Nombres premiers : des Éléments d'Euclide à la conjecture de Riemann

Jean Mawhin

Université Catholique de Louvain

Retournons à l'école primaire

- **entiers positifs** : $1, 2, 3, 4, 5, \ldots, 27, \ldots, 2017, \ldots$
- **addition** : $1 + 1 = 2, 1 + 2 = 2 + 1 = 3, \ldots$
- **élément neutre pour l'addition** : 0
  $0 + 3 = 3 + 0 = 3$

Retournons à l'école primaire

- **entiers positifs** : $1, 2, 3, 4, 5, \ldots, 27, \ldots, 2017, \ldots$
- **addition** : $1 + 1 = 2, 1 + 2 = 2 + 1 = 3, \ldots$
- **élément neutre pour l'addition** : 0
  $0 + 3 = 3 + 0 = 3$
- **multiplication** :
  $3 \times 6 = 6 + 6 + 6 = 3 + 3 + 3 + 3 + 3 + 3 = 6 \times 3$
- **élément neutre pour la multiplication** : 1
  $1 \times 4 = 4 \times 1 = 4$

Les atomes de l'arithmétique

- **addition** : $2 = 1 + 1,\ 3 = 1 + 1 + 1,\ \ldots$
  - $n = 1 + 1 + \ldots + 1$ *(n fois)*
  - tout entier positif pour s'obtenir par additions successives à partir du seul “atome" 1

Les atomes de l'arithmétique

- **addition** : $2 = 1 + 1,\ 3 = 1 + 1 + 1,\ \ldots$
  - $n = 1 + 1 + \ldots + 1$ *(n fois)*
  - tout entier positif pour s'obtenir par additions successives à partir du seul "atome" 1

- **multiplication** :

$1 = 1$	$8 = 2 \times 2 \times 2$	$15 = 3 \times 5$
$2 = 2$	$9 = 3 \times 3$	$16 = 2 \times 2 \times 2 \times 2$
$3 = 3$	$10 = 2 \times 5$	$17 = 17$
$4 = 2 \times 2$	$11 = 11$	$18 = 2 \times 3 \times 3$
$5 = 5$	$12 = 2 \times 2 \times 3$	$19 = 19$
$6 = 2 \times 3$	$13 = 13$	$20 = 2 \times 2 \times 5$
$7 = 7$	$14 = 2 \times 7$	$21 = 3 \times 7$

Les nombres premiers

- **entiers** : ceux qui ne peuvent pas s'écrire comme produit de deux entiers plus petits,
  et ceux qui le peuvent
  - ces derniers s'écrivent comme produits de nombres de la première catégorie
  - les nombres de la première catégorie constituent les “atomes" pour la multiplication

Les nombres premiers

- **entiers** : ceux qui ne peuvent pas s'écrire comme produit de deux entiers plus petits,
  et ceux qui le peuvent
  - ces derniers s'écrivent comme produits de nombres de la première catégorie
  - les nombres de la première catégorie constituent les “atomes" pour la multiplication
- **nombre premier** : entier positif > 1 qui ne peut pas s'écrire comme produit de deux entiers plus petits
  - n'est divisible par aucun entier $(\neq 1)$ plus petit que lui
  - a exactement deux diviseurs différents

Les nombres premiers

- **entiers** : ceux qui ne peuvent pas s'écrire comme produit de deux entiers plus petits,
  et ceux qui le peuvent
  - ces derniers s'écrivent comme produits de nombres de la première catégorie
  - les nombres de la première catégorie constituent les “atomes" pour la multiplication
- **nombre premier** : entier positif > 1 qui ne peut pas s'écrire comme produit de deux entiers plus petits
  - n'est divisible par aucun entier $(\neq 1)$ plus petit que lui
  - a exactement deux diviseurs différents
- $2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97, \ldots$

Des jumeaux et des couples

- la définition exclut 1 (inutile comme atome multiplicatif)
- 2 est le seul nombre premier pair

Des jumeaux et des couples

- la définition exclut 1 (inutile comme atome multiplicatif)
- 2 est le seul nombre premier pair
- **nombres premiers jumeaux** (leur différence est 2)
  - $(3,5),\ (5,7),\ (11,13),\ (17,19),\ (29,31),\ (41,43),\ (59,61),\ (71,73),\ldots$
  - on ne sait pas s'il y en a une infinité

Des jumeaux et des couples

- la définition exclut 1 (inutile comme atome multiplicatif)
- 2 est le seul nombre premier pair
- **nombres premiers jumeaux** (leur différence est 2)
  - $(3,5),\ (5,7),\ (11,13),\ (17,19),\ (29,31),\ (41,43),\ (59,61),\ (71,73),\ldots$
  - on ne sait pas s'il y en a une infinité
- $4=2+2,\ 6=3+3,\ 8=3+5,\ 10=5+5,\ 12=5+7,\ 14=7+7,\ 16=5+11,\ 18=7+11,\ 20=7+13,\ \ldots$
  - on ne sait pas si tout nombre pair supérieur à 2 est la somme de deux nombres premiers
  - **conjecture de Goldbach** (1742)

Euclide fait aussi de l'arithmétique

EUCLIDE (300 AVJC), *Éléments*, Livre VII

- *si un nombre premier* p *divise un produit* ab *, il divise* a *ou* b
  - exemple : 2 *divise* $12 = 3 \times 4$ *et* 4

Euclide fait aussi de l'arithmétique

EUCLIDE (300 AVJC), *Éléments*, Livre VII

- *si un nombre premier* p *divise un produit* ab *, il divise* a *ou* b
  - exemple : 2 *divise* $12 = 3 \times 4$ *et* 4
- *tout entier se décompose de manière unique, à l'ordre des facteurs près, en un produit de nombres premiers*
  - exemple : $140 = 2^2 \times 5 \times 7$

Euclide fait aussi de l'arithmétique

EUCLIDE (300 AVJC), *Éléments*, Livre VII

- *si un nombre premier p divise un produit ab, il divise a ou b*
  - exemple : 2 *divise* $12 = 3 \times 4$ *et* 4
- *tout entier se décompose de manière unique, à l'ordre des facteurs près, en un produit de nombres premiers*
  - exemple : $140 = 2^2 \times 5 \times 7$
- *il existe des nombres premiers arbitrairement grands*

Les preuves les plus courtes sont ...

