Allons compter les résidus !

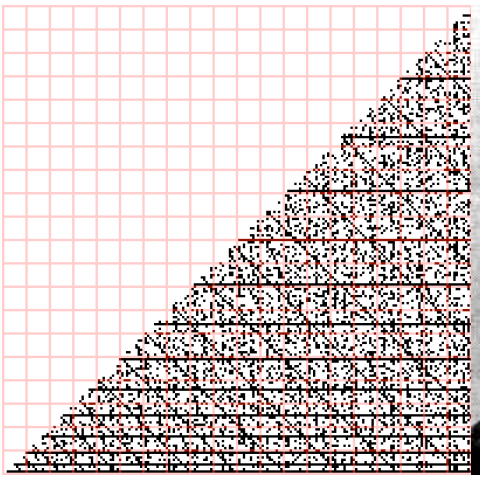
Cyril Banderier

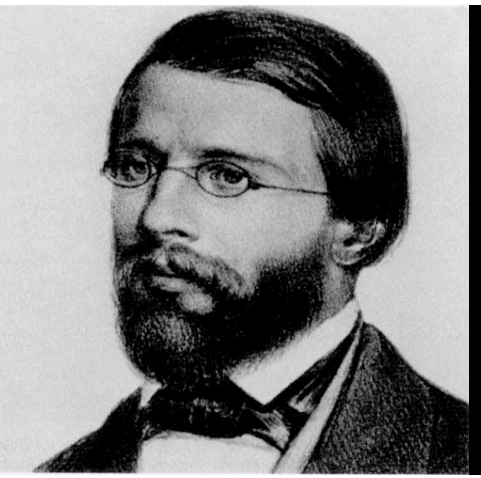
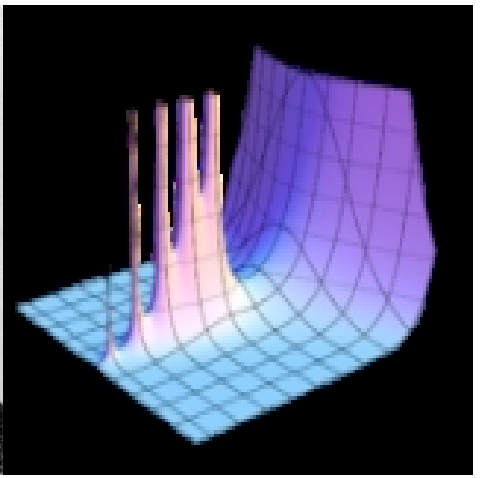
Laboratoire d'Informatique de Paris Nord.
équipe CALIN: Combinatoire, algorithmique et interactions

http://lipn.fr/~banderier

Travaux en commun avec

Haja Andriamanalintsoa (Antananarivo),
Apostol Vourdas (Bradford).



Quelques fonctions multiplicatives...

Leonard Euler (1707-1783)

$f(n.m) = f(n).f(m)$ pour n et m premiers entre eux

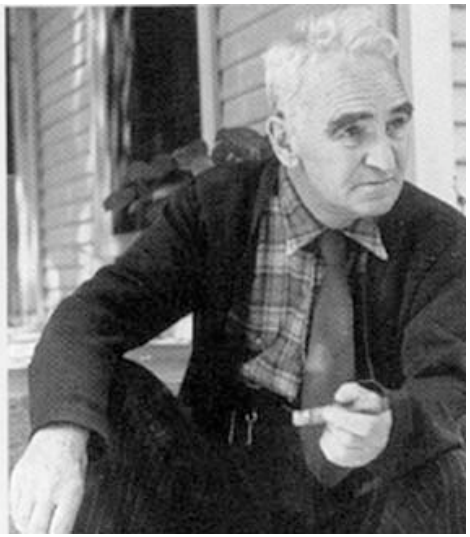
- $Id_k(n) = n^k$
- $\epsilon(1) = 1$ et $\epsilon(n) = 0$ pour $n > 1$
- $\gcd(n, k)$

