HAL open science

Le théorème des nombres premiers

Emmanuel Royer

▶ To cite this version:

Emmanuel Royer. Le théorème des nombres premiers. Revue d'Auvergne, 2014, Des mathématiques en AUvergne, 611-612, pp.241-267. hal-02457459

HAL Id: hal-02457459
https://hal.science/hal-02457459

Submitted on 28 Jan 2020

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

LE THÉORÈME DES NOMBRES PREMIERS

EMMANUEL ROYER

Les nombres construits sur les entiers

L'ensemble des entiers naturels est l'ensemble des nombres 0, 1, 2.... À partir de chaque entier naturel, on construit son successeur en ajoutant 1. Chaque entier naturel, à l'exception de 0, est donc successeur d'un entier naturel appelé prédécesseur de cet entier. Pour construire un ensemble contenant l'ensemble des entiers naturels mais où tout élément aurait un prédécesseur, on introduit l'ensemble $\mathbb{Z}$ des entiers relatifs. Il est constitué, en plus de tous les entiers naturels, des nombres -1 (le prédécesseur de 0), -2 (le prédécesseur de -1)... L'ensemble $\mathbb{D}$ des nombres décimaux est l'ensemble des nombres qui sont quotient d'un entier relatif par une puissance positive de 10. C'est l'ensemble des nombres qui ont un nombre fini de chiffres décimaux après la virgule. Par exemple, le nombre $-10,723$ s'écrit comme le quotient de -10723 par $10^3 = 1000$. Les entiers relatifs sont tous des nombres décimaux : tout entier relatif est en effet le quotient de lui même par $1 = 10^0$. En revanche, il existe des nombres décimaux qui ne sont pas entiers : $0,2$ est décimal puisqu'il est quotient de 2 par 10 mais il n'est pas entier puisqu'il est compris entre 0 et son successeur 1. L'ensemble $\mathbb{Q}$ des nombres rationnels est l'ensemble des nombres qui sont quotient d'un entier relatif par un entier naturel non nul. Le développement décimal des nombres rationnels est périodique à partir d'une certaine décimale : à partir d'une certaine décimale, le développement sera constitué d'une séquence de chiffres décimaux répétée indéfiniment. Le nombre $0,1234565656565656...$ est rationnel : la séquence répétée est 56. Ce nombre s'écrit aussi comme quotient de 61111 par 495000. Tout nombre décimal est rationnel. Mais il existe des nombres rationnels qui ne sont pas décimaux, par exemple $0,33333...$ n'est pas décimal (il a une infinité de décimales non nulles) mais il est rationnel (sa suite de décimales est constituée de la séquence 3 répétée indéfiniment). Si l'on multiplie $0,33333...$ par 3, on trouve $0,99999....$ Mais comme $0,33333...$ est le quotient de 1 par 3, en le multipliant par 3, on trouve 1. On a donc $1 = 0,99999...$ ce qui montre que l'écriture décimale d'un nombre n'est pas unique. On peut cependant prouver que cette écriture est unique si l'on remplace toutes les suites infinies de 9 par des suites infinies de 0 précédées de 1.

Une nouvelle espèce de nombres

Enfin, l'ensemble $\mathbb{R}$ des nombres réels est l'ensemble de tous les nombres possédant une écriture décimale. Tout nombre rationnel est réel mais le nombre

$$1,0100100010000100000100000010000000 1...$$

(chaque 1 du développement décimal est suivi d'un nombre de 0 égal au nombre de 0 le précédant augmenté de 1) est réel sans être rationnel.

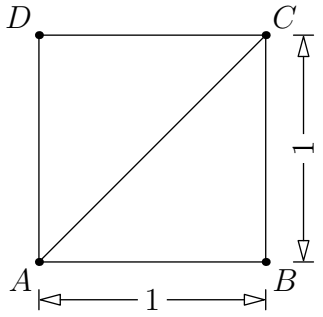

FIGURE 1. La diagonale du carré unité n'est pas de longueur rationnelle

Construisons un autre nombre réel non rationnel. Considérons un carré $ABCD$ de côté de longueur 1 (voir la figure 1). D'après l'égalité de Pythogore, le carré de la longueur de la diagonale AC vaut la somme des carrés des longueurs des côtés AB et BC, c'est-à-dire 2. La longueur de la diagonale est donc l'unique nombre réel positif dont le carré vaut 2. On note $\sqrt{2}$ ce nombre. Montrons qu'il n'est pas rationnel. Pour cela, on rappelle qu'un entier est pair s'il est le double d'un autre entier et impair sinon. Supposons que $\sqrt{2}$ est rationnel : on peut alors trouver deux entiers naturels non nuls a et b tels que $\sqrt{2} = \dfrac{a}{b}$. Si a et b sont tous les deux pairs, on écrit $a = 2a'$ et $b = 2b'$ de sorte que $\sqrt{2} = \dfrac{a'}{b'}$ est toujours quotient de deux entiers naturels. On répète ce procédé le nombre nécessaire de fois pour écrire $\sqrt{2} = \dfrac{r}{s}$ avec r et s deux entiers naturels dont l'un au moins est impair. On a alors $2s^2 = r^2$. On en déduit que r^2 puis que r est pair (le produit de deux nombres impairs est en effet impair). On a donc $r = 2r'$ puis $2s^2 = 4r'^2$ et $s^2 = 2r'^2$. On en déduit que s^2 est pair puis que s est pair. On obtient la contradiction que r et s sont tous deux pairs. Il en résulte que $\sqrt{2}$ ne peut pas s'écrire comme quotient de deux entiers : ce n'est pas un nombre rationnel.

Les nombres premiers

Considérons l'entier naturel 12. On peut l'écrire comme produit de deux entiers naturels de diverses façons :

$$12 = 1 \cdot 12$$
$$12 = 2 \cdot 6$$
$$12 = 3 \cdot 4.$$

On dit que les entiers naturels 1, 2, 3, 4, 6 et 12 sont des diviseurs de 12 ou encore que 12 est divisible par 1, par 2, par 3, par 4, par 6 et par 12. Plus généralement, si n et d sont deux entiers naturels, on dit que d divise n, ou encore que n est divisible par d s'il existe un entier naturel q tel que $n = qd$. L'entier 0 est divisible par tous les entiers naturels. L'entier 1 n'est divisible que par 1. Tout entier naturel au moins égal à deux est divisible par au moins deux nombres entiers : 1 et lui-même. Des nombres proches peuvent avoir des nombres de diviseurs très différents. Par exemple, le nombre 200560490130 a 2048 diviseurs alors que son successeur 200560490131 n'a que deux diviseurs.

Définition: nombre premier

Un entier naturel est premier *s'il a exactement deux diviseurs.*

Dans tout ce texte, on notera $\mathcal{P}$ l'ensemble des nombres premiers.

L'entier 2 est premier. L'entier 3 aussi puisque 2 ne divise pas 3 : en effet $2 \cdot 1 = 1 < 2$ et $2 \cdot k \geq 4 > 3$ si $k \geq 2$. De cette façon, le lecteur se convaincra que les nombres premiers inférieurs à 20 sont 2, 3, 5, 7, 11, 13, 17 et 19. Il est difficile, parce que long, de montrer que de très grands nombres sont premiers. Au 25 décembre 2013, le plus grand nombre premier est $2^{57885161} - 1$. Ce nombre s'écrit à l'aide de 17425170 chiffres.

La méthode dite du *crible d'Eratosthène* permet de trouver tous les nombres premiers inférieurs à un nombre premier fixé N. Cette méthode consiste à cocher, dans une table qui contient tous les entiers naturels non nuls inférieurs à N, tous les nombres qui ne sont pas premiers. L'algorithme est donné page suivante.

Le crible d'Eratosthène programmé diffère légèrement de celui décrit en utilisant le fait que si un entier n doit être coché, alors il s'écrit $n = ab$ avec $1 < a \leq \sqrt{n}$. Il a donc été coché comme multiple d'un nombre inférieur à $\sqrt{n}$.

