

Voyage en première classe au pays des nombres

« Des calculi mésopotamiens à la fonction zêta »

Clément Sire

Laboratoire de Physique Théorique

CNRS & Université Paul Sabatier

Toulouse, France

www.lpt.ups-tlse.fr/clement

Introduction

- La **théorie des nombres** (l'arithmétique) étudie les propriétés des **nombre entiers**
- Les nombres sont à la fois la **base des mathématiques**, mais savoir « compter » a aussi accompagné **l'essor de l'humanité**
 - **-30000** : Présence d'entailles numériques



- **-8000** : Apparition des *calculi* au Moyen Orient



Calculi sumérien en base 60

Introduction

- **-3300** : Premiers chiffres (sunia → sifr → zefiro → zéro) à Sumer (~Iraq) et en Élam (~Iran). Naissance de l'écriture et de la numérotation écrite



- **-300 à +500** : apparition de la graphie moderne et de la numération de position (Inde → Moyen Orient arabe → Afrique du Nord → Espagne maure)

୨ ୨ ୩ ୪ ୫ ୬ ୭ ୮ ୯ ୦
 ୧ ୨ ୩ ୪ ୫ ୬ ୭ ୮ ୯ ୦
 ୧ ୨ ୩ ୪ ୫ ୬ ୭ ୮ ୯ ୦

1 2 3 4 5 6 7 8 9 0
 1 2 3 4 5 6 7 8 9 0
 1 2 3 4 5 6 7 8 9
 1 2 3 4 5 6 7 8 9

Introduction

- La **théorie des nombres** a initié le développement des mathématiques et est à l'origine de nombre de ses sous domaines
- A l'inverse, les outils les plus complexes des mathématiques sont **revenus contribuer** à notre compréhension des propriétés des nombres entiers !
- Des **applications directes** aujourd'hui en cryptographie, informatique (« hashing », générateurs de « nombres aléatoires »...).

Introduction

- La **théorie des nombres** présente une **esthétique** fascinante, s'attachant aux éléments les plus « simples » des mathématiques, au caractère **universel**, qui nous accompagnent tout le long de notre vie
- Contrairement à la plupart des autres branches des mathématiques, de nombreux **problèmes centraux** en théorie des nombres **peuvent être exposés aux néophytes**, même s'ils n'ont **pas encore été résolus** par les mathématiciens, et même s'ils impliquent en fait des outils et méthodes mathématiques **extrêmement sophistiqués**

Un bref historique

- **-800** : équations diophantiennes en Inde
- **-600 à -200** : l'âge d'or des mathématiques grecques (Pythagore, Diophante...)
- **500-700** : le retour de l'Inde (Aryabhata, Brahmagupta...)
- **800-1400** : prééminence des mathématiciens arabes (Thabit ibn Qurra, Al-Baghdadi, Al-Haytham ou Alhazen...) et perses (Al-Farisi...)
- **À partir de 1600** : la théorie des nombres prend son essor en Europe (Viète, **Fermat, Euler, Lagrange, Legendre, Gauss**, Dirichlet, Jacobi, Kronecker, Kummer, Riemann, Tchebychev, Landau, Ramanujan, Serre, Wiles...), avant de s'internationaliser (USA, Japon...)

Quelques icônes de la théorie des nombres



Diophante



Aryabhata



Brahmagupta



Thabit ibn Qurra



Al-Haytham



Fermat



Euler



Lagrange



Gauss



Legendre

Quelques problèmes célèbres

- Le « dernier théorème de Fermat »
(Wiles 1994)

Il n'existe pas de nombres entiers non nuls x , y et z tels que :

$$x^n + y^n = z^n$$

dès que $n > 2$

« ... J'ai trouvé une merveilleuse démonstration de cette proposition. Mais la marge est trop étroite pour la contenir. »
Pierre de Fermat (~1595-1665)

Contributions majeures de Euler, Legendre, Cauchy, Dirichlet, Germain, Lamé, Kummer, Hellegouarch, Langlands, Shimura, Taniyam, Weil, Frey, Serre, Ribet...

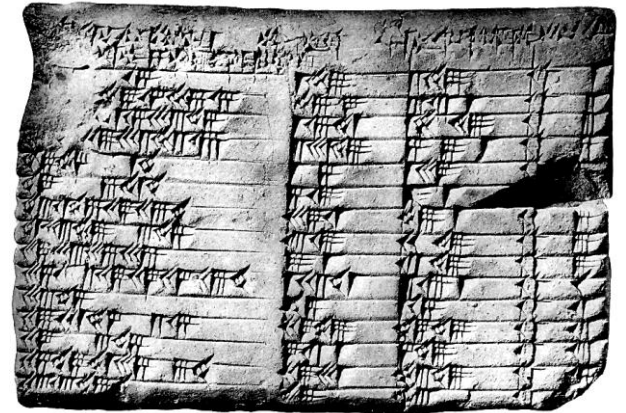
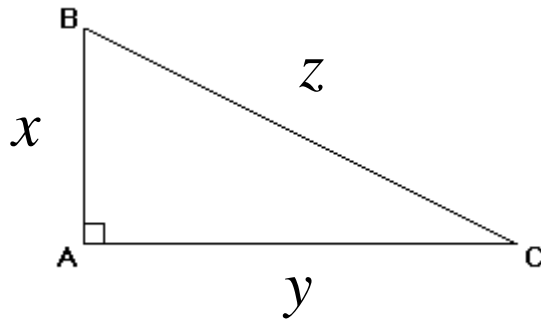
Les outils et méthodes impliqués sont d'une sophistication les plaçant à la pointe des mathématiques actuelles