- *il n'existe pas de plus grand nombre premier*
  - on le montre par l'absurde
  - soit n le plus grand nombre premier
  - l'entier $(2 \times 3 \times \ldots \times p \times \ldots \times n) + 1$ n'est divisible ni par 2, ni par 3, $\ldots$, ni par n
  - sa décomposition en produit de nombres premiers contient un nombre premier plus grand que n
  - cela contredit la définition de n

Les preuves les plus courtes sont ...

- *il n'existe pas de plus grand nombre premier*
  - on le montre par l'absurde
  - soit n le plus grand nombre premier
  - l'entier $(2 \times 3 \times \ldots \times p \times \ldots \times n) + 1$ n'est divisible ni par 2, ni par 3, $\ldots$, ni par n
  - sa décomposition en produit de nombres premiers contient un nombre premier plus grand que n
  - cela contredit la définition de n
- le **plus grand nombre premier** explicitement connu à ce jour contient $22.338.618$ chiffres (2016)

Les preuves les plus courtes sont ...

- *il n'existe pas de plus grand nombre premier*
  - on le montre par l'absurde
  - soit n le plus grand nombre premier
  - l'entier $(2 \times 3 \times \ldots \times p \times \ldots \times n) + 1$ n'est divisible ni par $2,$ ni par $3,$ $\ldots$, ni par n
  - sa décomposition en produit de nombres premiers contient un nombre premier plus grand que n
  - cela contredit la définition de n
- le **plus grand nombre premier** explicitement connu à ce jour contient $22.338.618$ chiffres (2016)
- celui qui en donnera un de plus de $10.000.000$ de chiffres recevra 100.000 \$ de l'*Electronic Frontier Foundation*

Des nombres premiers en formules

- **nombres de** MARIN MERSENNE (1588-1648) : $2^p - 1$
  - ils ne sont pas tous premiers
  - $2^{11} - 1 = 2047 = 23 \times 89$

Des nombres premiers en formules

- **nombres de** MARIN MERSENNE (1588-1648) : $2^p - 1$
  - ils ne sont pas tous premiers
  - $2^{11} - 1 = 2047 = 23 \times 89$
- **conjecture de** PIERRE DE FERMAT (1601-1665) :
  - *les nombres* $2^{2^n} + 1 \quad (n = 1, 2, 3, \ldots)$ *sont premiers*
  - LEONHARD EULER (1707-1783) : $2^{2^5} = 641 \times 6.700.417$! (1732)

Des nombres premiers en formules

- **nombres de** MARIN MERSENNE (1588-1648) : $2^p - 1$
  - ils ne sont pas tous premiers
  - $2^{11} - 1 = 2047 = 23 \times 89$
- **conjecture de** PIERRE DE FERMAT (1601-1665) :
  - *les nombres* $2^{2^n} + 1 \quad (n = 1, 2, 3, \ldots)$ *sont premiers*
  - LEONHARD EULER (1707-1783) : $2^{2^5} = 641 \times 6.700.417$! (1732)
- **formules du second degré**
  - *pour* $1 \leq n \leq 40, \quad n^2 - n + 41$ *est premier*
  - *pour* $1 \leq n \leq 78, \quad n^2 - 79n + 1601$ *est premier*
  - **conjecture de** MARCEL PAGNOL (1895-1974) :
    - *pour* n *impair,* $n + (n+2) + n(n+2)$ *est premier*
    - mais pour $n = 55,$ on trouve $3.247 = 17 \times 91$!

Le compteur de nombres premiers

- $\forall\, x \geq 0,\ \pi(x)$ $=$ **nombre de nombres premiers** $\leq x$

$\pi(x) = 0$	si	$0 \leq x < 2$	$\pi(x) = 3$	si	$5 \leq x < 7$
$\pi(x) = 1$	si	$2 \leq x < 3$	$\pi(x) = 4$	si	$7 \leq x < 11$
$\pi(x) = 2$	si	$3 \leq x < 5$	$\pi(x) = 5$	si	$11 \leq x < 13$

Le compteur de nombres premiers

- $\forall\, x \geq 0,\ \pi(x)$ $=$ **nombre de nombres premiers** $\leq x$

$$\begin{array}{lll|lll} \pi(x)=0 & \textbf{si} & 0 \leq x < 2 & \pi(x)=3 & \textbf{si} & 5 \leq x < 7 \\ \pi(x)=1 & \textbf{si} & 2 \leq x < 3 & \pi(x)=4 & \textbf{si} & 7 \leq x < 11 \\ \pi(x)=2 & \textbf{si} & 3 \leq x < 5 & \pi(x)=5 & \textbf{si} & 11 \leq x < 13 \end{array}$$

- il existe des formules explicites compliquées pour $\pi(x)$:

  $\pi(m) = \sum_{k=2}^{m} \left[\frac{(2\times 3\times\cdots\times(k-1))+1}{k} - \left[\frac{2\times 3\times\ldots\times(k-1)}{k} \right] \right]$

  $[y]$ désigne la **partie entière** du nombre réel y

Le compteur de nombres premiers

- $\forall x \geq 0,\ \pi(x)$ = **nombre de nombres premiers** $\leq x$

$\pi(x) = 0$	si	$0 \leq x < 2$	$\pi(x) = 3$	si	$5 \leq x < 7$
$\pi(x) = 1$	si	$2 \leq x < 3$	$\pi(x) = 4$	si	$7 \leq x < 11$
$\pi(x) = 2$	si	$3 \leq x < 5$	$\pi(x) = 5$	si	$11 \leq x < 13$

- il existe des formules explicites compliquées pour $\pi(x)$:
$$\pi(m) = \sum_{k=2}^{m} \left[\frac{(2\times 3\times\cdots\times(k-1))+1}{k} - \left[\frac{2\times 3\times\ldots\times(k-1)}{k}\right]\right]$$
$[y]$ désigne la **partie entière** du nombre réel y