- le symbole de Legendre: $\left(\frac{n}{p}\right) = 1$ si n est un carré mod p, -1 sinon (et 0 si $p|n$).
- les caractères de Dirichlet $\chi_d(n) = \omega_n$ (où $\omega_n^{\phi(d)} = 1$)
- l'indicatrice d'Euler $\phi(n) = \#(\mathbb{Z}/n\mathbb{Z})^*$
- la fonction de Möbius $\mu(n) = \begin{cases} 1 & \text{si} \quad n = 1 \\ (-1)^r & \text{si} \quad n = p_1 \cdots p_r \\ 0 & \text{sinon} \end{cases}$
- la somme des diviseurs $\sigma_k(n) = \sum_{d|n} d^k$
- les fonctions de Liouville $\lambda(n) = a^{\Omega(n)}$ où $\Omega(n)$ est le nombre de facteurs premiers de n (avec ou sans leur multiplicité)
- fonction ψ de Dedekind $\psi(n) = n \prod_{p|n}(1 + 1/p)$
- fonction de Jordan $J_k(n) = n^k \prod_{p|n}(1 - p^{-k})$, en particulier: $J_1 = \phi, J_2(n) = \phi(n)\psi(n)$
- ...

Johann Heinrich Lambert (1728-1777)

$$F(z) := \sum_{n \geq 0} f(n) \frac{z^n}{1 - z^n}$$

plein de formules... (liens avec fonctions elliptiques de Jacobi...)



Eric Temple Bell (1883-1960)

$$F(z) := \sum_{n \geq 0} f(p^n) z^n$$

plein de formules... (souvent fractions rationnelles)

Bernhard Riemann
(1826-1866)

$$L(s,f) = \sum_{n\geq 1} f(n) n^{-s}$$

Produit de convolution :

$$L(s,f).L(s,g) = \sum_{n\geq 1} \left(\sum_{d|n} f(d) g(n/d) \right) n^{-s} = L(s, f*g)$$

Formule du produit d'Euler :

$$L(s,f) = \prod_{p\in\mathcal{P}} \sum_{i=0}^{\infty} \frac{f(p^i)}{p^{is}} = \prod_{p\in\mathcal{P}} \frac{1}{1-f(p)p^{-s}}$$

Quelques formules explicites:

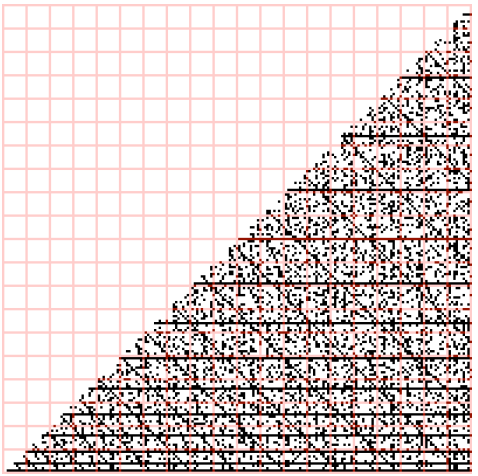
$$L(s,\epsilon) = 1, \qquad L(s,1) = \sum_{n\geq 1} \frac{1}{n^s} = \zeta(s), \qquad L(s, Id_k) = \sum_{n\geq 1} \frac{n^k}{n^s} = \zeta(s-k)$$

$$L(s,\mu) = \frac{1}{\zeta(s)} \qquad \text{car } L(s,\epsilon) = L(s,\mu)L(s,1)$$

$$L(s,\sigma_k) = L(s, Id^k)L(s,1) = \zeta(s-k)\zeta(s), \qquad L(s,J_k) = \frac{\zeta(s-k)}{\zeta(s)}$$

$$L(s,|\mu|) = \frac{\zeta(s)}{\zeta(2s)}, \qquad L(s,\delta) = L(s,|\mu|)L(s,1) = \frac{\zeta(s)^2}{\zeta(2s)}, \qquad L(s,\lambda) = \frac{\zeta(2s)}{\zeta(s)}$$

Résidus modulo n



x est résidu k-ième $\iff x \equiv y^k \mod n$.

$k = 2, 3, 4, 5 \cdots$: résidus quadratiques, cubiques, quartiques ou biquadratiques, quintiques...

