4}+\cdots}\right)\left(\frac{1}{1+\frac{1}{5^2}+\frac{1}{5^4}+\cdots}\right)\cdots$$

$$=\frac{1}{\left(1+\frac{1}{2^2}+\frac{1}{3^2}+\frac{1}{4^2}+\frac{1}{5^2}+\frac{1}{6^2}+\cdots+\frac{1}{30^2}+\frac{1}{31^2}+\cdots\right)}.$$

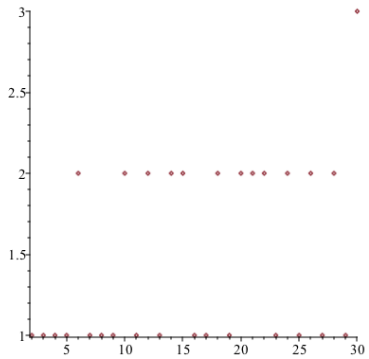
Pour finir,

$$P_{\text{premiers entre eux}}=\frac{6}{\pi^2}.$$

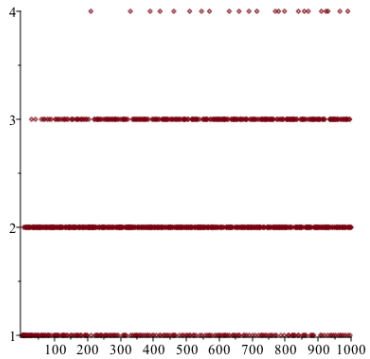
Dernière égalité par constatation numérique (pour $n=10^{16}$, 15 décimales exactes). Preuve rigoureuse de tout ce raisonnement accessible en licence de mathématiques.

5 Combien de facteurs premiers ?

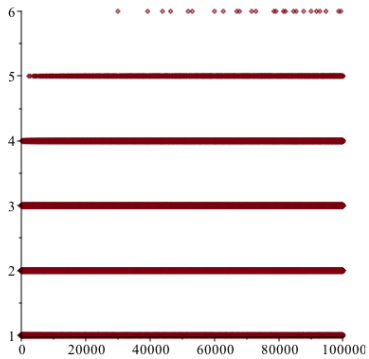
On note $\omega(n)$ le nombre de diviseurs premiers (distincts) de l'entier n.
Les premières valeurs : $\omega(2)=1,\ \omega(3)=1,\ \omega(4)=1,\ \omega(5)=1,\ \omega(6)=2,\omega(7)=1,\dots$
Quelques dessins de la fonction omega :



$\omega(n), 2\leq n\leq 30$

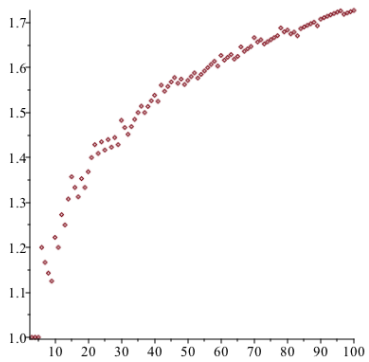


$\omega(n), 2\leq n\leq 1000$

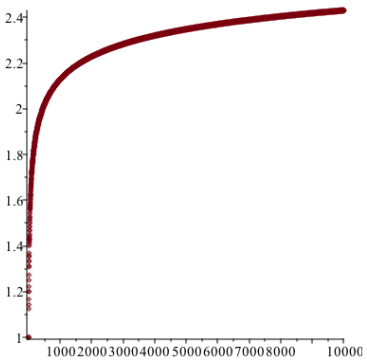


$\omega(n), 2\leq n\leq 10^5$

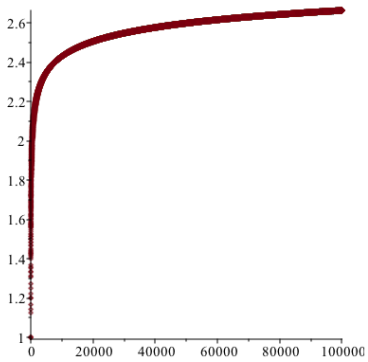
Cette fonction est très irrégulière. On dessine, pour chaque entier n, la moyenne $\overline{\omega}(n)$ de $\omega(2),\omega(3),\dots,\omega(n)$.
Le dessin :