- Leonard Euler (1751) : *certains mystères échapperont toujours à l'esprit humain. Il suffit de jeter un coup d'oeil au tableau des nombres premiers, et l'on verra qu'il n'y règne ni ordre, ni règles*

Des amusements de Gauss

CARL-FRIEDRICHS GAUSS (1777-1855)

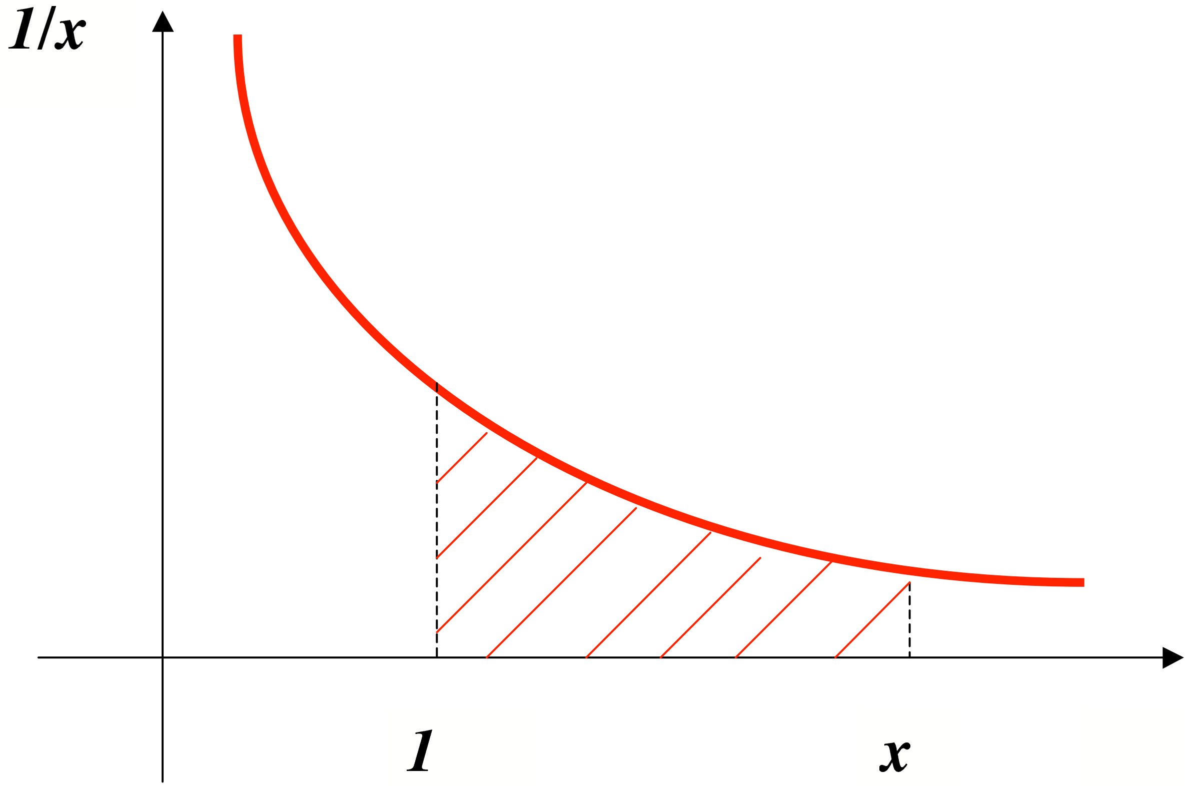
- vers 15 ans (1792)
  - scrute une table de nombres premiers
  - observe qu'aux environs de l'entier m la **proportion** de nombres premiers est environ $\frac{1}{\ln m}$
  - écrit : *vous n'avez aucune idée de la poésie que recèle une table de logarithmes*

Des amusements de Gauss

CARL-FRIEDRICHS GAUSS (1777-1855)

- vers 15 ans (1792)
  - scrute une table de nombres premiers
  - observe qu'aux environs de l'entier m la **proportion** de nombres premiers est environ $\frac{1}{\ln m}$
  - écrit : *vous n'avez aucune idée de la poésie que recèle une table de logarithmes*
- **logarithme népérien** $\ln$
  - logarithme en base $e = 2,718281...$
  - $\ln x = \int_1^x \frac{ds}{s}, \quad \ln 1 = 0, \quad \ln e = 1, \quad \ln e^x = e^{\ln x} = x$

Logarithme népérien



$$\boxed{\ln x = \int_1^x \frac{ds}{s}}$$

Logarithme intégral

- l'observation de Gauss entraîne :
  - $\pi(x)$ doit être approximativement égal à $\int_2^x \frac{ds}{\ln s}$
  - **logarithme intégral** : $Li(x) := \int_2^x \frac{ds}{\ln s}$

Logarithme intégral

- l'observation de Gauss entraîne :
  - $\pi(x)$ doit être approximativement égal à $\int_2^x \frac{ds}{\ln s}$
  - **logarithme intégral** : $Li(x) := \int_2^x \frac{ds}{\ln s}$
- remarque :
  - $\lim_{x\to+\infty} \frac{Li(x)}{x/\ln x} = 1$
  - règle de l'Hospital :

    $\lim_{x\to\infty} \frac{Li(x)\ln x}{x} = \lim_{x\to\infty}(1 + \frac{Li(x)}{x})$

    $= 1 + \lim_{x\to\infty} \frac{1}{\ln x} = 1$

Les tables de la loi

x	$\pi(x)$	$Li(x)$	$x/\ln x$
10	4	6	4
10^2	25	30	22
10^3	168	178	145
10^4	1.229	1.246	1.086
10^5	9.592	9.630	8.686
10^6	78.498	78.628	72.382
10^7	664.579	664.918	620.421
10^8	5.761.455	5.762.209	5.428.711
10^9	50.847.534	50.849.237	48.254.942
10^{10}	455.052.511	455.055.615	434.594.481
10^{11}	4.118.054.813	4.118.066.401	3.928.131.653
10^{12}	37.607.912.018	37.607.950.281	36.191.205.825

Conjectures

- **conjecture de** GAUSS (1792) :
  - $\lim_{x \to +\infty} \frac{\pi(x)}{Li(x)} = 1$
  - $\Leftrightarrow \quad \lim_{x \to \infty} \frac{\pi(x)}{x/\ln x} = 1$
  - il va falloir plus de cent ans pour la prouver