En mettant en œuvre l'algorithme d'Eratosthène, on trouve rapidement à la main la liste des nombres premiers jusqu'à 100 :

$$\{p \in \mathcal{P} : p \leq 100\} = \\ \{2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97\}.$$

Proposition: diviseur premier d'un entier

Tout entier naturel supérieur à 2 admet un diviseur premier.

Démonstration. Soit $n \geq 2$ un entier naturel.

- Si n est premier, il admet un diviseur premier : lui ;
- Sinon, il existe un entier naturel $d_1 \geq 2$ différent de n tel que d_1 divise n.
  - Si d_1 est premier, il admet un diviseur premier : lui et on a donc trouvé un diviseur premier de n (c'est d_1) ;
  - Sinon, il existe $d_2 \geq 2$ différent de d_1 tel que d_2 divise d_1 (et donc n). On applique l'étape précédente en remplaçant d_1 par d_2 ;
  - On construit ainsi une suite d'entiers d_1, d_2, . . . ,d_k telle que $2 \leq d_k < ... < d_2 < d_1 < n$;
  - Tant qu'un diviseur d_i est non premier, on peut construire un diviseur d_{i+1} ;
  - Puisqu'il n'y a que $n - 2$ places possibles pour ces diviseurs, le procédé finit par s'arrêter et fournir un diviseur premier.

□

Existe-t-il une infinité de nombres premiers ?

L'ensemble des entiers naturels est infini. Quel est le sens de cette affirmation ? Considérez n'importe quelle ensemble fini d'entiers naturels. Il est toujours possible de trouver

Algorithme: crible d'Eratosthène

Entrée – *Un entier naturel $N \geq 2$.*
Sortie – *La liste des nombres premiers inférieurs ou égaux à N.*
Description – *Cocher l'entier 1 puis répéter les opérations suivantes tant qu'il existe des nombres qui ne sont ni soulignés ni cochés :*

- *trouver le plus petit nombre de la table, p qui n'est ni souligné ni coché ;*
- *souligner ce nombre ;*
- *cocher tous les nombres de la table qui sont produit de p par un entier supérieur à 2.*

Les nombres premiers sont tous les nombres soulignés.
Programmation –

```
EstPremier[1] ← 0          ▷ EstPremier contiendra 1 en place i si i est premier
for i ← 2, N do                                                  ▷ Initialisation
    EstPremier[i] ← 1
end for
p ← 2
while p^2 < N do
    j ← 2p
    while j ≤ N do                                   ▷ Élimination des multiples
        EstPremier[j] ← 0
        j ← j + p
    end while
    repeat                                          ▷ Le plus petit ni souligné ni barré
        p ← p + 1
    until EstPremier[p]=1
end while
j ← 0                                          ▷ Construction de la liste des premiers
for i ← 1, N do
    if EstPremier[i]=1 then
        j ← j + 1
        ListePremiers[j] ← i
    end if
end for
return ListePremiers
```

un entier naturel qui n'est pas dans cette liste. Comment ? Il suffit de rechercher le plus grand élément de l'ensemble fini et de lui ajouter un.

L'ensemble des nombres premiers est-il fini ou infini ? Autrement dit, considérant un ensemble quelconque fini de nombres premiers, est-il possible de trouver un nombre premier qui n'est pas dans cet ensemble ? La réponse est plus délicate que pour les entiers naturels car il est difficile de trouver le successeur premier d'un nombre premier. À ce moment du texte, on ne sait même pas encore que ce successeur premier existe ! Considérons un ensemble fini de nombres premiers. On note $p_1 < p_2 < \ldots < p_\omega$ les nombres

premiers de cet ensemble. On construit l'entier naturel

$$N = p_1 p_2 \cdots p_\omega + 1.$$

Si p_1 divise N, il existe un entier naturel k_1 tel que $N = p_1 k_1$. On a alors

$$p_1 k_1 = p_1 p_2 \cdots p_\omega + 1$$

puis

$$1 = p_1(k_1 - p_2 \cdots p_\omega).$$

C'est impossible puisque $p_1 \neq 1$. Le même raisonnement montre qu'aucun des nombres premiers $p_1, \ldots, p_\omega$ ne divise N. Mais l'entier naturel N admet un diviseur premier : il existe donc un nombre premier qui n'est pas dans l'ensemble $\{p_1, \ldots, p_\omega\}$.

Théorème 1: Euclide

Il existe une infinité de nombres premiers.

Comment les nombres sont-ils répartis ?

Les nombres pairs sont régulièrement répartis parmi les entiers naturels. Il y a 6 entiers pairs inférieurs ou égaux à 10, il y en a 51 inférieurs à 100 et 501 inférieurs à 1000. Plus généralement, si $x \geq 1$ est réel, le nombre d'entiers pairs inférieurs ou égaux à x est $1 + \lfloor x/2 \rfloor$ où $\lfloor x/2 \rfloor$ est le plus grand entier inférieur ou égal $x/2$. Si x est de plus en plus grand, la proportion de nombres pairs se rapproche de $1/2$. On dit que la proportion asymptotique des nombres pairs est $1/2$, on écrit :

$$\lim_{x \to +\infty} \frac{\#\{n \in \mathbb{N} \colon n \leq x \text{ et } n \text{ est pair}\}}{\#\{n \in \mathbb{N} \colon n \leq x\}} = \frac{1}{2}.$$

En revanche, les puissances de 10 sont rares. Il y en a 2 inférieures ou égales à 10 : 1 et 10. Il y en a 3 inférieures ou égales à 100 : 1, 10 et 100. Il y en a 4 inférieures ou égales à 1000. Pour décrire le nombre de puissances de 10 inférieurs ou égales à un réel $x \geq 1$, on introduit la fonction logarithme décimale log. Le graphe de cette fonction est donné figure 2 page suivante. Elle est définie sur l'ensemble $\mathbb{R}^{+*}$ des réels strictement positifs, est strictement croissante, s'annule en 1 et prend la valeur 1 en 10. Si a et b sont deux réels strictement positifs, on a

$$\log(ab) = \log(a) + \log(b).$$

En particulier, pour tout réel x strictement positif, on a

$$\log(10x) - \log(x) = \log(10) = 1.$$

Enfin, si n est entier naturel et x réel strictement positif, l'inéquation $10^n \leq x$ équivaut à $n \leq \log x$. On obtient alors que la proportion de puissances de 10 inférieures à un réel $x \geq 1$ est

$$\frac{\#\{n \in \mathbb{N} \colon 10^n \leq x\}}{\#\{m \in \mathbb{N} \colon m \leq x\}} = \frac{\lfloor \log x \rfloor}{\lfloor x \rfloor} + \frac{1}{\lfloor x \rfloor}.$$

La proportion asymptotique est donc de l'ordre de $\lfloor \log x \rfloor / \lfloor x \rfloor$ et en particulier,

$$\lim_{x \to +\infty} \frac{\#\{n \in \mathbb{N} \colon 10^n \leq x\}}{\#\{m \in \mathbb{N} \colon m \leq x\}} = 0.$$