Exemple dans $\mathbb{Z}_{10} = \mathbb{Z}/10\mathbb{Z}$:

x	1	2	3	4	5	6	7	8	9	10
x^2	1	4	9	6	5	6	9	4	1	0
x^3	1	8	7	4	5	6	3	2	9	0
x^4	1	6	1	6	5	6	1	6	1	0

Les résidus k-ième dans $\mathbb{Z}_{10}$ sont ainsi:

- pour $k = 2$: 0, 1, 4, 5, 6, 9
- pour $k = 3$: 0, 1, 2, 3, 4, 5, 6, 7, 8, 9
- pour $k = 4$: 0, 1, 5, 6

$\rho_k(n) :=$ nombre de résidus k-ièmes dans $\mathbb{Z}/n\mathbb{Z}$.
$\rho_2(10) = 6, \rho_3(10) = 10, \rho_4(10) = 4$

Coût du calcul de $\rho_k(n)$: $\dfrac{n \ln(k)}{2 \ln 2}$ opérations. Peut-on faire mieux ?

Théorème

ρ_k est une fonction multiplicative: $\rho_k(nm) = \rho_k(n)\rho_k(m)$ (pour n et m premiers entre eux).

Sketch of proof.

On construit une bijection entre $(\mathbb{Z}_{nm})^k$ et $(\mathbb{Z}_n)^k \times (\mathbb{Z}_m)^k$.

$$Card((\mathbb{Z}_{nm})^k) = Card((\mathbb{Z}_n)^k).Card((\mathbb{Z}_m)^k)$$

$$\rho_k(nm) = \rho_k(n)\rho_k(m)$$

Injectivité, surjectivité... key tool = lemme chinois :
Pour n et m premiers entre eux (donc $un + vm = 1$ d'après l'identité de Bézout)

$$\left.\begin{array}{ll} x = a & \mod n \\ x = b & \mod m \end{array}\right\} \Longleftrightarrow x = (aun + bvm) \mod nm$$

□

Théorème

$\rho_P(n) := \#\{x_i \in \mathbb{Z}_n : P(x_1, \ldots, x_k) = 0 \mod n\}$ est une fonction multiplicative.

(Caveat $\rho_{x_1^2+x_2^2-x_3}(n) \neq r_2(n) =$ nb de représentations de n comme sommes de deux carrés).

Théorème

$$\rho_k(2^n) = \begin{cases} 1 & si \quad n = 0 \\ 2 & si \quad n = 1 \\ 1 + \dfrac{\phi(2^n)}{gcd(k,2)gcd(k,2^{n-2})} & si \quad 2 \leq n < k \\ \rho_k(2^{n-k}) + \dfrac{\phi(2^n)}{gcd(k,2)gcd(k,2^{n-2})} & si \quad n \geq k \end{cases}$$

Théorème

Pour p premier impair,

$$\rho_k(p^n) = \begin{cases} 1 & si \quad n = 0 \\ 1 + \dfrac{\phi(p^n)}{gcd(k,\phi(p^n))} & si \quad 1 \leq n < k \\ \rho_k(p^{n-k}) + \dfrac{\phi(p^n)}{gcd(k,\phi(p^n))} & si \quad n \geq k \end{cases}$$

Théorème

Le nombre des résidus quadratiques dans $\mathbb{Z}_{2^n}$ est

$$\rho_2(2^n) = \frac{3}{2} + \frac{1}{6}2^n + \frac{(-1)^{(n+1)}}{6} \qquad \text{pour } n \geq 1$$

Théorème

Le nombre des résidus quadratiques dans $\mathbb{Z}_{p^n}$ est

$$\rho_2(p^n) = \frac{3}{4} + \frac{(p-1)(-1)^{(n+1)}}{4(p+1)} + \frac{p^{n+1}}{(2p+2)}$$

Théorème

Si $k > p$, on a:

$$\rho_k(p^n) = \begin{cases} 1 + \dfrac{(p-1)p^{n-1}(1-p^{-n})}{1-p^{-k}} & \text{si} \quad n = 0 \bmod k \\ 1 + \dfrac{(p-1)p^{n-1}\left(1-p^{-k([n/k]+1)}\right)}{1-p^{-k}} & \text{sinon} \end{cases}$$