Conjectures

- **conjecture de** Gauss (1792) :
  - $\lim_{x\to+\infty} \frac{\pi(x)}{Li(x)} = 1$
  - $\Leftrightarrow \quad \lim_{x\to\infty} \frac{\pi(x)}{x/\ln x} = 1$
  - il va falloir plus de cent ans pour la prouver
- **conjecture de** Legendre (1798, 1808)
  - $\pi(x) = \frac{x}{\ln x - A(x)}$ *avec* $\lim_{x\to+\infty} A(x) = 1,08366\ldots$

Adrien-Marie Legendre (1752-1833)

Progresser par progressions

- soit x un réel et n un entier positif
- **progression géométrique de raison** x : $1, x, x^2, x^3, \ldots$

Progresser par progressions

- soit x un réel et n un entier positif
- **progression géométrique de raison** x : $1, x, x^2, x^3, \ldots$
- **somme** S_n **des** n **premiers termes d'une progression géométrique de raison** x
  - $S_n = 1 + x + x^2 + x^3 + \ldots + x^{n-1} = \sum_{k=0}^{n-1} x^k$
  - $xS_n = x + x^2 + x^3 + x^4 + \ldots + x^n = S_n - 1 + x^n$
  - $(x-1)S_n = x^n - 1$
  - *si* $x \neq 1, \quad S_n = \frac{x^n - 1}{x - 1} = \frac{1}{1-x} + \frac{x^n}{x-1}$
  - *si* $x = 1, \quad S_n = n$

Travailler en séries

- $S_n = \frac{1}{1-x} + \frac{x^n}{x-1}$ *si* $x \neq 1$
  - *si* $-1 < x < 1$ ($\Leftrightarrow$ $|x| < 1$), $\lim_{n\to\infty} \frac{x^n}{x-1} = 0$
  - $\lim_{n\to\infty} S_n = 1 + x + x^2 + \ldots = \sum_{k=0}^{\infty} x^k = \frac{1}{1-x}$ *si* $|x| < 1$
  - *si* $|x| \geq 1$, $\lim_{n\to\infty} S_n$ *n'existe pas*
  - **série** : “somme d'une infinité de termes"

Travailler en séries

- $S_n = \frac{1}{1-x} + \frac{x^n}{x-1}$ *si* $x \neq 1$
  - *si* $-1 < x < 1$ ($\Leftrightarrow$ $|x| < 1$), $\lim_{n\to\infty} \frac{x^n}{x-1} = 0$
  - $\lim_{n\to\infty} S_n = 1 + x + x^2 + \ldots = \sum_{k=0}^{\infty} x^k = \frac{1}{1-x}$ *si* $|x| < 1$
  - *si* $|x| \geq 1$, $\lim_{n\to\infty} S_n$ *n'existe pas*
  - **série** : “somme d'une infinité de termes"
- exemple :
  - un premier pas de longueur 1 mètre
  - la longueur de chaque pas est la moitié du précédent
  - on parcourt $1 + \frac{1}{2} + \frac{1}{2^2} + \ldots = \frac{1}{1-\frac{1}{2}} = 2$ mètres

La formule magique d'Euler

- $1 + y + y^2 + \ldots + y^n + \ldots = \frac{1}{1-y}$ *si* $|y| < 1$
- $x > 1$ *réel,* p *premier* $\Rightarrow 0 < \frac{1}{p^x} < 1$

La formule magique d'Euler

- $1 + y + y^2 + \ldots + y^n + \ldots = \frac{1}{1-y}$ *si* $|y| < 1$
- $x > 1$ *réel,* p *premier* $\Rightarrow$ $0 < \frac{1}{p^x} < 1$
  - $y = \frac{1}{2^x}$: $1 + \frac{1}{2^x} + \frac{1}{2^{2x}} + \ldots + \frac{1}{2^{nx}} + \ldots = \frac{1}{1-\frac{1}{2^x}}$
  - $y = \frac{1}{3^x}$: $1 + \frac{1}{3^x} + \frac{1}{3^{2x}} + \ldots + \frac{1}{3^{nx}} + \ldots = \frac{1}{1-\frac{1}{3^x}}$
  - $\ldots \quad \ldots \quad \ldots \quad \ldots \quad \ldots \quad \ldots \quad \ldots \quad \ldots \quad \ldots$
  - $y = \frac{1}{p^x}$: $1 + \frac{1}{p^x} + \frac{1}{p^{2x}} + \ldots + \frac{1}{p^{nx}} + \ldots = \frac{1}{1-\frac{1}{p^x}}$
  - $\ldots \quad \ldots \quad \ldots \quad \ldots \quad \ldots \quad \ldots \quad \ldots \quad \ldots \quad \ldots$

La formule magique d'Euler

- $1 + y + y^2 + \ldots + y^n + \ldots = \frac{1}{1-y}$ *si* $|y| < 1$
- $x > 1$ *réel,* p *premier* $\Rightarrow 0 < \frac{1}{p^x} < 1$
  - $y = \frac{1}{2^x} \ : \ 1 + \frac{1}{2^x} + \frac{1}{2^{2x}} + \ldots + \frac{1}{2^{nx}} + \ldots = \frac{1}{1-\frac{1}{2^x}}$
  - $y = \frac{1}{3^x} \ : \ 1 + \frac{1}{3^x} + \frac{1}{3^{2x}} + \ldots + \frac{1}{3^{nx}} + \ldots = \frac{1}{1-\frac{1}{3^x}}$
  - $\ldots \quad \ldots \quad \ldots \quad \ldots \quad \ldots \quad \ldots \quad \ldots \quad \ldots \quad \ldots$
  - $y = \frac{1}{p^x} \ : \ 1 + \frac{1}{p^x} + \frac{1}{p^{2x}} + \ldots + \frac{1}{p^{nx}} + \ldots = \frac{1}{1-\frac{1}{p^x}}$
  - $\ldots \quad \ldots \quad \ldots \quad \ldots \quad \ldots \quad \ldots \quad \ldots \quad \ldots \quad \ldots$
- on multiplie et on trouve
- $1 + \frac{1}{2^x} + \frac{1}{3^x} + \ldots + \frac{1}{n^x} + \ldots = \frac{1}{\left(1-\frac{1}{2^x}\right)\left(1-\frac{1}{3^x}\right)\cdots\left(1-\frac{1}{p^x}\right)\cdots}$