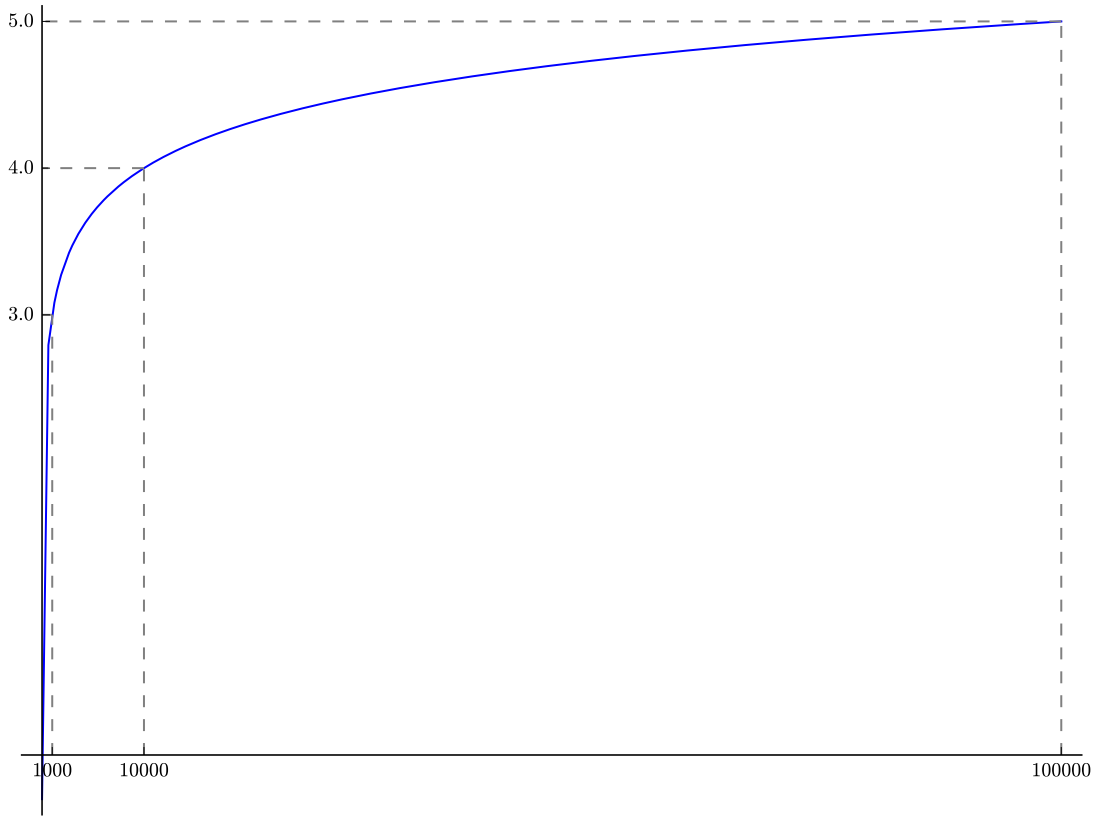

FIGURE 2. Graphe du logarithme décimal

Les exemples des entiers pairs et des puissances de 10 montrent que les éléments d'une suite infinie peuvent être plus ou moins rares, plus ou moins bien répartis parmi les entiers naturels. C'est cette répartition que nous voulons étudier pour les nombres premiers.

Une expérience

Pour commencer une étude expérimentale, nous utilisons le crible d'Eratosthène pour compter le nombre de nombres premiers inférieurs à la suite des puissances de 10. Les résultats sont donnés table 1 page suivante.

Nous calculons ensuite la proportion des nombres premiers inférieurs à une puissance de 10 donnée, puis l'inverse de cette proportion et enfin les écarts entre ces proportions. Les résultats sont donnés table 2 page ci-contre. Notons $P(x)$ la proportion de nombres premiers inférieurs à x. On a donc

$$P(x) = \frac{\#\{p \in \mathcal{P} \colon p \leq x\}}{\lfloor x \rfloor}.$$

x	Premiers inférieurs à x
100	25
1 000	168
10 000	1 229
100 000	9 592
1 000 000	78 498
10 000 000	664 579
100 000 000	5 761 455

TABLE 1. Décompte des nombres premiers

x	Premiers inférieurs à x	Proportion $P(x)$	$1/P(x)$	$1/P(10x) - 1/P(x)$
100	25	$0,25$	4	
1 000	168	$0,17$	$5,95$	$1,95$
10 000	1 229	$0,12$	$8,14$	$2,18$
100 000	9 592	$0,1$	$10,43$	$2,29$
1 000 000	78 498	$0,08$	$12,74$	$2,31$
10 000 000	664 579	$0,07$	$15,05$	$2,31$
100 000 000	5 761 455	$0,06$	$17,36$	$2,31$

TABLE 2. Répartition des nombres premiers

Une conjecture du jeune Gauss

À la lecture de la table 1, il semble que x devenant grand, la différence

$$\frac{1}{P(10x)} - \frac{1}{P(x)}$$

se rapproche d'une constante dont le début du développement décimal est $2,31$.

Il existe une fonction très proche de la fonction log précédemment rencontrée satisfaisant à cette propriété. C'est la fonction logarithme népérien, notée ln. Elle est reliée à la fonction log par la relation

$$\ln(x) = \frac{\log(x)}{\log(e)}$$

où e est une constante mathématique, appelée constante de Neper, dont on obtient des valeurs de plus en plus approchées en calculant successivement les nombres

$$1,\ 1+\frac{1}{1},\ 1+\frac{1}{1}+\frac{1}{1\cdot 2}, 1+\frac{1}{1}+\frac{1}{1\cdot 2}+\frac{1}{1\cdot 2\cdot 3}, 1+\frac{1}{1}+\frac{1}{1\cdot 2}+\frac{1}{1\cdot 2\cdot 3}+\frac{1}{1\cdot 2\cdot 3\cdot 4}, \ldots$$

En calculant

$$1+\frac{1}{1}+\frac{1}{1\cdot 2}+\frac{1}{1\cdot 2\cdot 3}+\frac{1}{1\cdot 2\cdot 3\cdot 4}+\cdots+\frac{1}{1\cdot 2\cdot 3\cdot 4\cdots 100}$$

on trouve qu'une valeur approchée de e est

$$e = 2,718281828459045235360287471352662497\ldots$$

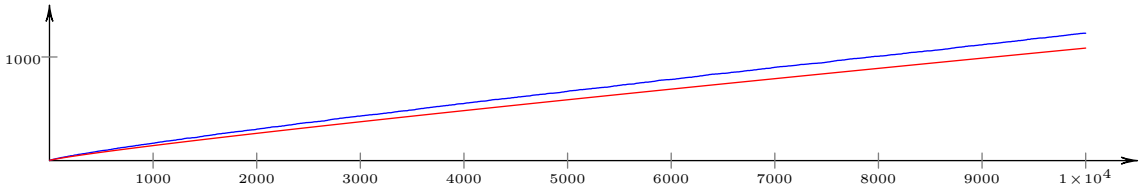

FIGURE 3. Approximation du jeune Gauss

Notre expérience suggère alors que

$$\frac{1}{P(x)} \approx \ln(x)$$

donc que la proportion de nombres premiers inférieurs à x est

$$\frac{\#\{n \in \mathbb{N} \colon n \leq x \text{ et } n \in \mathcal{P}\}}{\#\{n \in \mathbb{N} \colon n \leq x\}} \approx \frac{1}{\ln(x)}.$$

Cette conjecture[1] a été pensée par Gauss en 1792 alors qu'il était âgé de 15 ans.

Conjecture: Approximation du jeune Gauss

Lorsque x devient de plus en plus grand, le quotient de la proportion de nombres premiers inférieurs à x et de $1/\ln(x)$ se rapproche de 1 :

$$\frac{\#\{n \in \mathbb{N} \colon n \leq x \text{ et } n \in \mathcal{P}\}}{\#\{n \in \mathbb{N} \colon n \leq x\}} \sim \frac{1}{\ln(x)}.$$

Le jeune Gauss est-il précis ?

Pour tester la précision de l'approximation du jeune Gauss, on trace le graphe de la fonction de comptage des nombres premiers

$$x \mapsto \#\{n \in \mathbb{N} \colon n \leq x \text{ et } n \in \mathcal{P}\}$$

que l'on compare à

$$x \mapsto \frac{x}{\ln(x)}.$$

Pour chaque valeur du réel positif x, la fonction de comptage des nombres premiers prend pour valeur le nombre de nombres premiers inférieurs à x. Elle est donc constante entre chaque entier et son successeur, c'est une fonction en escalier. On trace le graphe de cette fonction (figure 3, courbe bleue) et on le compare au graphe de $x \mapsto x/\ln(x)$ (figure 3, courbe rouge). Quoique proches l'une de l'autre, il semble difficile de considérer que les courbes se rapprochent.[2]

Gauss a calculé des nombres premiers toute sa vie : *„Ich habe (da ich meiner anhaltendenden Abzählung der Reihe nach keine Gedult hatte) sehr oft einzelne unbeschäftigte*

1. Une conjecture est un énoncé mathématique non démontré mais suffisamment plausible pour constituer un défi intéressant. Un travail du mathématicien est de transformer les conjectures en théorèmes.