Théorème

Si $k = p$, on a:

$$\rho_k(p^n) = \begin{cases} 1 + \dfrac{(p-1)p^{n-2}(1-p^{-n})}{1-p^{-k}} & \text{si} \quad n = 0 \bmod k \\ p + \dfrac{(p-1)p^{n-2}(1-p^{-k[n/k]})}{1-p^{-k}} & \text{si} \quad n = 1 \bmod k \\ 1 + \dfrac{(p-1)p^{n-2}(1-p^{-k([n/k]+1)})}{1-p^{-k}} & \text{sinon} \end{cases}$$

Théorème

Si $k < p$ et k est divisible par $p-1$, on a :

$$\rho_k(p^n) = \begin{cases} 1 + \dfrac{(p-1)p^{n-1}(1-p^{-n})}{k(1-p^{-k})} & \text{si} \quad n = 0 \bmod k \\ 1 + \dfrac{(p-1)p^{n-1}\left(1-p^{-k([n/k]+1)}\right)}{k(1-p^{-k})} & \text{sinon} \end{cases}$$

Théorème

Si $k < p$ et k n'est pas divisible par $p-1$, on a :

$$\rho_k(p^n) = \begin{cases} 1 + \dfrac{(p-1)p^{n-1}(1-p^{-n})}{1-p^{-k}} & \text{si} \quad n = 0 \bmod k \\ 1 + \dfrac{(p-1)p^{n-1}\left(1-p^{-k([n/k]+1)}\right)}{1-p^{-k}} & \text{sinon} \end{cases}$$

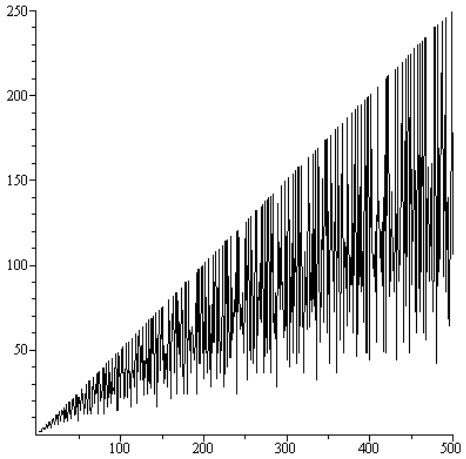
Théorème

$$\rho_k(2^n) = \begin{cases} 1 + \dfrac{2^{n-1}(1-2^{-n})}{1-2^{-k}} & \text{si} \quad n = 0 \bmod k \\ 1 + \dfrac{2^{n-1}\left(1-2^{-k([n/k]+1)}\right)}{1-2^{-k}} & \text{sinon} \end{cases}$$

Quid de l'asymptotique ?

Ernesto Cesàro (1859-1906)

Si a_n a un comportement chaotique,
on peut regarder $\sum_{k=1}^{n} a_k$.
En un sens, $\frac{\sum_{k=1}^{n} a_k}{n}$ donnera
le comportement "moyen" de a_n.

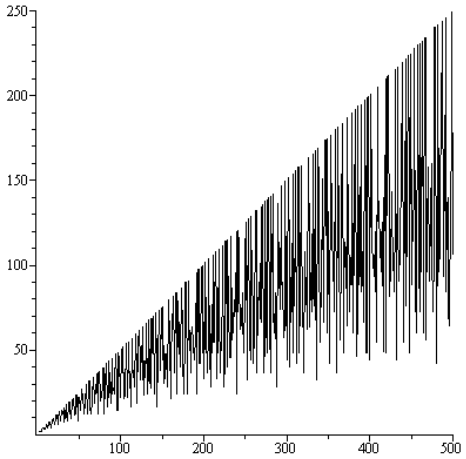


$\rho_2(n)$

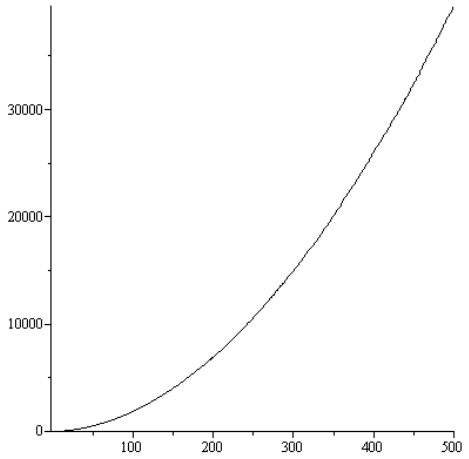
Quid de l'asymptotique ?

