L'arithmétique

LA SCIENCE DES NOMBRES

À l'origine, c'est-à-dire pour les premiers mathématiciens que sont les Grecs de l'Antiquité, il existe deux grandes disciplines mathématiques, d'ailleurs très imbriquées l'une dans l'autre : la géométrie et l'arithmétique (de *arithmos*, nombre). Alors que la géométrie s'occupe des figures, l'arithmétique consiste en l'étude des nombres figurés et de leurs relations avec les différentes opérations qui sont l'addition, la soustraction, la multiplication et la division (et ensuite les élévations au carré et au cube). Plus tard, l'adoption de la numération de position à base 10 fait réaliser d'immenses progrès dans cette branche des mathématiques, même si la base 2 est universelle pour les ordinateurs et la base 12 subsiste pour les heures. L'arithmétique s'occupe plus particulièrement des nombres entiers naturels (0, 1, 2, 3…), mais aussi des autres nombres, des relations entre eux et des techniques permettant de les manipuler.
À partir du concept de division, l'arithmétique définit les nombres premiers, les nombres pairs et impairs, les nombres parfaits, etc. Malgré la simplicité des énoncés des problèmes arithmétiques, leur résolution peut s'avérer très ardue et impliquer des concepts dépassant très largement la seule arithmétique. Il existe d'ailleurs encore aujourd'hui de nombreuses questions ouvertes.

LES ORIGINES

Pythagore (570-490 av J.-C.) est l'un des premiers mathématiciens à considérer des problèmes liés aux nombres. Outre le célèbre théorème qui porte son nom, on doit à Pythagore et à son école, les premiers concepts arithmétiques comme les nombres parfaits et amiables. Un autre mathématicien grec, Diophante (325-409) est à l'origine des équations dites diophantiennes qui sont emblématiques des questions de l'arithmétique. Ce sont des équations à plusieurs inconnues dont les coefficients sont des nombres entiers et dont on cherche des solutions parmi les nombres entiers. L'exemple le plus simple étant : $3^2 + 4^2 = 5^2$.
Après les grecs, l'arithmétique a pu se développer en grande partie grâce à l'invention de la numération décimale de position avec le zéro provenant d'Inde (Vᵉ siècle), transmise aux Arabes qui l'ont introduite en Occident vers le IXᵉ siècle. Ensuite l'introduction du calcul littéral a permis de formaliser les méthodes algébriques qui sont encore utilisées aujourd'hui. L'arithmétique élémentaire décrite plus haut s'est alors enrichie et on peut décrire des arithmétiques plus formelles dites « d'anneaux principaux ». Les anneaux étant des structures mathématiques construites à l'image des nombres avec une multiplication et une addition. C'est ainsi que l'on traite par exemple de l'arithmétique des polynômes.

LES DIFFÉRENTES ARITHMÉTIQUES

L'addition et la multiplication – et leurs inverses, la soustraction et la division – sont les principales opérations étudiées en arithmétique. Ainsi on effectue une première distinction entre arithmétique additive et arithmétique multiplicative.
La théorie des partitions fait par exemple partie de l'arithmétique additive, alors que l'étude de la fonction φ (phi) d'Euler fait partie de l'arithmétique multiplicative.
L'étude des propriétés des nombres entiers peut également parfois se plonger dans l'analyse qui est l'étude des fonctions (réelles, complexes, p-adique, etc.). Cela donne lieu à différentes approches de l'arithmétique. Par exemple, l'étude de la densité asymptotique des nombres premiers (leur distribution lorsque l'on « va vers l'infini »), fait partie d'une arithmétique asymptotique.
De façon encore plus abstraite, l'étude de la fonction ζ (zêta) de Riemann où interviennent des notions appartenant à la théorie des fonctions analytiques, fait partie de l'arithmétique analytique.
En fait, l'arithmétique n'a pas de frontière bien définie, et ses problèmes peuvent concerner toutes les autres branches des mathématiques. Un exemple très récent est le théorème de Fermat-Wiles, dont l'énoncé est très simple et à base de nombres entiers, de multiplications et d'additions, et dont la démonstration en 1994 a nécessité, après plusieurs siècles, l'intervention d'un nombre important de disciplines mathématiques.