2. Cela n'empêche cependant pas que le rapport entre $\pi(x)$ et $x/\ln(x)$ se rapproche de 1 lorsque x est de plus en plus grand.

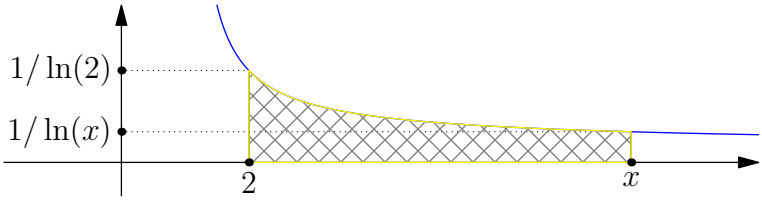

FIGURE 4. Aire sous la courbe

Viertelstunden verwandt, von bald hie bald dort eine Chiliade abzuzählen.“[3] Il a découvert une autre approximation du nombre de nombres premiers inférieurs à un réel donné. Nous commençons par énoncer cette approximation puis expliquerons son sens.

Conjecture: Approximation du vieux Gauss

Lorsque x devient de plus en plus grand, le nombre de nombres premiers inférieurs à x est bien approché par :

$$\int_2^x \frac{1}{\ln(t)}\,\mathrm{d}t$$

c'est-à-dire

$$\#\{n \in \mathbb{N} \colon n \leq x \text{ et } n \in \mathcal{P}\} \sim \int_2^x \frac{1}{\ln(t)}\,\mathrm{d}t.$$

Mesurons des surfaces

Expliquons le sens du symbole de droite. Le lecteur est invité à se reporter figure 4. Si x est un réel fixé supérieur à 2, on trace le graphe de la fonction $t \mapsto 1/\ln(t)$ (en bleu). On délimite ensuite un contour qui suit la partie de cette courbe formée des points d'abscisse comprise entre 2 et x, la droite verticale formée des points d'abscisse x, l'axe des abscisses et la droite verticale formée des points d'abscisse 2. Ce contour enferme une région hachurée en gris. Cette région a une surface que l'on note

$$\int_2^x \frac{1}{\ln(t)}\,\mathrm{d}t.$$

La conjecture du vieux Gauss exprime donc que le nombre des nombres premiers inférieurs à x est bien approché par l'aire enfermée par la courbe de $t \mapsto 1/\ln(t)$, les droites verticales formées des points d'abscisses 2 et x et l'axe horizontale formé des points d'ordonnée nulle.

Le vieux Gauss est-il précis ?

Pour simplifier l'écriture, on note désormais

$$\pi(x) = \#\{n \in \mathbb{N} \colon n \leq x \text{ et } n \in \mathcal{P}\}$$

3. « J'ai très souvent (parce que je n'ai pas la patience de calculer de façon continue) passé un quart d'heure inoccupé à calculer de ci de là un nouveau millier de nombres premiers »

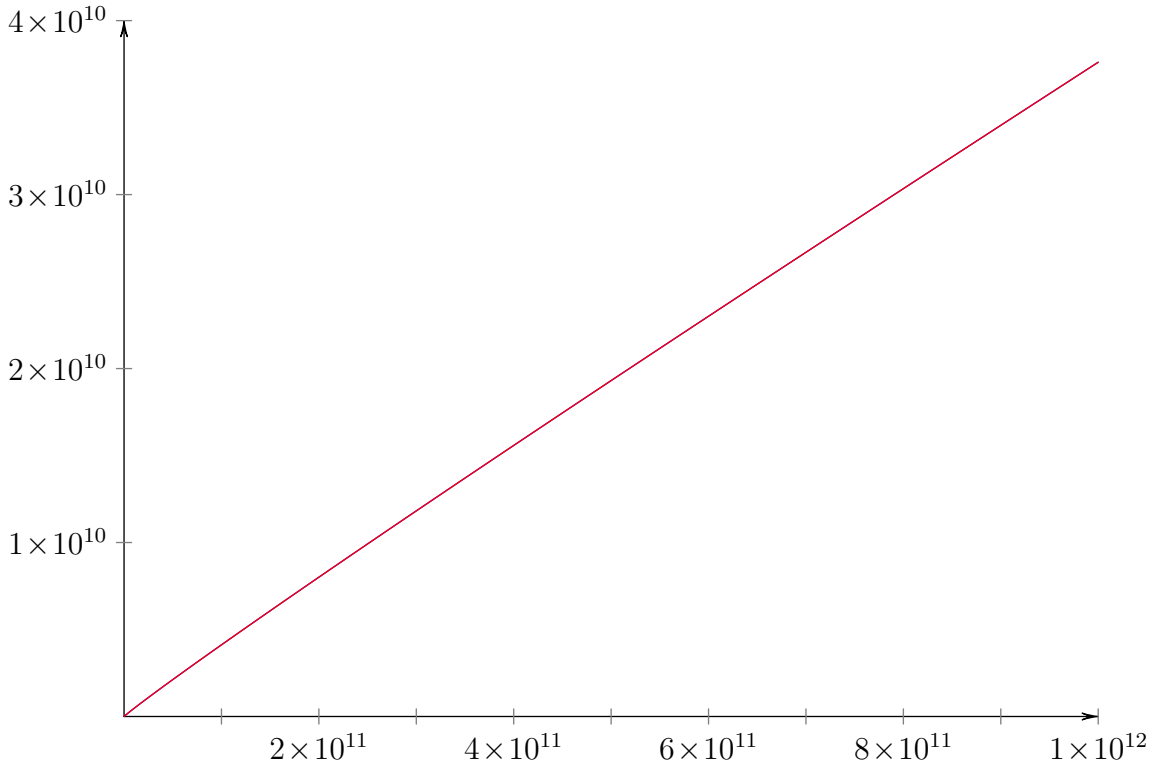

FIGURE 5. Approximation du vieux Gauss

et

$$\mathrm{Li}(x) = \int_2^x \frac{1}{\ln(t)}\,\mathrm{d}t.$$

Le graphe 5 montre que l'adéquation entre $\pi(x)$ et $\mathrm{Li}(x)$ est remarquable. Sur ce graphe, on a tracé la courbe de π en bleu et de Li en rouge. Á cette échelle, on ne note aucune différence entre les deux courbes. Expérimentalement, lorsque x est suffisamment grand, l'ordre de grandeur de la différence $\pi(x)-\mathrm{Li}(x)$, autrement dit l'erreur faite en remplaçant le nombre de nombres premiers inférieurs à x par $\mathrm{Li}(x)$ est proche de $\sqrt{x}$. C'est donc très petit puisque l'ordre de grandeur de $\mathrm{Li}(x)$ est $x/\ln(x)$. On met en valeur cette différence en traçant sur le graphe 6 page ci-contre la courbe de

$$\frac{\pi(x)-\mathrm{Li}(x)}{\sqrt{x}}.$$

Il faut remarquer qu'il y a des variations qui semblent très chaotiques. Cependant, l'erreur oscille très peu autour de $\sqrt{x}$. En effet, si on écrit $\pi(x)-\mathrm{Li}(x) = c(x)\sqrt{x}$, alors $c(x)$ varie entre $-0,06$ et $-0,02$ (intervalle de longueur $0,04$) alors que x varie entre $10^{12}-10^{11}$ et 10^{12} (intervalle de longueur 10^{11}).