$\overline{\omega}(n), 2 \leq n \leq 100$



$\overline{\omega}(n), 2 \leq n \leq 10000$

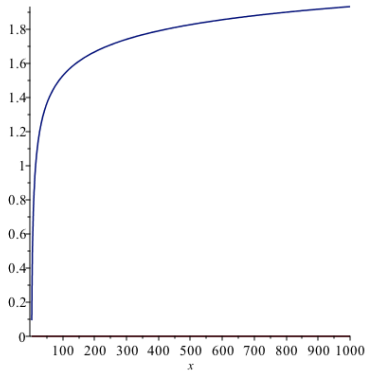


$\overline{\omega}(n), 2 \leq n \leq 10^5$

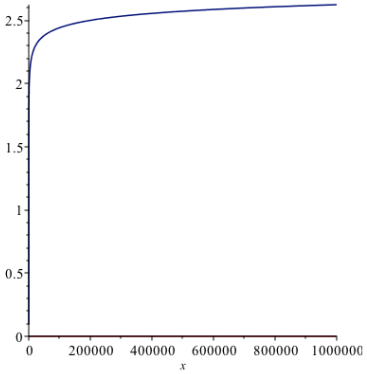
On montre, aujourd'hui avec les moyens d'une licence de mathématiques, que

$$\overline{\omega}(n) \sim \ln \ln n$$

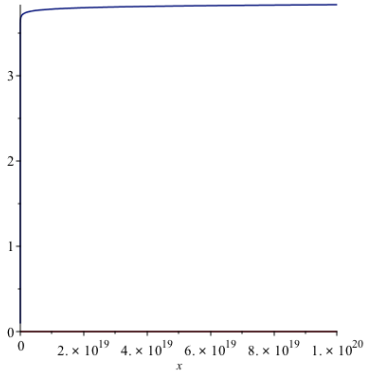
lorsque n tend vers l'infini (pour les élèves qui ne connaissent pas encore le logarithme, expliquer ce qu'il est). Ce résultat est un théorème de Hardy et Ramanujan[4], démontré en 1917. Le dessin de la fonction $x \mapsto \ln \ln x$:



$\ln \ln x,\ x \leq 10^3$



$\ln \ln x,\ x \leq 10^6$



$\ln \ln x,\ x \leq 10^{20}$

Malgré la lenteur de sa croissance, cette fonction tend vers l'infini en $+\infty$!

Rappelons-nous pile ou face. Au gain de n jets, on a enlevé sa moyenne. En divisant par la racine carrée de cette moyenne, on obtient un nombre aléatoire dont la distribution prend, très lentement lorsque n grandit, la forme d'une courbe de Gauss. Il en va de même pour le nombre de facteurs premiers des nombres entiers. Dans le jargon, on dit que la distribution des

$$\frac{\omega(k) - \ln \ln n}{\sqrt{\ln \ln n}}, 2 \leq k \leq n$$

tend vers une loi *gaussienne* (ou *normale*) centrée et réduite. Ce théorème difficile a été démontré par Erdös et Kac[5] en 1939.

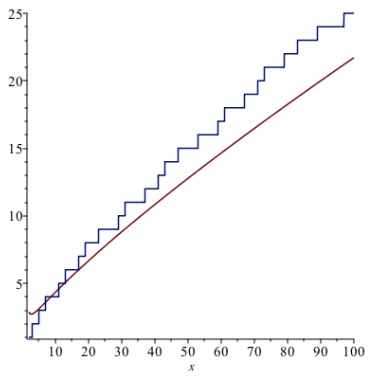
[Doit-on pour autant en déduire que le nombre des facteurs premiers distincts des nombres entiers est tiré "au hasard" ???]

[4] Geoffrey Harold Hardy, 1877 – 1947 ; Srinivasa Ramanujan, 1887 – 1920.
[5] Paul Erdös, 1913 – 1996 ; Mark Kac, 1914 – 1984

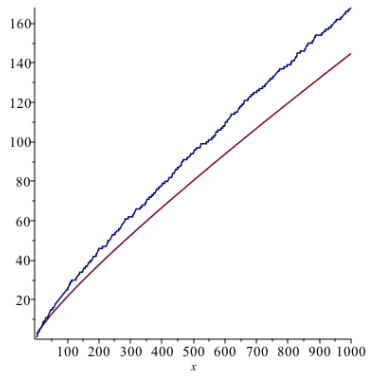
6 Combien de nombres premiers ?