Ernesto Cesàro (1859-1906)

Si a_n a un comportement chaotique,
on peut regarder $\sum_{k=1}^{n} a_k$.
En un sens, $\frac{\sum_{k=1}^{n} a_k}{n}$ donnera
le comportement "moyen" de a_n.



$\rho_2(n)$

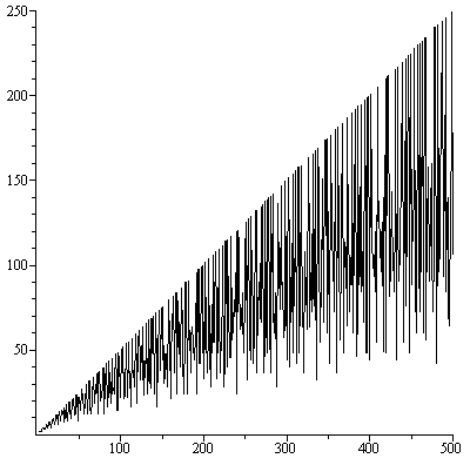


$\sum_{k=1}^{n} \rho_2(k)$

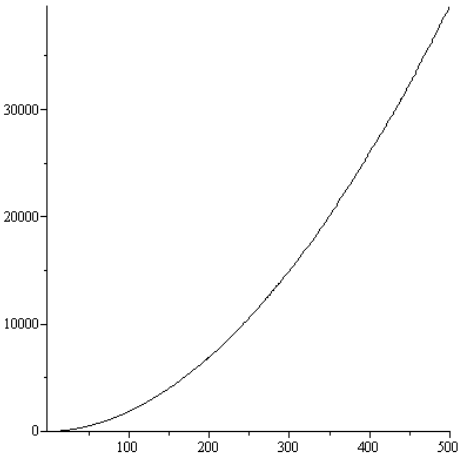
Quid de l'asymptotique ?

Ernesto Cesàro (1859-1906)

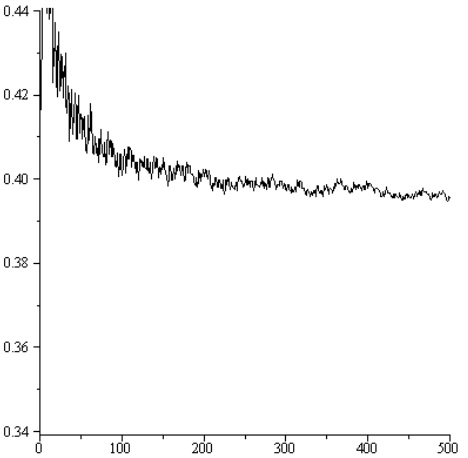
Si a_n a un comportement chaotique,
on peut regarder $\sum_{k=1}^{n} a_k$.
En un sens, $\frac{\sum_{k=1}^{n} a_k}{n}$ donnera
le comportement "moyen" de a_n.



$\rho_2(n)$



$\sum_{k=1}^{n} \rho_2(k)$



$(\sum_{k=1}^{n} \rho_2(k))/(n^2/\sqrt{\ln(n)})$

Hubert Delange (1913-2003)
a donné un moyen d'obtenir l'asymptotique de sommes de Cesàro.

Théorème (théorème taubérien de Wiener–Ikehara–Delange (1930,31,54,63):)

Soit $F(s)$ une série de Dirichlet à coefficients $a_n > 0$ convergeant pour $\Re(s) > \sigma > 0$. Si $F(s) = \dfrac{A(s)}{(s-\sigma)^{\gamma+1}} + B(s)$ (avec F analytique pour $\Re(s) = \sigma, s \neq \sigma$), alors

$$\sum_{n \leq N} a_n = \frac{A(\sigma)}{\sigma \Gamma(\gamma+1)} N^\sigma \ln^\gamma N \, (1 + o(1)).$$

NB: cohérent avec $\zeta(s)$.