Quelques problèmes célèbres

- Le « **dernier théorème de Fermat** » (Wiles 1994) : liens avec les « triplets pythagoriciens » et la géométrie ($n=2$)
- **Toutes les solutions** entières de $x^2 + y^2 = z^2$ s'écrivent sous la forme

- $x = p^2 - q^2$
- $y = 2pq$
- $z = p^2 + q^2$



Plimpton 322 (Iraq -1800)

avec p et q entiers ($p > q$)

- **Exemple** : $p = 3, q = 1 \Rightarrow x = 8, y = 6, z = 10$

Irrationalité de nombres remarquables

- Une question majeure en mathématiques (liée à « l'analyse ») est de savoir si certains nombres sont **irrationnels** (ne peuvent s'écrire comme p/q), ou même « **transcendants** » (non solution d'un polynôme à coefficients entiers)
- **Exemples** (Leibniz, Lambert, Euler, Hermite, von Lindemann, Shimura...):
 - $\sqrt{2}$ est irrationnel mais pas transcendant ($x^2 - 2 = 0$)
 - $e = 1 + \frac{1}{1!} + \frac{1}{2!} + \frac{1}{3!} + \frac{1}{4!} + \dots = \sum_{n=0}^{\infty} \frac{1}{n!} \approx 2,718\dots$ est transcendant
 - π est transcendant (l'impossible quadrature du cercle !)
 - $2^{\sqrt{2}}, e^{\pi}, \zeta(3), e^{p/q}, \log(p/q)\dots$ (p/q fraction d'entiers) sont transcendants et donc irrationnels
 - $e + \pi, e\pi, \log(\pi), \pi^e, e^e, \log(2)\log(3), \zeta(5) ???$

Quelques problèmes célèbres

➤ La « conjecture $3n+1$ » (Collatz 1937)

- On part d'un entier n quelconque
- Si n est pair : $n \rightarrow n/2$
Si n est impair : $n \rightarrow (3n+1)/2$
- On recommence, sauf si on atteint $n=1$

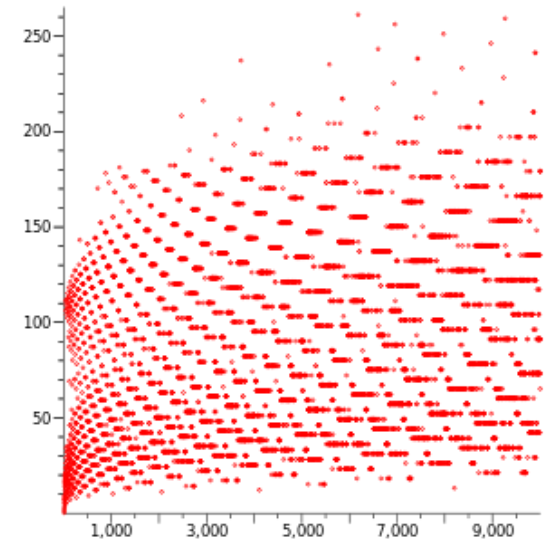
➤ **Conjecture** : pour tout n initial, cette suite retourne à $n=1$

« Les mathématiques ne sont pas encore mûres pour ce type de problèmes » – Paul Erdős

➤ « **Démonstration** » :

$$n_k \approx (1/2)^{k/2} (3/2)^{k/2} n_0 = (3/4)^{k/2} n_0$$

$$k_{\text{fin}} \approx 2 \frac{\log(n_0)}{\log(4/3)}$$



La fonction logarithme (Napier 1614 ; Euler 1730)

➤ $\log(x)$ est **l'aire** entre 1 et x sous la courbe $y = 1/x$

➤ Il existe un unique nombre

$$e = 1 + \frac{1}{1!} + \frac{1}{2!} + \frac{1}{3!} + \frac{1}{4!} + \dots = \sum_{n=0}^{\infty} \frac{1}{n!} = 2.7182818284\dots$$

tel que $\log(e) = 1$

➤ Si $x = e^y$ ($e^y = \sum_{k=0}^{\infty} \frac{y^k}{k!}$; « l'exponentielle »), alors **inversement**, on a $y = \log(x)$