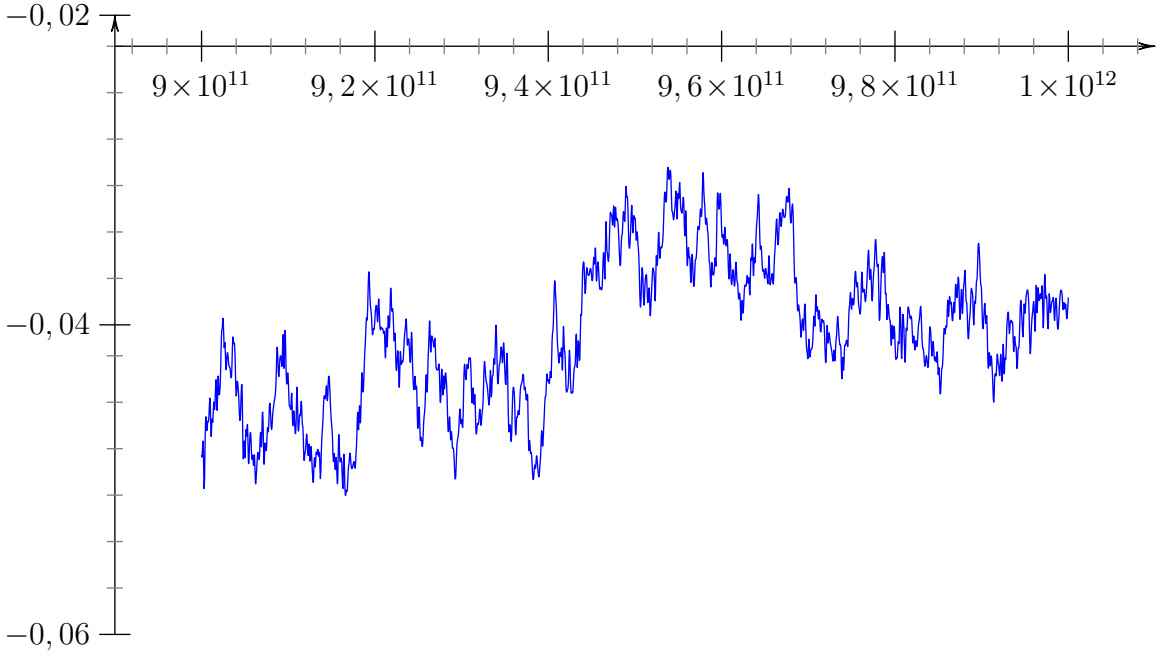

FIGURE 6. Écart normalisé entre π et Li

Il faut noter que les conjectures de Gauss ne sont pas incompatibles. La conjecture du vieux Gauss exprime en effet que

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

et la conjecture du jeune Gauss que

$$\lim_{x\to+\infty} \frac{\pi(x)}{x/\ln(x)} = 1.$$

Or on peut montrer que $x/\ln(x)$ est une approximation de Li. Plus précisément

$$\mathrm{Li}(x) = \frac{x}{\ln(x)}\,(1+\varepsilon(x))$$

où ε est une fonction qui tend vers 0 lorsque x tend vers $+\infty$.

Une somme infinie

Il a fallu beaucoup de temps à la communauté des mathématiciens pour démontrer les conjectures de Gauss. Un pas important a été accompli par Riemann. La description de ce pas nécessite quelques développements de mathématiques élémentaires. Pour tout entier N, on définit la somme

$$S_2(N) = \frac{1}{1^2} + \frac{1}{2^2} + \frac{1}{3^2} + \frac{1}{4^2} + \cdots + \frac{1}{N^2}$$

N	$S_2(N)$
1	1
2	$1,250000000$
3	$1,361111111$
4	$1,423611111$
100	$1,634983900$
1000	$1,643934567$
5000	$1,644734087$

TABLE 3. Valeurs de $S_2(N)$

qu'on note en abrégé

$$S_2(N) = \sum_{k=1}^{N} \frac{1}{k^2}.$$

Avec de la patience, ou avec un ordinateur, on calcule les valeurs de $S_2(N)$ pour N de plus en plus grand. Les résultats sont donnés dans le tableau 3.

On remarque que lorsque N devient de plus en plus grand, $S_2(N)$ se rapproche d'un nombre dont le début du développement est $1,64$. C'est une chose que l'on peut montrer rigoureusement. Lorsque N tend vers $+\infty$, la somme $S_2(N)$ admet une limite finie que l'on note $\zeta(2)$. On écrit

$$\sum_{k=1}^{+\infty} \frac{1}{k^2} = \zeta(2).$$

La somme de gauche est obtenue en sommant une infinité de nombres. Mais ces nombres sont suffisamment de plus en plus petits pour que leur somme soit un nombre réel. On peut donner la valeur du nombre $\zeta(2)$ en fonction π. Précisément,

$$\zeta(2) = \frac{\pi^2}{6}.$$

De la même façon, on pourrait calculer

$$S_3(N) = \sum_{k=1}^{N} \frac{1}{k^3}$$

pour des valeurs du N de plus en plus grandes. Le faisant, vous trouverez que $S_3(N)$ s'approche d'un nombre réel dont le début du développement décimal est $1,202056$. On peut montrer rigoureusement que la somme $S_3(N)$ admet une limite finie que l'on note $\zeta(3)$. On écrit

$$\sum_{k=1}^{+\infty} \frac{1}{k^3} = \zeta(3).$$

On ne connaît pas d'expression de $\zeta(3)$ en fonction de constantes mathématiques usuelles telles que π ou e. Si on remplaçait 3 par 4, on aurait un résultat semblable. De façon

N	$S_1(N)$
1	1
10	$2,928968$
100	$5,187377$
1000	$7,485470$
10000	$9,787606$
100000	12.090146
1000000	14.392726

TABLE 4. Valeurs de $S_1(N)$

plus générale, si n est un entier valant au moins 2 et si

$$S_n(N) = \sum_{k=1}^{N} \frac{1}{k^n},$$

alors, la somme $S_n(N)$ admet une limite finie que l'on note $\zeta(n)$.

Cela marche-t-il toujours ?

Et si on calcule juste la somme des inverses des entiers ? Autrement dit, calculons

$$S_1(N) = \sum_{k=1}^{N} \frac{1}{k}$$

pour N de plus en plus grand. Les résultats sont donnés dans le tableau 4.

Les valeurs obtenues sont de plus en plus grandes ! Il ne semble pas que la somme $S_1(N)$ s'approche d'un nombre réel lorsque N devient de plus en plus grand. Là encore, c'est une chose que l'on peut démontrer rigoureusement : choisissez n'importe quel réel X, il existe un entier M tel que, pour tous les entiers $N \geq M$ on a $S_1(N) \geq X$. On dit que $S_1(N)$ tend vers $+\infty$. Pour le moment, on ne sait donc définir des nombres $\zeta(n)$ que pour les entiers n valant au moins 2.

Des exposants réels

Un entier non nul élevé à la puissance 0 vaut toujours 1. La somme

$$S_0(N) = \sum_{k=1}^{N} \frac{1}{k^0}$$

est une somme de N nombres 1, elle est égale à N. Cette somme tend elle aussi vers $+\infty$.

Il existe une fonction, notée ζ qu'on peut calculer pour tous les nombres réels sauf 1, qui pour tout entier naturel $n \geq 2$, prend la valeur

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

et dont les propriétés traduisent une grande régularité. Les graphes 7 page suivante et 8 page suivante représentent une partie de cette fonction. Nous décrivons cette fonction pour les réels $x > 1$. Si t est un réel, il existe un unique réel y qui vérifie $\ln(y) = t$. Ce réel