Le Jean-Sébastien des séries

LEONHARD EULER

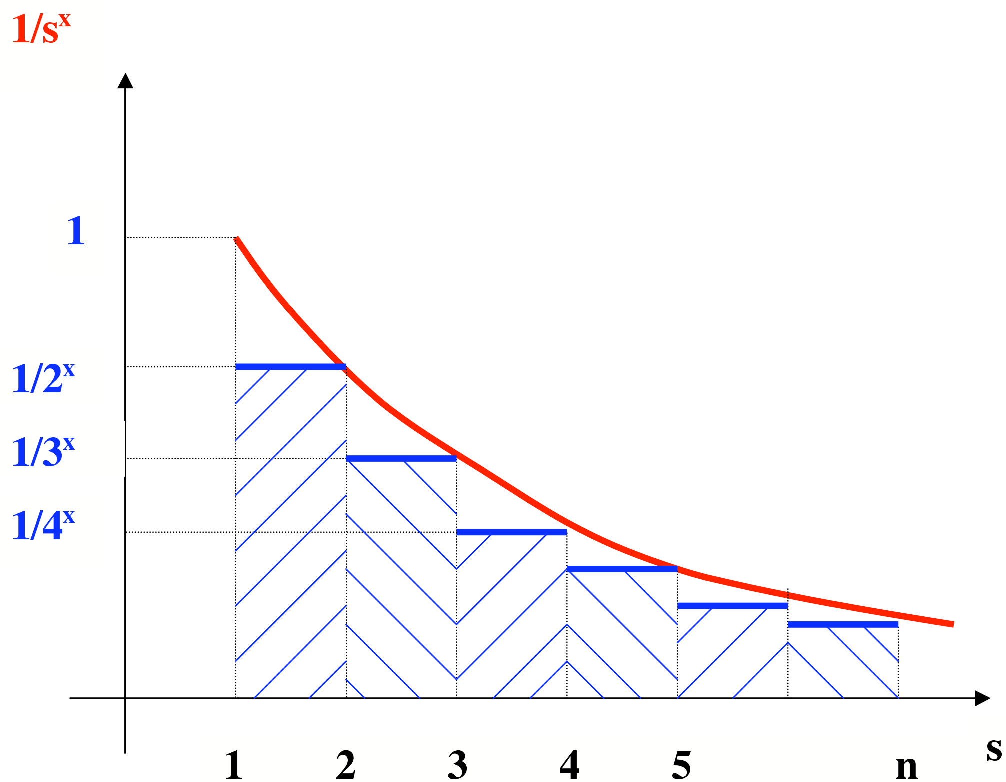
- $x > 1\ :\ \sum_{k=0}^{\infty} \frac{1}{k^x} = \frac{1}{\prod_{p\ premier} \left(1 - \frac{1}{p^x}\right)}$

Le Jean-Sébastien des séries

LEONHARD EULER

- $x > 1 \ : \ \sum_{k=0}^{\infty} \frac{1}{k^x} = \frac{1}{\prod_{p\ premier} \left(1 - \frac{1}{p^x}\right)}$
- $\sum_{k=0}^{\infty} \frac{1}{k^x} = 1 + \frac{1}{2^x} + \frac{1}{3^x} + \ldots + \frac{1}{n^x} + \ldots$
  - *converge* $\Leftrightarrow \ x > 1$
  - sa somme se calcule pour x entier pair (EULER)
    - $1 + \frac{1}{2^2} + \frac{1}{3^2} + \ldots = \frac{\pi^2}{6}$
    - $1 + \frac{1}{2^4} + \frac{1}{3^4} + \ldots = \frac{\pi^4}{90}$
  - toujours pas de formule de somme pour x entier impair

Convergence en image

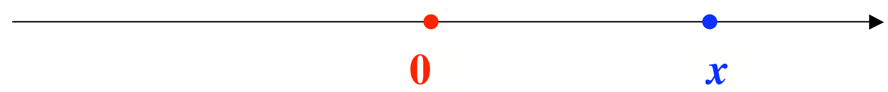


$$1+\frac{1}{2^x}+\frac{1}{3^x}+\ldots+\frac{1}{(n-1)^x}\leq 1+\int_1^n \frac{ds}{s^x}=\frac{x-n^{1-x}}{x-1}\leq \frac{x}{x-1}$$

$$si \quad x>1 \quad (p.ex. \quad \leq 2 \;\; si \;\; x=2)$$

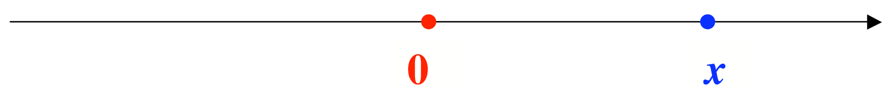
Complexifier pour y voir plus clair

- **nombres réels** : mesurent la position sur une droite munie d'une origine
  - **valeur absolue** $|x|$ de x : distance à l'origine



Complexifier pour y voir plus clair

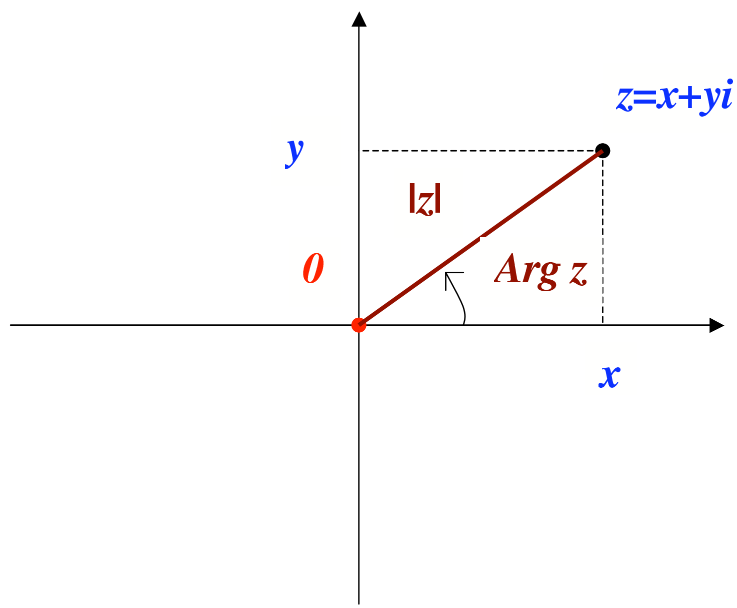
- **nombres réels** : mesurent la position sur une droite munie d'une origine
  - **valeur absolue** $|x|$ de x : distance à l'origine