➤ Si $x_1 = e^{y_1}$ et $x_2 = e^{y_2}$, on a

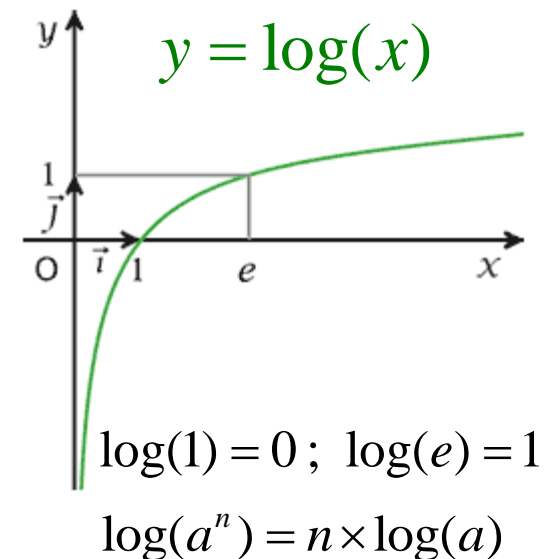
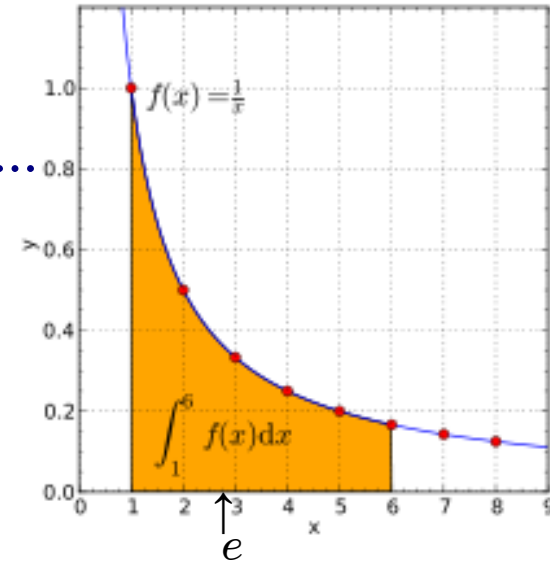
$$x_1 \times x_2 = e^{y_1} e^{y_2} = e^{y_1 + y_2}$$

et donc $\log(x_1 x_2) = \log(x_1) + \log(x_2)$

➤ Si $x = a^y$, et comme $a = e^{\log(a)}$, on a

$$x = e^{y \log(a)}$$

et donc $y = \frac{\log(x)}{\log(a)}$



Les nombres « premiers »

- **Définition** : un nombre premier **n'est divisible que par lui-même** (et par 1, bien sûr)
- **Exemples** : 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, ..., $2^{57} 885 161 - 1$ (17 425 170 chiffres ; $\sim 10^{80}$ atomes dans l'univers observable),...
- Il existe une **infinité** de nombres premiers
- Ils forment les « **briques élémentaires** » de l'ensemble de tous les entiers et, sont donc les objets les plus importants de la théorie des nombres
- Ils sont de plus en plus « **rares** » parmi les grands nombres

L'infinitude des nombres premiers

➤ Supposons qu'il n'existe **que** n nombres premiers p_1, p_2, \dots, p_n

➤ Mais alors, les deux nombres

- $P = p_1 \times p_2 \times \dots \times p_n + 1$

- $Q = 1 \times 2 \times 3 \times 4 \dots \times p_n + 1 = p_n! + 1$

ne sont divisibles par **aucuns** des n nombres premiers, et sont donc **tous les deux premiers !**
(et plus grands que p_n)

➤ Cette **contradiction** avec notre hypothèse initiale implique qu'il existe une **infinité de nombres premiers** (Euclide ~-300)



Les nombres premiers vus comme « briques élémentaires »

- Tout nombre n est décomposable (ou factorisable) de **façon unique** en produit de nombres premiers

$$n = p_1^{a_1} \times p_2^{a_2} \times \dots \times p_k^{a_k} \quad (a_i \geq 1, i = 1, \dots, k)$$

- **Comment factoriser un nombre en facteurs premiers ?**

- **Force brute**: le diviser successivement par les nombres premiers inférieurs (si n n'est divisible par aucun nombre premier inférieur à \sqrt{n} , n est alors premier)

- **Algorithme de Shor** (cryptographie)

- **Exemples**: factorisez **12276** et **197**

(Rappel : 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, ...)

- $12276 = 2^2 \times 3^2 \times 11^1 \times 31^1$

- $197 = 197^1$ est premier (arrêt après 13, car $17^2 = 289$)

PGCD

- **Définition :** deux nombres n_1 et n_2 sont **premiers entre eux (PEE)** si et seulement si le **plus grand diviseur commun (PGCD)** est 1
- Pour trouver le PGCD, il suffit de compter les facteurs premiers en commun entre n_1 et n_2
Il existe des entiers relatifs tels que $an_1 + bn_2 = \text{PGCD}(n_1, n_2)$
(théorème de Bachet-Bézout 1624)
- **Exemples :**
 - $n_1 = 24 = 2^3 \times 3^1$ et $n_2 = 245 = 5^1 \times 7^2$
sont premiers entre eux et $5 \times n_2 - 51 \times n_1 = 1$
 - $n_1 = 120 = 2^3 \times 3^1 \times 5$ et $n_2 = 252 = 2^2 \times 3^2 \times 7^2$
ne sont pas premiers entre eux et $1 \times n_2 - 2 \times n_1 = 12$
avec comme PGCD $2^2 \times 3^1 = 12$ ($n_1 / 12 = 10$; $n_2 / 12 = 21$)