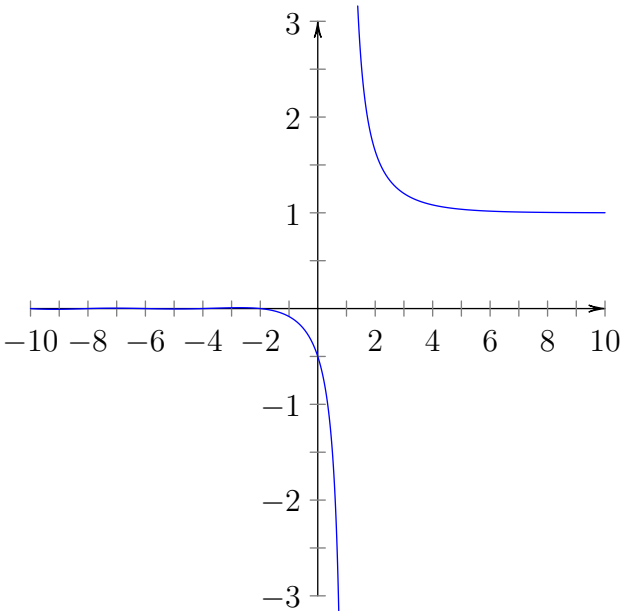

FIGURE 7. La fonction ζ

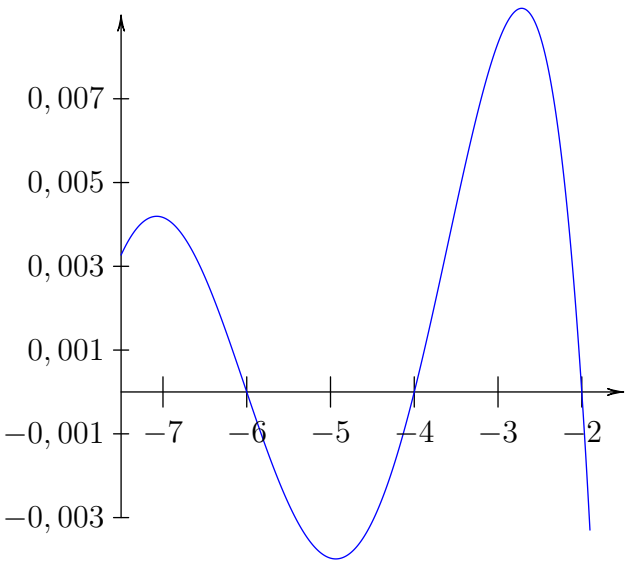

FIGURE 8. La fonction ζ

est noté $y = \exp(t)$. On a donc $\exp(\ln(y)) = \exp(t)$ et donc $\exp(\ln(y)) = y$. D'autre part, si t et t' sont deux nombres réels, alors $\exp(t + t') = \exp(t) \cdot \exp(t')$. En prenant $t = t'$, on trouve $\exp(2t) = \exp(t)^2$. Puis en choisissant $t' = 2t$, on trouve $\exp(3t) = \exp(t)^3$. On réitère ce procédé et, pour tout entier naturel $n \geq 1$, on obtient $\exp(nt) = \exp(t)^n$. Si a

est un réel strictement positif et $n \geq 1$ un entier, on calcule alors

$$\exp(n\ln(a)) = \exp(\ln(a))^n = a^n.$$

On utilise cette propriété pour définir les puissances réels. Si $a > 0$ est un réel, si x est un réel, on définit a^x en posant

$$a^x = \exp(x\ln(a)).$$

Grâce à cette extension, on définit (après avoir montré que la somme infinie tend vers un nombre réel) $\zeta(x)$ pour tout réel $x > 1$ par

$$\zeta(x) = \sum_{k=1}^{+\infty} \frac{1}{k^x}. \tag{1}$$

Et ailleurs ?

On peut alors décrire une méthode de calcul de ζ pour tous les réels négatifs. Là encore, nous devons décrire une fonction usuelle de l'analyse mathématique. Si t est un réel, strictement supérieur à 1, on sait montrer que le quotient

$$\frac{n!n^t}{t(t+1)(t+2)\cdots(t+n)}$$

se rapproche d'un réel lorsque n devient de plus en plus grand. On note $\Gamma(t)$ ce réel, de sorte que

$$\Gamma(t) = \lim_{n\to+\infty} \frac{n!n^t}{t(t+1)(t+2)\cdots(t+n)}.$$

Si maintenant x est un réel strictement négatif, alors $1-x$ est un réel strictement supérieur à 1, et on a

$$\zeta(x) = 2^x\pi^{x-1}\sin\left(\frac{\pi x}{2}\right)\Gamma(1-x)\zeta(1-x). \tag{2}$$

Comme on sait calculer $\Gamma(2) = 1$ et $\zeta(2) = \pi^2/6$, cette formule permet par exemple de trouver

$$\zeta(-1) = -\frac{1}{12}.$$

On décrit enfin le calcul de $\zeta(x)$ lorsque x est un réel positif et strictement inférieur à 1. Si t est un réel positif, on note $\{t\}$ sa partie fractionnaire. Pour $x = 0$, on a

$$\zeta(0) = -\frac{1}{2}.$$

Pour x fixé dans $]0,1[$, on considère le graphe de la fonction $t \mapsto \{t\}t^{-x-1}$ (la figure 9 page suivante représente le graphe de cette fonction pour $x = 1/2$). Ce graphe est formé de « dents » appuyées sur l'axe des abscisses et chaque dent a une surface. Si $N \geq 1$ est entier, on calcule la somme des surfaces des $N-1$ premières dents (celles qui sont hachurées sur la figure). On montre que, lorsque N devient de plus en plus grand, cette somme des surfaces des dents s'approche de plus en plus d'un nombre réel que l'on note

$$\int_1^{+\infty} \{t\}t^{-x-1}\,\mathrm{d}t.$$

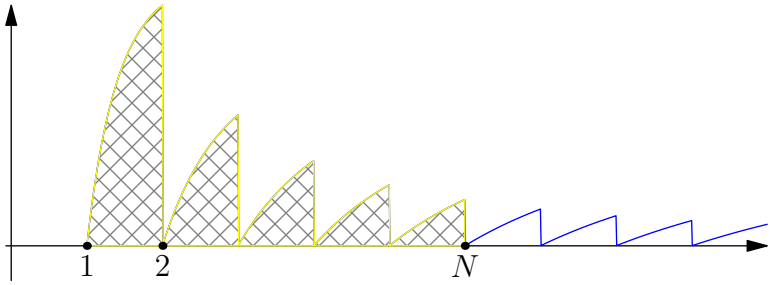

FIGURE 9. La fonction $t \mapsto \{t\}t^{-x-1}$ (pour $x = 1/2$)

Pour tout réel $x > 0$, on pose alors

$$\zeta(x) = \frac{x}{x-1} + x \int_1^{+\infty} \{t\}t^{-x-1}\,\mathrm{d}t.$$

Si $x > 1$, cette formule donne la même valeur que (1). C'en est donc un prolongement.[4]

On dispose donc d'une formule de calcul de $\zeta(x)$ pour tout réel $x \neq 1$. La formule (2) est valable pour tout $x \neq 1$. Elle porte le nom d'*équation fonctionnelle* de ζ.

Quel rapport avec les nombres premiers ?

Arrivé à ce point, le lecteur est peut-être fasciné par les propriétés de cette étonnante fonction ζ, mais se demande bien le rapport avec les nombres premiers. Notons $p_1 = 2$, $p_2 = 3$, $p_3 = 5$ etc. la suite croissante des nombres premiers. Tout nombre entier n s'écrit sous la forme

$$n = p_1^{v_1} p_2^{v_2} \cdots p_\omega^{v_\omega}$$

où v_1, v_2,...,v_ω sont des entiers naturels et p_ω est la plus grand diviseur premier de n. C'est la décomposition en facteur premier de n. Par exemple,

$$452540 = 2^2 \cdot 3^0 \cdot 5^1 \cdot 7^0 \cdot 11^3 \cdot 13^0 \cdot 17^1.$$

Lorsque l'on fait le produit

$$\left(1 + \frac{1}{p_1} + \frac{1}{p_1^2} + \frac{1}{p_1^3} + \cdots\right) \times \left(1 + \frac{1}{p_2} + \frac{1}{p_2^2} + \frac{1}{p_2^3} + \cdots\right) \times \left(1 + \frac{1}{p_3} + \frac{1}{p_3^2} + \frac{1}{p_3^3} + \cdots\right) \times \ldots$$

on trouve donc, formellement, la somme de tous les inverses des entiers

$$1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \frac{1}{5} + \ldots$$

4. On pourrait prolonger ζ à peu près n'importe comment. Pourquoi donc ce prolongement et pas un autre ? Répondre rigoureusement dépasse largement le cadre de ce texte. Nous nous contentons donc de dire que c'est le seul qui donne à ζ un comportement suffisamment régulier et riche de propriétés.