- **nombres complexes** : couples (x, y) de réels, qu'on écrit $z = x + yi$ et sur lesquels on calcule algébriquement en remplaçant à la fin i^2 par -1
  - exemple : $(3+2i)(1-4i) = 3-12i+2i-8i^2 = 11-10i$
  - x est la **partie réelle** $\Re z$ de $z = x + yi$
  - y est la **partie imaginaire** $\Im z$ de $z = x + yi$
  - les complexes $(x, 0)$ sont identifiés aux réels
  - les complexes $(0, y)$ s'appellent les **imaginaires**

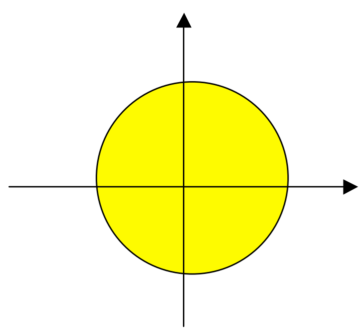
Planifier l'imaginaire

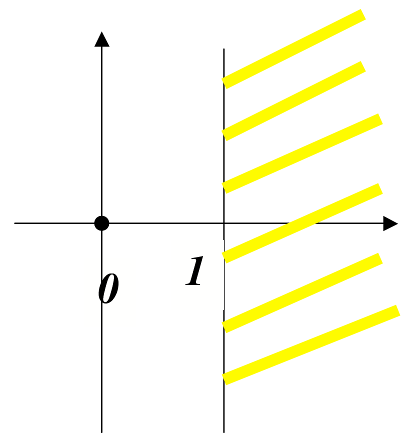
- **plan complexe** : on représente **géométriquement** $z = x + yi$ comme point du plan d'**abscisse** x et d'**ordonnée** y
- **module** de z : distance $|z| = \sqrt{x^2 + y^2}$ de z à 0
- **argument** de z : angle orienté positivement entre le demi-axe $0x$ et la demi-droite $0z$; noté $\arg z$



Complexes en séries

- *la série* $\sum_{k=0}^{\infty} z^k = 1 + z + z^2 + z^3 + \ldots$ *garde un sens pour* z *complexe et on a encore*
  $1 + z + z^2 + z^3 + \ldots = \frac{1}{1-z} \Leftrightarrow |z| < 1$
- *la série* $\sum_{k=0}^{\infty} \frac{1}{k^z} = 1 + \frac{1}{2^z} + \frac{1}{3^z} + \ldots$ *garde un sens pour* z *complexe et converge si et seulement si* $\Re z > 1$





Prolongement analytique

- $1 + z + z^2 + \ldots + z^n + \ldots = \frac{1}{1-z}$ *si* $|z| < 1$
  - le membre de gauche est une fonction de z définie $\Leftrightarrow$ $|z| < 1$
  - le membre de droite est une fonction de z définie $\Leftrightarrow$ $z \neq 1$
  - ces deux fonctions sont égales lorsque $|z| < 1$

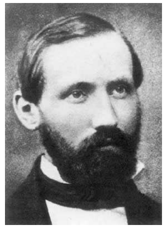
Prolongement analytique

- $1 + z + z^2 + \ldots + z^n + \ldots = \frac{1}{1-z}$ *si* $|z| < 1$
  - le membre de gauche est une fonction de z définie $\Leftrightarrow\ |z| < 1$
  - le membre de droite est une fonction de z définie $\Leftrightarrow\ z \neq 1$
  - ces deux fonctions sont égales lorsque $|z| < 1$
- la fonction $\frac{1}{1-z}$ est un **prolongement analytique** de la fonction $1 + z + z^2 + \ldots + z^n + \ldots$

Prolongement analytique

- $1 + z + z^2 + \ldots + z^n + \ldots = \frac{1}{1-z}$ *si* $|z| < 1$
  - le membre de gauche est une fonction de z définie $\Leftrightarrow |z| < 1$
  - le membre de droite est une fonction de z définie $\Leftrightarrow z \neq 1$
  - ces deux fonctions sont égales lorsque $|z| < 1$
- la fonction $\frac{1}{1-z}$ est un **prolongement analytique** de la fonction $1 + z + z^2 + \ldots + z^n + \ldots$
- si $|z| \geq 1$ la formule ci-dessus n'est plus valable; elle donnerait, par exemple pour $z = 2$ $1 + 2 + 2^2 + \ldots + 2^n + \ldots = -1$!

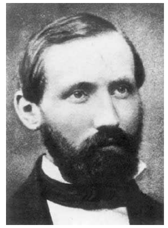
Un timide révolutionnaire



BERNHARD RIEMANN (1826-1866)

- a l'idée de considérer la fonction d'Euler $1 + \frac{1}{2^z} + \frac{1}{3^z} + \ldots + \frac{1}{n^z} + \ldots$ pour z complexe et $\Re z > 1$

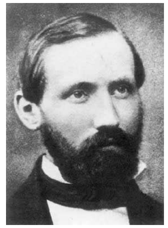
Un timide révolutionnaire



BERNHARD RIEMANN (1826-1866)

- a l'idée de considérer la fonction d'Euler $1 + \frac{1}{2^z} + \frac{1}{3^z} + \ldots + \frac{1}{n^z} + \ldots$ pour z complexe et $\Re z > 1$
- en trouve un prolongement analytique au plan complexe privé de $(1, 0)$, qu'il baptise $\zeta(z)$ et qui
  - *s'annule si* $z = -2, -4, -6, \ldots,$ **zéros triviaux**
  - *a ses autres zéros dans la bande* $0 \leq \Re z \leq 1$