Arithmétique et « probabilités »

- Si on prend deux nombres entiers n_1 et n_2 au hasard, quelle est la « probabilité » P_2 pour qu'ils soient **premiers entre eux** (PEE) ?
- $1 - P_2$ est la probabilité pour qu'il ne soient pas PEE
- La probabilité pour que leur PGCD soit n est que n divise n_1 et n_2 , et que n_1/n et n_2/n soient PEE
Cet événement a comme probabilité

$$\frac{1}{n} \times \frac{1}{n} \times P_2 = \frac{P_2}{n^2}$$

- Au total,

$$1 - P_2 = \frac{P_2}{2^2} + \frac{P_2}{3^2} + \frac{P_2}{4^2} + \frac{P_2}{5^2} + \dots = P_2 \sum_{n=2}^{\infty} \frac{1}{n^2}$$

$$P_2 = 1 / \sum_{n=1}^{\infty} \frac{1}{n^2} = 1 / \zeta(2), \quad \text{avec} \quad \zeta(x) = \sum_{n=1}^{\infty} \frac{1}{n^x}$$

Les nombres premiers

- Plus généralement, la probabilité pour que k nombres soient PPE est

$$P_k = 1 / \sum_{n=1}^{\infty} \frac{1}{n^k} = 1 / \zeta(k)$$

ou $\zeta(k)$ est la **fonction zêta de Riemann**, omniprésente en théorie des nombres

- $\zeta(2) = \frac{\pi^2}{6}$, $\zeta(4) = \frac{\pi^4}{90}$... (Euler); $\zeta(3)$ est irrationnel (Apéry 1978)

- **Expériences** : par deux, choisissez chacun un nombre au hasard entre 2 et 61. Nous compterons le pourcentage de paires PPE, qui devrait être proche de 60% ($P_2 = 1 / \zeta(2) = \frac{6}{\pi^2} \approx 0.6079...$)

Les nombres premiers se font de plus en plus rares !

➤ On définit

$$\Pi(n) = \# \text{ de nombres premiers } \leq n$$

En particulier, $\Pi(p_n) = n$, si p_n est le n -ième nombre premier

➤ « **Théorème des nombres premiers** »

(La Vallée Poussin & Hadamard 1896)

$$\Pi(n) \approx \frac{n}{\log(n)}, \quad \text{quand } n \rightarrow \infty$$

➤ « **Théorème des nombres premiers** » amélioré

(La Vallée Poussin 1899)

$$\Pi(n) \approx \int_0^n \frac{dx}{\log(x)} = \text{li}(n), \quad \text{quand } n \rightarrow \infty$$

n	$\Pi(n)$	$\Pi(n) - \frac{n}{\log(n)}$	Erreur Relative (%)
10^2	25	3	15
10^4	1 229	143	13
10^6	78 498	6 116	8,4
10^9	50 847 534	2 592 592	5,4
10^{12}	37 607 912 018	1 416 705 193	3,9
10^{18}	24 739 954 287 740 860	612 483 070 893 536	2,5
10^{23}	1 925 320 391 606 803 968 923	37 083 513 766 578 631 309	2,0

n	$\Pi(n)$	$\text{li}(n) - \Pi(n)$	Erreur Relative (%)
10^2	25	5	20
10^4	1 229	17	1,3
10^6	78 498	130	0,17
10^9	50 847 534	1 701	$3,3 \times 10^{-3}$
10^{12}	37 607 912 018	38 263	$1,0 \times 10^{-4}$
10^{18}	24 739 954 287 740 860	21 949 555	$8,9 \times 10^{-8}$
10^{23}	1 925 320 391 606 803 968 923	7 250 186 216	$4,0 \times 10^{-10}$

Conséquences du théorème des nombres premiers

- $P(n) = \Pi(n) - \Pi(n-1)$ est une mesure de la « **probabilité** » pour que n soit premier

Pour des grands n , le théorème des nombres premiers implique (en moyenne)

$$P(n) \approx \frac{1}{\log(n)}$$

- Il donne aussi une **estimation** du n -ième nombre premier, quand n est grand :

$$\Pi(p_n) = n \approx \frac{p_n}{\log(p_n)} \Rightarrow p_n \approx n \log(n)$$

Conjecture de Goldbach (1742)

➤ Tout nombre entier pair supérieur à 3 peut s'écrire comme la **somme de 2 nombres premiers**

➤ **Exemples** : $4 = 2 + 2$, $6 = 3 + 3$, $8 = 3 + 5$, $10 = 3 + 7 = 5 + 5$,
 $12 = 5 + 7, \dots$, $50 = 19 + 31 = 13 + 37 = 7 + 43 = 3 + 47, \dots$

➤ « **Preuve probabiliste** » (aucune preuve connue)