Gustav Lejeune Dirichlet
(1805-1859)

On prouve ici la conjecture de
[Finch & Sebah 2006] sur l'asymptotique des cubes.
NB: ils donnent aussi un schéma numérique
pour calculer les produits infinis.

$$F(s) = \zeta(s)\left(1 + \frac{2^{2s+1} - 2^{s+1} - 1}{2^{s+2}(2^{2s+1} - 2^{s-1} - 1)}\right)\prod_p \left(1 - \frac{(p^{s+1}+2)(p-1)}{2(p^{s+1}+1)(p^{s+1}-1)}\right) = G(s)\cdot\zeta(s)^{1/2}$$

$$\sum_{n\le N} b(n) \sim C_2 \cdot N^2 \cdot (\ln N)^{-1/2} = (0.376\ldots)N^2 \cdot (\ln N)^{-1/2}.$$

$$C_2 \quad = \quad \frac{17}{32}\frac{1}{\sqrt{\pi}}\prod_p \left(1 - \frac{p^2+2}{2(p^2+1)(p+1)}\right)\left(1 - \frac{1}{p}\right)^{-1/2}$$

Théorème

$$\sum_{n\ge 1}\frac{\rho_k(n)}{n^{s+1}} = G_k(s)\zeta(s)^{k/(k-1)} \qquad \sum_{n=1}^{N}\rho_k(n) \sim \frac{G_k(1)}{\Gamma((k-1)/k)}\frac{N^2}{2}\ln N^{-1/k}$$

Gauss (1777-1855)

Algorithme de
Fermat–Gauss–Kraïtchik (–Lehmer–Powers–Morrison–Brillhart):

$x^2 = y^2 \mod n$
$\iff x^2 - y^2 = 0 \mod n$
$\iff (x-y)(x+y) = 0 \mod n$
et donc si $x \neq \pm y \mod n$,
alors $gcd(x+y, n)$ sera un diviseur de n.

Généralisation :

$x^k = y^k \mod n \iff (x-y)(\sum_{k=0}^{n} x^k y^{n-k}) = 0 \mod n$

On doit trouver des m-uplets tels que $x^k = x_1 \dots x_m \equiv y_1 \dots y_j = y^k \mod n$
$\rightarrow$ algèbre linéaire ! On peut se limiter à des nombres friables (produit de petits premiers $\leq p$),

(open problem : quel p prendre? Davenport Pomerance & al., Alon & al.)

Combien d'éléments de $\mathbb{Z}_n$ ne sont pas des puissances ? $:= \rho_0(n)$

Inclusion-exclusion : $\rho_0(n) = n - \rho_2(n) - \rho_3(n) - \cdots + \rho_6(n) \ldots ...$
non trivial,... ce n'est pas une fonction multiplicative.

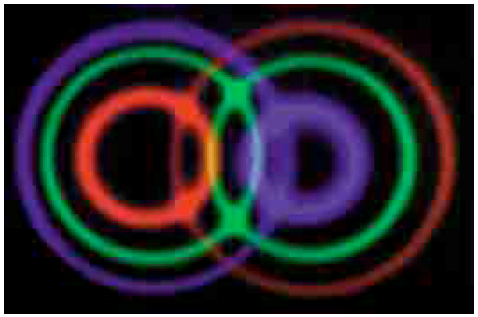
Théorème

Si n est sans facteur carré, alors $\rho_0(n) = 0$.
Pour tout n, $\rho_0(n) \leq n - \phi(n) - 1$.

(work in progress with Haja Andriamanalintsoa).

Camille Jordan (1838-1922)

Théorème :
Taille du groupe symplectique (det $M = 1 \mod n$) :
$\#Sp(2, \mathbb{Z}_n) = nJ_2(n)$
preuve via : $\#Sp(2, \mathbb{Z}_{p^e}) = p^{2e}\phi(p^e)(1 + 1/p)$
(in Jordan, Œuvres complètes?)



Optique quantique, oscillateur anharmonique,
fonctions de Weyl, de Wigner... $\Longrightarrow$ Apostol Vourdas ;-)
Théorème: pour réailiser cette tomographique quantique,
il suffit en moyenne de $\sim \dfrac{n^2}{3\zeta(3)}$ " lignes".
Preuve via moyenne de Cesàro : $\displaystyle\sum_{m=1}^{n} J_k(m) \sim \frac{n^{k+1}}{(k+1)\zeta(k+1)}$

That's all folks!

Maryse, Michèle, Olivier : merci !