Un timide révolutionnaire



BERNHARD RIEMANN (1826-1866)

- a l'idée de considérer la fonction d'Euler $1 + \frac{1}{2^z} + \frac{1}{3^z} + \ldots + \frac{1}{n^z} + \ldots$ pour z complexe et $\Re z > 1$
- en trouve un prolongement analytique au plan complexe privé de $(1, 0)$, qu'il baptise $\zeta(z)$ et qui
  - *s'annule si* $z = -2, -4, -6, \ldots,$ **zéros triviaux**
  - *a ses autres zéros dans la bande* $0 \leq \Re z \leq 1$
- **conjecture** : *les zéros non triviaux de* ζ *sont sur la droite* $\Re z = \frac{1}{2}$
- prouve que *sa conjecture fournit une estimation asymptotique de* $\pi(x)$ *plus précise que celle de* GAUSS

Une conjecture se fait théorème

- en 1896, indépendamment l'un de l'autre,

Charles de La Vallée Poussin et Jacques Hadamard

(1866-1962) (1965-1963)

  - montrent que *la conjecture de Gauss résulte du fait que les zéros non triviaux de* $\zeta(z)$ *ne se trouvent pas sur la droite* $\Re z = 1$
  - prouvent qu'*ils sont hors d'une zone contenant cette droite*

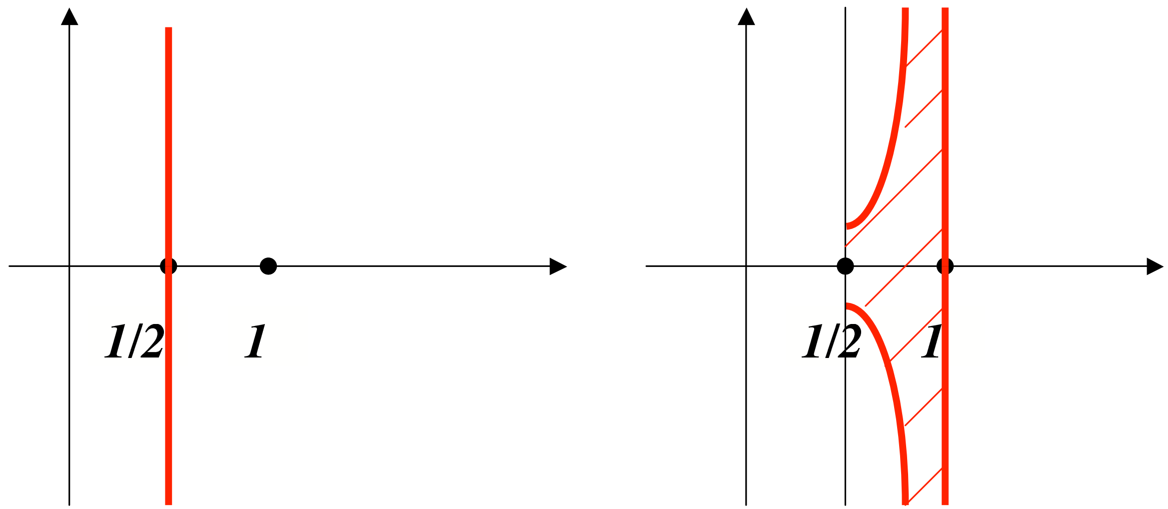
Une conjecture se fait théorème

- en 1896, indépendamment l'un de l'autre,

CHARLES DE LA VALLÉE POUSSIN (1866-1962) et JACQUES HADAMARD (1965-1963)

  - montrent que *la conjecture de Gauss résulte du fait que les zéros non triviaux de $\zeta(z)$ ne se trouvent pas sur la droite $\Re z = 1$*
  - prouvent qu'*ils sont hors d'une zone contenant cette droite*
- la conjecture de Gauss
  - devient le **théorème des nombres premiers**
  - reçoit de nombreuses autres preuves au XX^e siècle

Un petit dessin pour deux longs articles



conjecture de Riemann

zéros de $\zeta(z)$ sur la droite

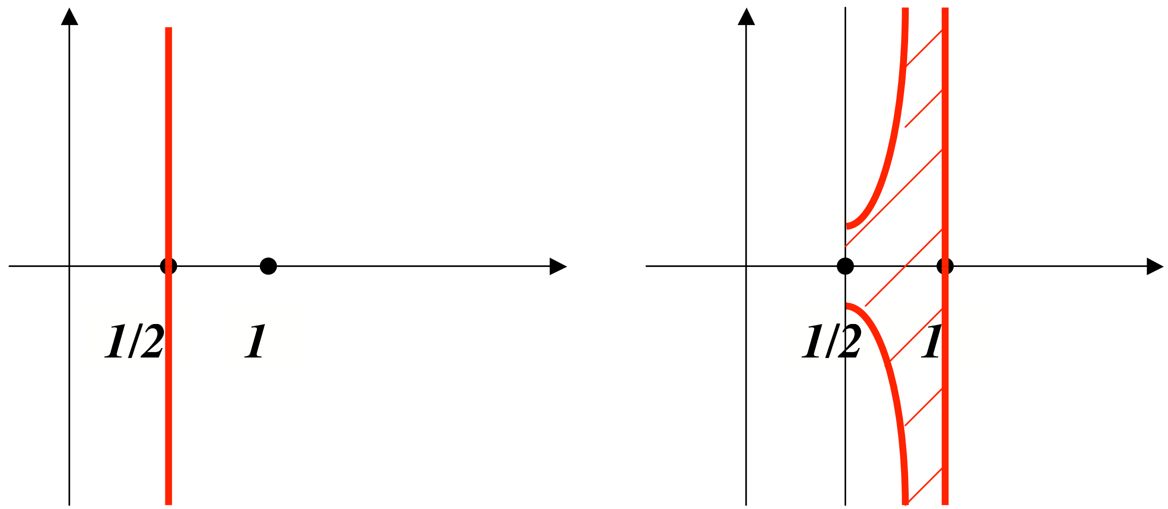
$\Re z = 1/2$

théorème de DLVP-Hadamard

pas de zéros de $\zeta(z)$ dans la

zone hachurée

Un petit dessin pour deux longs articles



conjecture de Riemann	**théorème de DLVP-Hadamard**
zéros de $\zeta(z)$ *sur la droite* $\Re z = 1/2$	*pas de zéros de* $\zeta(z)$ *dans la zone hachurée*