La probabilité que $n = p + (n - p)$, avec p et $(n - p)$ premiers est

$$P(p) \times P(n - p) \approx \frac{1}{\log(p)} \times \frac{1}{\log(n - p)}$$

Le nombre $N_2(n)$ de façons d'écrire n comme la somme de deux nombres premiers est donc

$$N_2(n) \approx \sum_{p=3}^{n/2} \frac{1}{\log(p)} \times \frac{1}{\log(n - p)} \approx \frac{n}{\log^2(n)} \gg 1$$

Conjecture des nombres premiers « jumeaux » et de Polignac (1849)

- Pour tout $k \geq 1$, il existe une **infinité de nombres premiers** p tels que $p + 2k$ est **aussi premier**
- **Exemples ($k = 1$)** : (3, 5), (5, 7), (11, 13), (17, 19), (29, 31), (41, 43), (59, 61), (71, 73), (101, 103), (107, 109), (137, 139),..., $2003663613 \times 2^{195000} \pm 1$ (58711 chiffres ; Vautier 2007),..., $3756801695685 \times 2^{666669} \pm 1$ (200700 chiffres ; *PrimeGrid* 2011),...
- **Meilleurs résultats rigoureux connus**
 - Le nombre de jumeaux inférieurs à n est borné par $\frac{n}{\log^2(n)}$ (Brun 1911)
 - Il y a une infinité de k – jumeaux pour au moins un $k < 35$ millions (Zhang 2013 ; borne améliorée à 2707 par le projet *Polymath*)

Conjecture des nombres premiers jumeaux et de Polignac (1849)

➤ « Preuve probabiliste » (aucune preuve connue)

La probabilité que p et $p + 2k$ soient premiers est

$$P(p) \times P(p + 2k) \approx \frac{1}{\log(p)} \times \frac{1}{\log(p + 2k)}$$

Le nombre $J_k(n)$ de k – jumeaux inférieurs à n est donc de l'ordre

$$J_k(n) \approx \sum_{p=3}^n \frac{1}{\log(p)} \times \frac{1}{\log(p + 2k)} \approx C_k \frac{n}{\log^2(n)}$$

Conjecture de Hardy-Littlewood (1911)

$$C_1 = 2 \prod_{\substack{p \geq 3 \\ p \in P}} \frac{p(p-2)}{(p-1)^2} \approx 1,3203236316937\dots$$

Deux conjectures fausses

➤ **Nombres premiers de Fermat** $F_n = 2^{2^n} - 1$

$F_0 = 3, F_1 = 5, F_2 = 17, F_3 = 257, F_4 = 65\,537$ sont premiers,
mais... $F_5 = 4\,294\,967\,297 = 641 \times 6\,700\,417$ (Euler 1732)

➤ **Une conjecture « numérique » de Gauss**

(liée au théorème de La Vallée Poussin de 1899)

$$\Pi(n) < \int_0^n \frac{du}{\log(u)} = \text{li}(n)$$

On ne connaît pas de **contre-exemple** explicite,
mais **il a été démontré** qu'il existe au moins un
 $n < 10^{350}$ qui contredit cette inégalité

Les nombres de Mersenne (1588-1648)

- Les **nombres de Mersenne** s'écrivent sous la forme

$$M_p = 2^p - 1, \text{ où } p \text{ est premier}$$

- Ils sont des bons **candidats** pour former des nombres premiers. Leur intérêt est qu'il existe des **algorithmes très rapides** pour vérifier si M_p est premier (Lucas 1878 ; Lehmer 1930)
- Avec les **progrès de l'informatique**, les plus grands nombres premiers connus sont des nombres de Mersenne (48 connus en 2013) :

$$M_{19} = 524\,287 \text{ (Cataldi 1588)}, M_{31} = 2\,147\,483\,647 \text{ (Euler 1750)},$$

$$M_{127} = 39 \text{ chiffres (Lucas 1876)}, M_{521} = 157 \text{ chiffres (SWAC 1952)},$$

$$M_{1398269} = 420\,921 \text{ chiffres (GIMPS 1996)},$$

$$M_{57885161} = 17\,425\,170 \text{ chiffres (GIMPS 01/2013 ; 360000 processeurs),...}$$

Liens entre la fonction zêta de Riemann et les nombres premiers : formule d'Euler

➤ Si $|x| < 1$, on a $\frac{1}{1-x} = 1 + x + x^2 + x^3 + \dots = \sum_{k=1}^{\infty} x^k$ (somme géométrique)

En effet, $(1-x)(1+x+x^2+x^3+\dots) = 1+x+x^2+x^3+x^4+\dots$
 $-x-x^2-x^3-x^4-\dots = 1$

➤ **Considérons** $\frac{1}{1-\frac{1}{2^s}} \times \frac{1}{1-\frac{1}{3^s}} \times \frac{1}{1-\frac{1}{5^s}} \times \frac{1}{1-\frac{1}{7^s}} \times \dots = \prod_{k=1}^{\infty} \frac{1}{1-\frac{1}{p_k^s}}$,

qui peut s'écrire en développant en séries géométriques

$$\left(1 + \frac{1}{2^s} + \frac{1}{2^{2s}} + \frac{1}{2^{3s}} + \dots\right) \times \left(1 + \frac{1}{3^s} + \frac{1}{3^{2s}} + \frac{1}{3^{3s}} + \dots\right) \times$$

$$\left(1 + \frac{1}{5^s} + \frac{1}{5^{2s}} + \frac{1}{5^{3s}} + \dots\right) \times \left(1 + \frac{1}{7^s} + \frac{1}{7^{2s}} + \frac{1}{7^{3s}} + \dots\right) \times \dots$$