Cela ne peut pas être rendu rigoureux puisque l'on a vu que cette somme n'était pas un nombre réel. En revanche, si l'on fait le produit

$$\left(1+\frac{1}{p_1^2}+\frac{1}{(p_1^2)^2}+\frac{1}{(p_1^2)^3}+\cdots\right)\times\left(1+\frac{1}{p_2^2}+\frac{1}{(p_2^2)^2}+\frac{1}{(p_2^2)^3}+\cdots\right)\times \\ \left(1+\frac{1}{p_3^2}+\frac{1}{(p_3^2)^2}+\frac{1}{(p_3^2)^3}+\cdots\right)\times\ldots$$

on trouve donc, formellement, la somme des tous les inverses des carrées des entiers. Cette somme infinie est le nombre réel

$$\sum_{n=1}^{+\infty}\frac{1}{n^2}=\zeta(2).$$

Par ailleurs, pour tout $X>1$, en multipliant

$$1+\frac{1}{X}+\frac{1}{X^2}+\frac{1}{X^3}+\cdots$$

par $1-X$, on trouve

$$1+\frac{1}{X}+\frac{1}{X^2}+\frac{1}{X^3}+\cdots-\left(X+1+\frac{1}{X}+\frac{1}{X^2}+\cdots\right)=-X.$$

On a alors

$$1+\frac{1}{X}+\frac{1}{X^2}+\frac{1}{X^3}+\cdots=\frac{-X}{1-X}=\frac{1}{1-1/X}$$

et donc

$$\left(1+\frac{1}{p_1^2}+\frac{1}{(p_1^2)^2}+\frac{1}{(p_1^2)^3}+\cdots\right)=\frac{1}{1-\frac{1}{p_1^2}}.$$

Comme cela reste vrai pour tous les nombres premiers, on a

$$\prod_{p\in\mathcal{P}}\frac{1}{1-1/p^2}=\sum_{n=1}^{+\infty}\frac{1}{n^2}.$$

Le réel $\zeta(2)$ peut être calculé en faisant le produit, sur tous les nombres premiers p, des facteurs $1-1/p^2$.

Ce procédé s'adapte à toutes les valeurs de $\zeta(x)$ pour $x>1$:

$$\zeta(x)=\prod_{p\in\mathcal{P}}\frac{1}{1-1/p^x}.$$

Cette formule confirme que l'ensemble $\mathcal{P}$ des nombres premiers est infini. S'il était fini, alors on pourrait calculer

$$\prod_{p\in\mathcal{P}}\frac{1}{1-1/p}$$

en faisant un nombre fini de multiplications et on trouverait que ce produit vaut la somme des inverses de tous les entiers. Or, on a vu que cette somme n'existe pas.

Cela suggère que connaître ζ autour de 1 pourrait fournir des informations sur les nombres premiers. Autour de 1, dans les nombres réels, c'est sur un intervalle contenant 1. Pour augmenter cet « autour de 1 », Riemann a eu l'idée formidable de non pas regarder

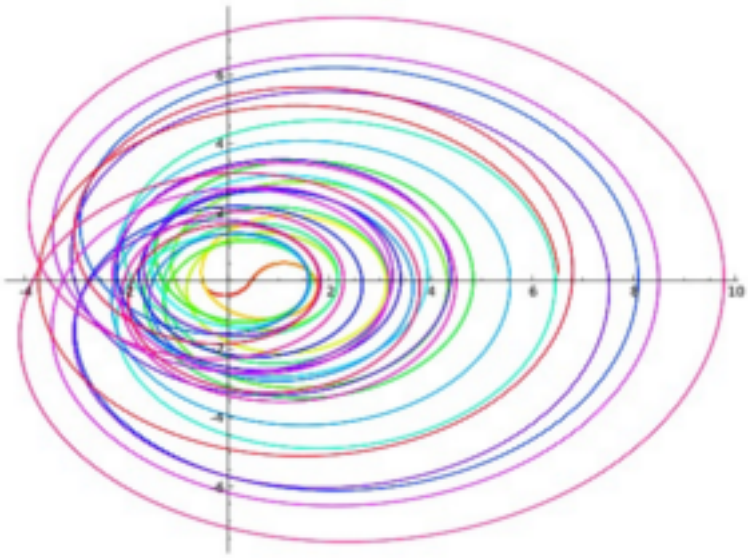

FIGURE 10. Représentation de $\zeta(0, y)$

autour de 1 dans les nombres réels mais dans le plan ! C'est-à-dire autour du point de coordonnées $(1, 0)$. Cette idée nécessite de définir ζ non pas seulement pour les nombres réels, ce qui nous a déjà coûté beaucoup de temps, mais pour tous les points du plan,[5] c'est-à-dire pour tous les couples de réels ! Nous n'allons pas le faire, c'est au delà de l'ambition de ce texte. Disons simplement, que grâce à Riemann, on sait calculer $\zeta(x, y)$ pour tous les couples de réels (x, y) sauf pour $(1, 0)$ et que, si $y = 0$ alors $\zeta(x, y) = \zeta(x)$. Ce que l'on obtient n'est en général plus un réel mais un couple de réel. Autrement dit, ζ est maintenant un application qui transforme un point du plan en un autre point du plan. À défaut de donner une définition, présentons des représentations graphiques qui peuvent aider à appréhender ζ.

Beaucoup de courbes pour décrire une seule fonction

On commence par donner des représentations statiques de $\zeta(x, y)$ pour des valeurs fixes de x et des valeurs de y variant entre 0 et 100. Commençons par $\zeta(0, y)$. Pour chaque valeur de y, $\zeta(0, y)$ est représenté par un point du plan. Lorsque y varie de 0 à 100 nous obtenons donc une infinité de points (un pour chaque valeur réelle de y) qui forment une courbe. Cette courbe est représentée figure 10.

Pour garder mémoire de la valeur de y qui donne le point $\zeta(0, y)$, on a colorié les points en fonction de y à l'aide de l'échelle de couleur (figure 11 page suivante). Le point $\zeta(0, 0)$ est ainsi en rouge, c'est le point de départ de notre courbe au point de coordonnées $(-1/2, 0)$. On remarque que la courbe ne passe pas par le point d'intersection des deux axes : cela traduit le fait que, pour toutes les valeurs de y représentées, on a $\zeta(0, y) \neq 0$.

5. En réalité, Riemann a défini ζ sur les nombres complexes. L'ensemble des nombres complexes peut être vu comme l'ensemble des points du plan que l'on sait additionner et multiplier entre eux. Voir par exemple `http://www.dimensions-math.org/Dim_CH5.htm` ou `http://www.youtube.com/watch?v=2GwSUDm_Rg8`

FIGURE 11. Échelle de couleurs

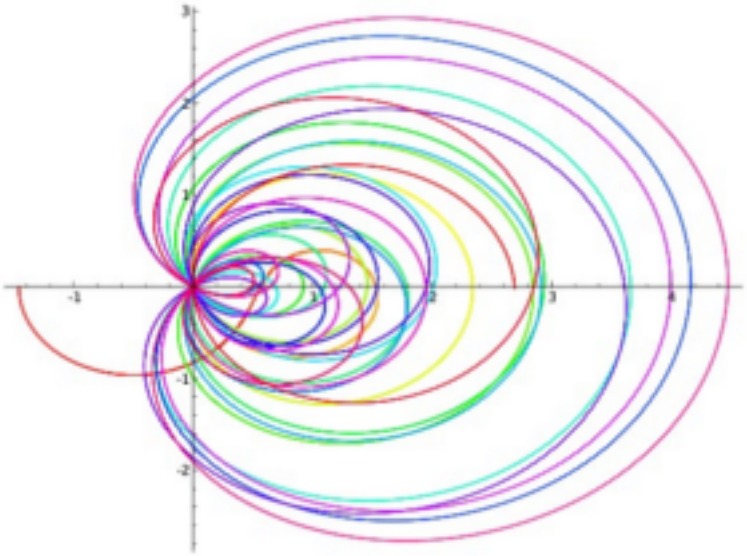

FIGURE 12. Représentation de $\zeta(1/2, y)$

De la même façon, la figure 12 représente les valeurs de $\zeta(1/2, y)$ pour y variant de 0 à 100. Cette fois la courbe passe plusieurs fois à l'intersection des deux axes : il existe plusieurs valeurs de y pour lesquelles $\zeta(1/2, y) = 0$.