- DLVP simplifie considérablement sa preuve en utilisant l'inégalité élémentaire $3 + 4\cos\theta + \cos 2\theta \geq 0$

Essais infructueux et résultats partiels

- entre Thomas Stieltjes (1894) et Louis de Branges (2004) plusieurs mathématiciens de toutes statures, y compris John Nash, ont cru avoir démontré la **conjecture de Riemann**

Essais infructueux et résultats partiels

- entre THOMAS STIELTJES (1894) et LOUIS DE BRANGES (2004) plusieurs mathématiciens de toutes statures, y compris JOHN NASH, ont cru avoir démontré la **conjecture de Riemann**
- NORMAN LEVINSON : *un tiers au moins des zéros sont sur la droite* $\Re z = \frac{1}{2}$
- VAN DE LUNE : *le premier milliard de zéros s'y trouve aussi*
- *pour plus de 99 % des zéros* z : $|\Re z - \frac{1}{2}| \leq \frac{8}{\ln|\Im z|}$

Essais infructueux et résultats partiels

- entre THOMAS STIELTJES (1894) et LOUIS DE BRANGES (2004) plusieurs mathématiciens de toutes statures, y compris JOHN NASH, ont cru avoir démontré la **conjecture de Riemann**
- NORMAN LEVINSON : *un tiers au moins des zéros sont sur la droite* $\Re z = \frac{1}{2}$
- VAN DE LUNE : *le premier milliard de zéros s'y trouve aussi*
- *pour plus de 99 % des zéros* z : $|\Re z - \frac{1}{2}| \leq \frac{8}{\ln|\Im z|}$
- la fonction ζ peut se définir sur certains corps plus abstraits que celui des complexes et la conjecture de Riemann est prouvée pour ces corps (ANDRÉ WEIL, PIERRE DELIGNE) !

Les spectres à la rescousse ?

- *le spectre d'un opérateur hermitien se trouve sur la droite réelle* : David Hilbert et George Polya ont suggéré il y a longtemps d'exprimer les zéros de la fonction zeta comme **spectre** d'un certain opérateur

Les spectres à la rescousse ?

- *le spectre d'un opérateur hermitien se trouve sur la droite réelle* : David Hilbert et George Polya ont suggéré il y a longtemps d'exprimer les zéros de la fonction zeta comme **spectre** d'un certain opérateur
- **formule de** Hugh Montgomery (1972) : décrit l'espacement moyen entre les zéros consécutifs de la fonction zeta (les petits écarts sont peu fréquents)

Les spectres à la rescousse ?

- *le spectre d'un opérateur hermitien se trouve sur la droite réelle* : DAVID HILBERT et GEORGE POLYA ont suggéré il y a longtemps d'exprimer les zéros de la fonction zeta comme **spectre** d'un certain opérateur
- **formule de** HUGH MONTGOMERY (1972) : décrit l'espacement moyen entre les zéros consécutifs de la fonction zeta (les petits écarts sont peu fréquents)
- le physicien FREEMAN DYSON identifie la formule de MONTGOMERY avec le résultat obtenu pour les valeurs propres de certaines matrices hermitiennes aléatoires décrivant les niveaux d'énergie des grands atomes ou des noyaux lourds (**Gaussian unitary ensemble**)

L'ordre viendra-t-il du chaos ?

- BERTRAND JULIA (1989) : introduit un “gaz numérique" abstrait (le **gaz de Riemann libre**) dont les particules sont des nombres premiers et dont la fonction de partition est identique à la fonction zeta

L'ordre viendra-t-il du chaos ?

- BERTRAND JULIA (1989) : introduit un “gaz numérique" abstrait (le **gaz de Riemann libre**) dont les particules sont des nombres premiers et dont la fonction de partition est identique à la fonction zeta
- J.B. BOST et ALAIN CONNES (1995) : construisent un C*-système dynamique dont la fonction de partition est la fonction zeta

L'ordre viendra-t-il du chaos ?

- Bertrand Julia (1989) : introduit un “gaz numérique" abstrait (le **gaz de Riemann libre**) dont les particules sont des nombres premiers et dont la fonction de partition est identique à la fonction zeta
- J.B. Bost et Alain Connes (1995) : construisent un C*-système dynamique dont la fonction de partition est la fonction zeta
- Michael Berry et Jon P. Keating cherchent à exprimer les zéros de la fonction zeta comme valeurs propres de systèmes quantiques chaotiques

Pour conclure

- *Le seul véritable voyage, ce ne serait pas d'aller vers de nouveaux paysages, mais d'avoir d'autres yeux*

  MARCEL PROUST, *A la recherche du temps perdu*

Pour conclure

- *Le seul véritable voyage, ce ne serait pas d'aller vers de nouveaux paysages, mais d'avoir d'autres yeux*

  MARCEL PROUST, *A la recherche du temps perdu*

- Ce sera bien nécessaire pour prouver la conjecture de RIEMANN
  - problème déjà retenus par HILBERT en 1900 pour stimuler les mathématiques du XX^e siècle
  - qui fait toujours partie des problèmes du deuxième millénaire

Pour conclure

- *Le seul véritable voyage, ce ne serait pas d'aller vers de nouveaux paysages, mais d'avoir d'autres yeux*

  MARCEL PROUST, *A la recherche du temps perdu*

- Ce sera bien nécessaire pour prouver la conjecture de RIEMANN
  - problème déjà retenus par HILBERT en 1900 pour stimuler les mathématiques du XX^{e} siècle
  - qui fait toujours partie des problèmes du deuxième millénaire
- Qui pourra prétendre au prix de 1.000.000 $ du *Clay Institute* ?

Merci de m'avoir accordé votre entière attention

Un café serré vous attend, j'espère, pendant la pause