Liens entre la fonction zêta de Riemann et les nombres premiers : formule d'Euler

En développant ces produits, on obtient **chaque entier une fois exactement** (unicité de la factorisation en facteurs premiers)

$$\begin{aligned} & \left(1 + \frac{1}{2^s} + \frac{1}{2^{2s}} + \frac{1}{2^{3s}} + \dots\right) \times \left(1 + \frac{1}{3^s} + \frac{1}{3^{2s}} + \frac{1}{3^{3s}} + \dots\right) \times \\ & \left(1 + \frac{1}{5^s} + \frac{1}{5^{2s}} + \frac{1}{5^{3s}} + \dots\right) \times \left(1 + \frac{1}{7^s} + \frac{1}{7^{2s}} + \frac{1}{7^{3s}} + \dots\right) \times \dots \\ &= 1 + \frac{1}{2^s} + \frac{1}{3^s} + \frac{1}{2^{2s}} + \frac{1}{5^s} + \frac{1}{2^s} \times \frac{1}{3^s} + \frac{1}{7^s} + \frac{1}{2^{3s}} + \frac{1}{3^{2s}} + \frac{1}{2^s} \times \frac{1}{5^s} + \dots \\ &= 1 + \frac{1}{2^s} + \frac{1}{3^s} + \frac{1}{4^s} + \frac{1}{5^s} + \frac{1}{6^s} + \frac{1}{7^s} + \frac{1}{8^s} + \frac{1}{9^s} + \frac{1}{10^s} + \dots \\ &= \sum_{n=1}^{\infty} \frac{1}{n^s} = \zeta(s) = \prod_{k=1}^{\infty} \frac{1}{1 - \frac{1}{p_k^s}} \end{aligned}$$

Fonction zêta de Riemann et fonction de Möbius

$$\frac{1}{\zeta(s)} = \prod_{p \in \mathcal{P}} \left(1 - \frac{1}{p^s}\right) = \left(1 - \frac{1}{2^s}\right) \times \left(1 - \frac{1}{3^s}\right) \times \left(1 - \frac{1}{5^s}\right) \times \left(1 - \frac{1}{7^s}\right) \times \dots,$$

On définit alors la **fonction de Möbius** pour $n = p_1^{a_1} \times p_2^{a_2} \times \dots \times p_k^{a_k}$

- $\mu(n) = 0$, si n possède au moins un facteur premier p_i avec $a_i > 1$
(divisible par un carré, comme p_i^2)
- $\mu(n) = 1$, si k est pair et tous les a_i valent 1
- $\mu(n) = -1$, si k est impair et tous les a_i valent 1

On a clairement

$$\frac{1}{\zeta(s)} = \prod_{k=1}^{\infty} \left(1 - \frac{1}{p_k^s}\right) = \sum_{n=1}^{\infty} \frac{\mu(n)}{n^s}$$

Remarque : si n_1 et n_2 sont PPE, alors $\mu(n_1 \times n_2) = \mu(n_1) \times \mu(n_2)$
(fonction arithmétique multiplicative)

Fonctions de Möbius et de Mertens

- On peut montrer que $\sum_{k=1}^n |\mu(k)| = \sum_{k=1}^n \mu^2(k) \approx \frac{6}{\pi^2} n$

En admettant qu'il y ait, en moyenne, autant de n pour lesquels $\mu(n) = \pm 1$, on a $\mu(n) = +1$ (ou -1) avec probabilité $\frac{3}{\pi^2}$, et $\mu(n) = 0$ avec probabilité $1 - \frac{6}{\pi^2}$

- On définit la **fonction de Mertens** $M(n) = \sum_{k=1}^n \mu(k)$

On a alors l'estimation $M^2(n) = \sum_{k=1}^n \mu^2(k) + 2 \sum_{i \neq j} \mu(i) \mu(j) \approx \frac{6}{\pi^2} n$,

liée à la **conjecture de Mertens** (Stieljes 1885 ; Mertens 1897)

$M^2(n) < n$, qui a été pourtant **infirmée pour une infinité de n** par Odlyzko et te Riele (1985)... sans qu'aucun contre-exemple explicite ne soit connu ! À suivre...