Enfin, la figure 13 page suivante représente les valeurs de $\zeta(0,95, y)$ pour y variant de 0 à 100. Elle montre que pour toutes les valeurs de y entre 0 et 100, on a $\zeta(0,95, y) \neq 0$.

Un défi transmis par Riemann

En construisant les images relatives à $\zeta(x, y)$ pour suffisamment de valeurs de x dans l'intervalle $]0, 1[$, on obtient un film que le lecteur est invité à consulté sur internet.[6,7] La visualisation de ce film laisse penser que, la seule valeur de x dans l'intervalle $]0, 1[$ pour laquelle existe y tel que $\zeta(x, y) = 0$ est $x = 1/2$. La démonstration rigoureuse de ce fait est un grand défi du XXIe siècle bien que ceci fut conjecturé en 1859 par Riemann.

Conjecture: Conjecture de Riemann

Soit x un réel de l'intervalle $]0, 1[$. S'il existe un réel y tel que $\zeta(x, y) = 0$, alors $x = \frac{1}{2}$.

6. http://www.youtube.com/watch?v=zpnt3EnOivw
7. http://www.youtube.com/watch?v=DSORQnePi8U

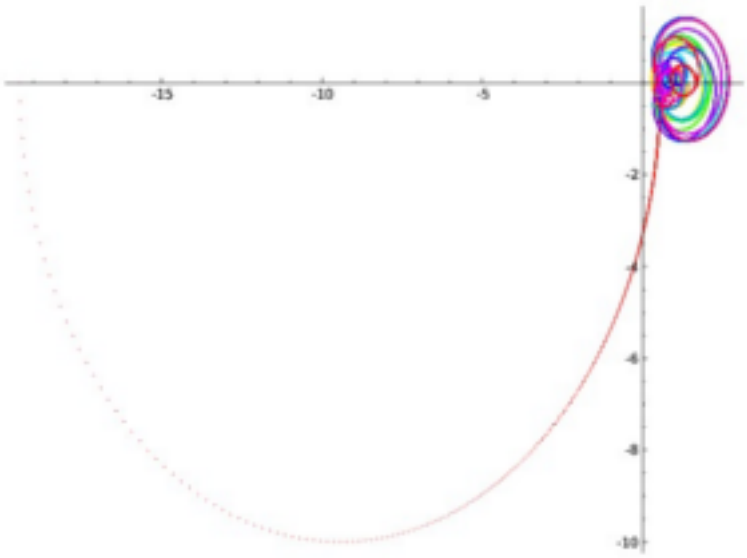

FIGURE 13. Représentation de $\zeta(0,95,y)$

Le théorème des nombres premiers

Très peu de choses sont connues en direction de cette hypothèse. Il s'agit de démontrer que, dans la bande délimitée par les droites verticales formées des points d'abscisse 0 et 1, la fonction ζ ne s'annule que sur la droite verticale formée des points d'abscisses 1/2. La seule chose que l'on sait montrer est que la fonction ζ ne s'annule pas dans une région située à droite d'une courbe, elle même située à gauche de la droite verticale des points d'abscisses 1 mais qui s'en rapproche de plus en plus (voir la figure 14 page ci-contre.[8]). En 1899, de la Vallée Poussin a démontré que si $x \in]0,1]$ et $y \neq 0$ vérifient

$$1 - x \leq \frac{c}{\ln|y|}$$

(pour une constante $c > 0$) alors $\zeta(x,y) \neq 0$. D'autre part, $\zeta(x,y) \neq 0$ si $|y| \leq 5$.

Si ce résultat peut sembler ridicule par rapport à la conjecture de Riemann, il est cependant à la base de la démonstration par Hadamard et de la Vallée Poussin de la conjecture du vieux Gauss.

8. Le bord gauche du graphe est en réalité très proche de 1

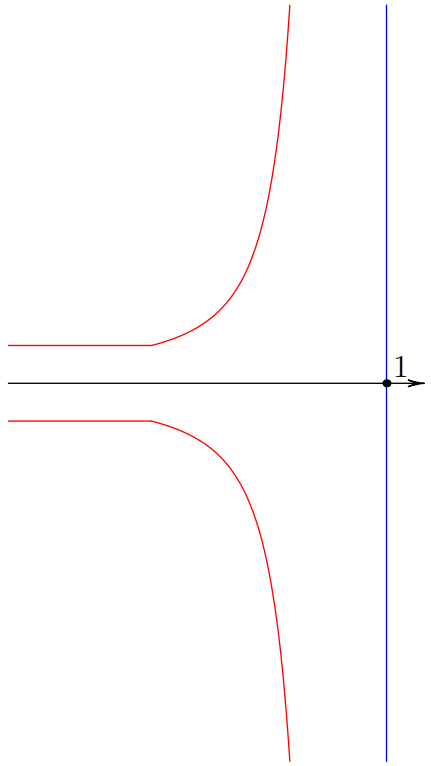

FIGURE 14. Région sans zéro de ζ

Théorème 2: Théorème des nombres premiers

Il existe des constantes $K_1 > 0$ et K_2 telles que, pour tout réel x, le nombre de nombres premiers inférieurs à x est donné par $\mathrm{Li}(x)$ avec une erreur inférieure à $K_1 \exp\left(-K_2\sqrt{\ln(x)}\right)$:

$$\left|\pi(x) - \int_2^x \frac{\mathrm{d}t}{\ln t}\right| \leq K_1 \exp\left(-K_2\sqrt{\ln(x)}\right).$$

Cet énoncé n'est intéressant que parce qu'on peut montrer que lorsque x devient grand, le terme d'erreur devient très petit relativement à

$$\mathrm{Li}(x) = \int_2^x \frac{\mathrm{d}t}{\ln(t)}.$$

Et si l'on savait résoudre le défi de Riemann ?

Plus la région où ζ ne s'annule pas est grande, plus précis est le terme d'erreur. En particulier, si l'hypothèse de Riemann était démontrée, on pourrait en déduire le résultat suivant.

Théorème 3: Théorème des nombres premiers conditionnel

Supposons vraie l'hypothèse de Riemann. Pour tout réel $x \geq 3000$, le nombre de nombres premiers inférieurs à x est donné par $\mathrm{Li}(x)$ *avec une erreur inférieure à* $\sqrt{x}\ln(x)$ *:*

$$\left|\pi(x) - \int_2^x \frac{\mathrm{d}t}{\ln t}\right| \leq \sqrt{x}\ln(x).$$

Lorsque x devient grand, le terme d'erreur $\sqrt{x}\ln(x)$ est bien plus petit que le terme $K_1 \exp\left(-K_2\sqrt{\ln(x)}\right)$. Autrement dit, si on savait démontrer l'hypothèse de Riemann, alors on saurait compter les nombres premiers avec bien plus de précision.

Terminons avec la conjecture du jeune Gauss. Sa démonstration ne nécessite que le connaissance d'une région minimale où ζ ne s'annule pas. En effet, elle est la conséquence du fait que si $x = 1$ et $y \neq 0$, alors $\zeta(x, y) \neq 0$.

Emmanuel Royer, Clermont Université, Université Blaise Pascal, Laboratoire de mathématiques, BP 10448, F-63000 Clermont-Ferrand, France

Current address: Université Blaise Pascal, Laboratoire de mathématiques, Les Cézeaux, BP 80026, F-63171 Aubière Cedex, France

E-mail address: `emmanuel.royer@math.univ-bpclermont.fr`