L'ensemble des nombres premiers est infini (preuve d'Euclide). Mais un réel strictement positif x étant donné, quel est le nombre de nombres premiers compris entre 1 et x ? On note ce nombre $\pi(x)$.

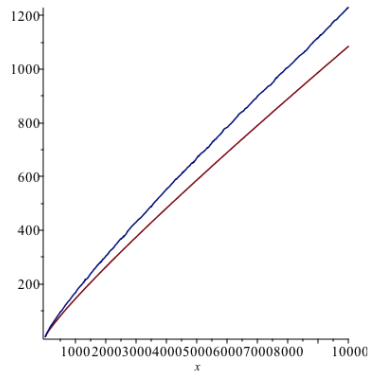
En 1896, Hadamard et de la Vallée-Poussin[6] démontrent indépendamment le difficile *théorème des nombres premiers* : $\pi(x) \sim \frac{x}{\ln x}$ lorsque x tend vers $+\infty$, ce qui signifie que $\lim_{+\infty} \frac{\pi(x)\ln x}{x} = 1$. Ce théorème n'est guère accessible avant quatre ou cinq années d'études supérieures en mathématiques, malgré des simplifications de la preuve originale.
Les dessins de la fonction π couplée avec la fonction $x \mapsto \frac{x}{\ln x}$, puis de la fonction $x \mapsto \pi(x)/\frac{x}{\ln x}$:



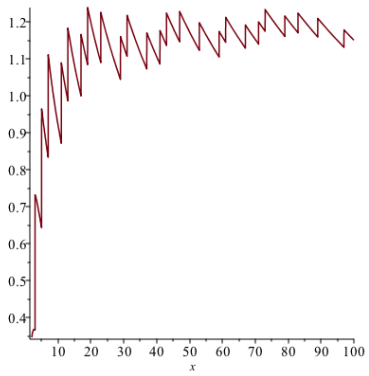
$\pi(x)$ et $\frac{x}{\ln x}$, $x \leq 100$



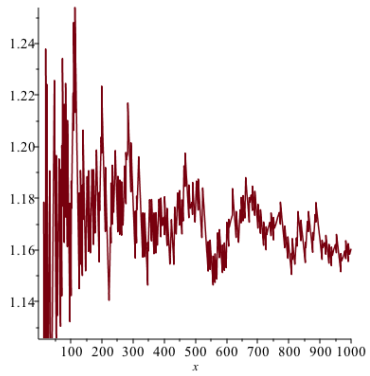
$\pi(x)$ et $\frac{x}{\ln x}$, $x \leq 1000$



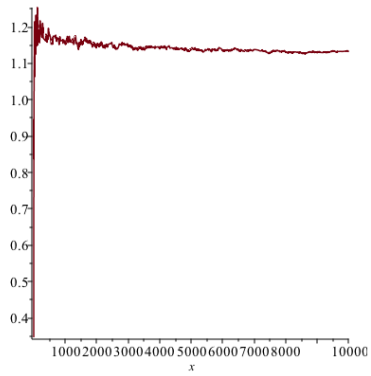
$\pi(x)$ et $\frac{x}{\ln x}$, $x \leq 10000$



$\pi(x)/\frac{x}{\ln x}$, $x \leq 100$



$\pi(x)/\frac{x}{\ln x}$, $x \leq 1000$



$\pi(x)/\frac{x}{\ln x}$, $x \leq 10000$

La convergence vers 1 de $\pi(x)/\frac{x}{\ln x}$ est (encore) lente. En 1859, Riemann[7] conjecture (sous une forme différente, mais équivalente) que

$$\forall \alpha > \frac{1}{2}, \quad \lim_{x \to +\infty} \frac{\left|\pi(x) - \frac{x}{\ln x}\right|}{x^\alpha} = 0. \tag{2}$$

C'est ce qu'on appelle *l'hypothèse de Riemann*, qui n'est aujourd'hui toujours pas démontrée ni infirmée et qui reste sans doute le plus grand défi pour les mathématiciens du monde entier.

[6] Jacques Hadamard , 1865 – 1963 ; Charles-Jean de la Vallée-Poussin, 1866 – 1962.
[7] Bernhard Riemann, 1826 – 1866.