Indicatrice d'Euler

On définit la **fonction indicatrice d'Euler**

$\phi(n) = \#$ d'entiers inférieurs à n qui sont premiers avec n

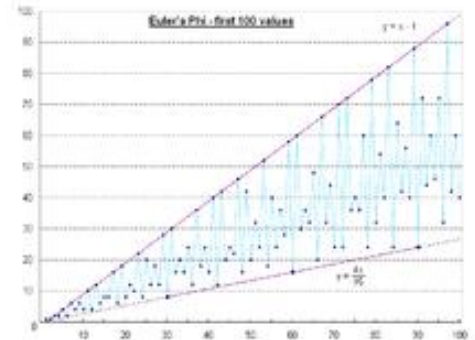
- Si $n = p_1^{a_1} \times p_2^{a_2} \times \dots \times p_k^{a_k}$, $\phi(n) = n \left(1 - \frac{1}{p_1}\right) \times \left(1 - \frac{1}{p_2}\right) \times \dots \times \left(1 - \frac{1}{p_k}\right)$
- Si n_1 et n_2 sont PPE, alors $\phi(n_1 \times n_2) = \phi(n_1) \times \phi(n_2)$
- **Quelques propriétés remarquables :**

$$\circ \phi(n) = n \sum_{d|n} \frac{\mu(d)}{d} ; \quad \sum_{d|n} \phi(d) = n ; \quad \sum_{n=1}^{\infty} \frac{\phi(n)}{n^s} = \frac{\zeta(s-1)}{\zeta(s)}$$

$$\circ \sum_{k=1}^n \phi(k) = \frac{1}{2} + \frac{1}{2} \sum_{k=1}^n \mu(k) \left[\frac{n}{k} \right]^2 \approx P_2 \times \# \text{ de paires} \approx \frac{3}{\pi^2} n^2$$

$$\circ 1 < \frac{n}{\phi(n)} < e^\gamma \log \log(n) + \frac{3}{\log \log(n)}$$

$$(\gamma = 0,5772156649\dots)$$



Les nombres « complexes » (Cardan 1545, Bombelli 1572)

- On définit **formellement** i tel que $i^2 = -1$
- Un **nombre complexe général** s'écrit $z = x + iy$, où x et y sont des nombres réels usuels
- On réalise les **opérations usuelles** (+, -, ×, ÷) « **normalement** » :

- $(2 + 3i) + (1 - 7i) = 3 - 4i$

- $(1 + 3i) \times (2 - 5i) = 2 - 5i + 6i - 15i^2 = 17 + i$

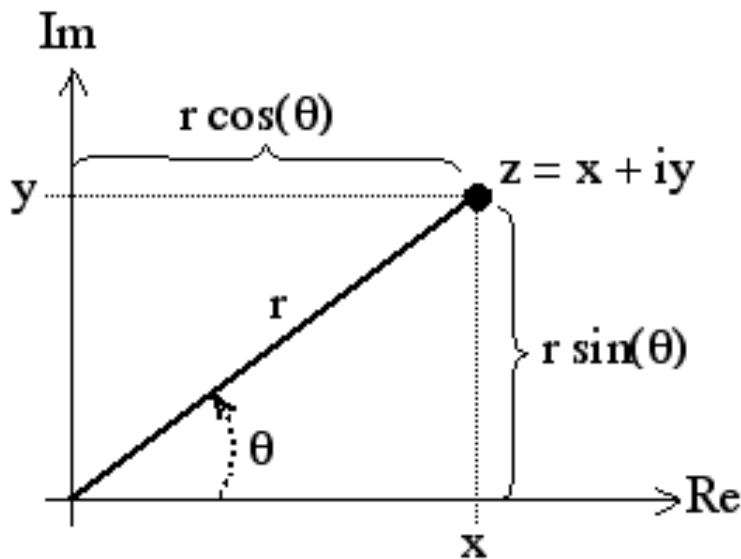
- $\frac{1}{1 + 2i} = \frac{1 - 2i}{(1 + 2i)(1 - 2i)} = \frac{1 - 2i}{1 + 2i - 2i - 4i^2} = \frac{1}{5} - \frac{2}{5}i$

➤ **Exercice :**

Montrer que pour $x = 1 + 2i$ et $x = 1 - 2i$, on a $x^2 - 2x + 5 = 0$

Les nombres « complexes » : interprétation géométrique

- On peut **représenter** de façon naturelle le nombre complexe $z = x + iy$ dans le plan (dit « complexe »)



- $r = \sqrt{x^2 + y^2}$ (Pythagore)
- $x = r \cos(\theta)$ (la partie *réelle*)
- $y = r \sin(\theta)$ (la partie *imaginaire*)

- L'addition de deux nombres complexes revient à une addition de vecteurs

L' hypothèse de Riemann (1859) : *le « Graal » des mathématiciens*

- On peut **étendre la fonction zêta de Riemann** aux nombres complexes $z = x + iy$, en posant

$$\zeta(z) = \sum_{n=1}^{\infty} \frac{1}{n^z}$$

et en utilisant

$$\frac{1}{n^z} = e^{-z \times \log n} = \sum_{k=0}^{\infty} \frac{(-z \log n)^k}{k!}$$

$$\left(\text{car } e^x = \sum_{k=0}^{\infty} \frac{x^k}{k!} \right)$$



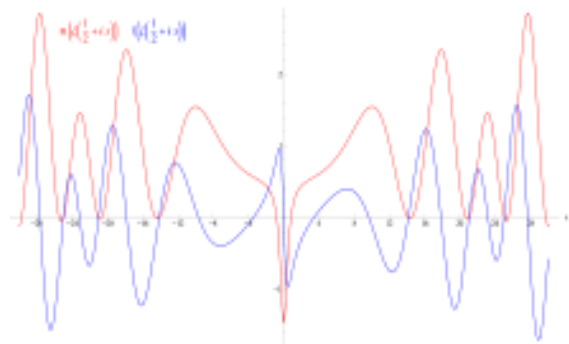
L' hypothèse de Riemann (1859) : *le « Graal » des mathématiciens*

➤ $\zeta(z)$ **s'annule** (c'est-à-dire $\zeta(z) = 0$) **uniquement pour**

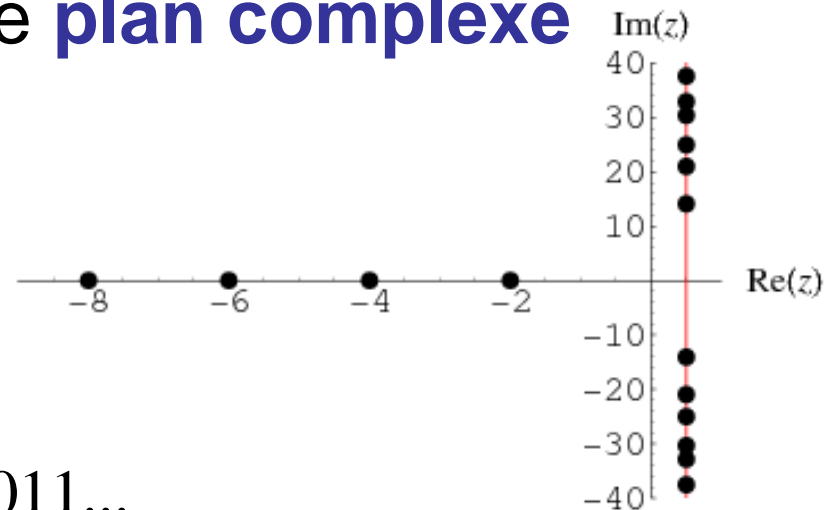
- $z = -2, -4, -6, -8...$ (les zéros "triviaux" de ζ)

- Et pour des nombres complexes de la forme $z_k = \frac{1}{2} \pm iy_k$

➤ **Interprétation géométrique :** les **zéros non triviaux** de zêta sont **tous** sur la droite verticale $x = \frac{1}{2}$ (la « ligne critique ») dans le **plan complexe**



$$y_1 = 14,135..., y_2 = 21,022..., y_3 = 25,011...$$



L' hypothèse de Riemann (1859): le « Graal » des mathématiciens

- C'est l'un des **23 problèmes majeurs** énoncés par **Hilbert** en 1902 (seuls 5 restent totalement non résolus, dont l'hypothèse de Riemann)
- C'est l'un des **8 problèmes** récompensés par un prix de 1 000 000\$ par la *Clay Foundation* (seule la conjecture de Poincaré a été résolue en 2003 par Perelman, qui a refusé le prix)
- L'hypothèse de Riemann est **confirmée numériquement**, et 10^{13} zéros ont été identifiés (et calculés numériquement) sur la ligne critique, ainsi que quelques zéros pour des très grands y_k (de l'ordre de 10^{24})
- Si elle est vraie, l'hypothèse de Riemann aurait une **multitude d'implications** en théorie des nombres, et en particulier, sur notre compréhension de la **répartition des nombres premiers**

Quelques conséquences de l'hypothèse de Riemann (HR)

➤ **Bornes** « optimales » de l'erreur de différentes estimations apparaissant en théorie des nombres

- $|\Pi(n) - \text{li}(n)| < \frac{1}{8\pi} \sqrt{n} \log(n)$, pour tout $n \geq 2657$

- On définit la **fonction de Mertens** $M(n) = \sum_{k=1}^n \mu(k)$

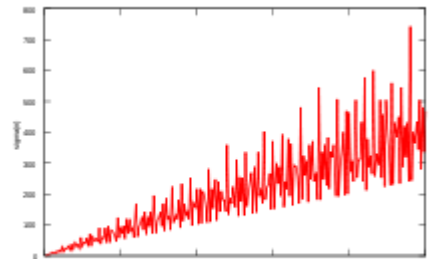
HR implique $|M(n)| < n^{\frac{1}{2} + \varepsilon}$, pour tout $\varepsilon > 0$ et n assez grand
alors que $|M(n)| > \sqrt{n}$, pour une infinité de valeurs de n

➤ HR est **équivalente** à de **nombreuses conjectures** en théorie des nombres

- Soit $H_n = 1 + \frac{1}{2} + \frac{1}{3} + \dots + \frac{1}{n} = \sum_{k=1}^n \frac{1}{k} \approx \log(n) + \gamma + \dots$, alors (Lagarias 2002)

$$\text{HR} \Leftrightarrow \sigma(n) < H_n + \log(H_n) e^{H_n}, \text{ pour } n > 1$$

où $\sigma(n)$ est la somme des diviseurs de n



***Conclusion d'un voyage dans
le temps (~10 000 ans), et
parmi les nombres (de 1 à ∞ ...
en passant par i) !***



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

(À mieux qu'un millionième de % près !)