LES CONCEPTS ARITHMÉTIQUES

Addition et soustraction

L'arithmétique est l'étude des relations des nombres avec les opérations, et en premier lieu avec la plus simple d'entre elles, l'addition notée « + ». Cette opération, qui paraît si évidente, est soumise à diverses propriétés :
1 - Si a et b sont deux nombres, on peut additionner indifféremment a à b et b à a. On obtient alors le même résultat : $a + b = b + a$. Par exemple, $3 + 5 = 5 + 3 = 8$. On dit que l'addition est commutative.
2 - Si a, b et c sont trois nombres, on obtient également le même résultat en additionnant $(a + b)$ à c ou en additionnant a à $(b + c)$:
$((a + b) + c) = (a + (b + c))$.
Ex. : $((1 + 2) + 3) = (1 + (2 + 3))$ car $(3 + 3) = (1 + 5) = 6$.
On dit que l'addition est associative.
3 - Si a est un nombre, $(a + 0) = a$. On dit que 0 (zéro) est l'élément neutre pour l'addition.
Ces trois propositions sont vraies pour n'importe lequel de ces types : entiers naturels (N), entiers relatifs (Z), rationnels (Q), réels (R), complexes (C)…
Si l'on se restreint au cas des nombres entiers naturels (0, 1, 2, 3…), seules ces trois premières propriétés sur l'addition sont valables. Mais si on y joint les entiers négatifs, on obtient alors les entiers relatifs : … – 2, – 1, 0, 1, 2, … dont l'ensemble est noté Z. Dans ce cas on a une quatrième propriété :
4 - Si a est un nombre, il existe un nombre b qui ajouté à a donne le résultat 0 : $(a + b) = 0$. Ce nombre est $(-a)$. Par exemple, $5 + (-5) = 0$.
Cette dernière assertion est à l'origine de la seconde opération de l'arithmétique : la soustraction.
Ces quatre propriétés sont fondamentales et permettent de débuter l'arithmétique.

Partitions

À partir de l'addition, on peut déjà définir la théorie des partitions.
Une partition d'un nombre entier $n \geq 1$ est un ensemble de nombres entiers non nuls dont la somme est n. Par exemple, le nombre « 4 » a 4 partitions qui sont :
3 + 1 ;
2 + 2 ;
2 + 1 + 1 ;
1 + 1 + 1 + 1.
Définie par Euler (1707-1783), cette notion donne naissance à la théorie des partitions qui est utilisée en théorie des nombres et en combinatoire.
De nombreux problèmes très complexes font partie de la théorie des partitions, tels les conjectures de Goldbach ou les problèmes de Waring.

Multiplication et division

La multiplication, notée « x » ou « . », vérifie les deux premières propriétés de l'addition : elle est commutative et associative.
Elle possède également un élément neutre qui est « 1 » (l'unité).
Le nombre « 0 » joue lui aussi un rôle par rapport à la multiplication : si a est un nombre, alors $(a \times 0) = 0$.
Pour la multiplication, on dit que 0 est un élément absorbant.
On sait que pour les nombres rationnels ou réels, il existe un inverse à n'importe quel nombre, c'est-à-dire un nombre b tel que $a \times b = 1$. Par exemple, $2 \times 1/2 = 1$.
On peut ainsi définir une opération qui s'appelle la division.
Cependant, pour l'ensemble des nombres entiers naturels N, qui est l'ensemble étudié principalement par l'arithmétique, un tel nombre n'existe pas, et la division ne tombe pas « juste ». On définit alors la division euclidienne :
si a et b sont deux nombres (entiers relatifs), il existe deux autres nombres (entiers relatifs) q et r tels que $a = b \times q + r$, avec $0 \leq r < b$.
Le nombre q est appelé le quotient et r le reste de la division euclidienne de a par b.
Ainsi, le quotient de la division de 13 par 5 est 2 et le reste de cette division est 3 :
$13 = 5 \times 2 + 3$, avec $0 \leq 3 < 5$.

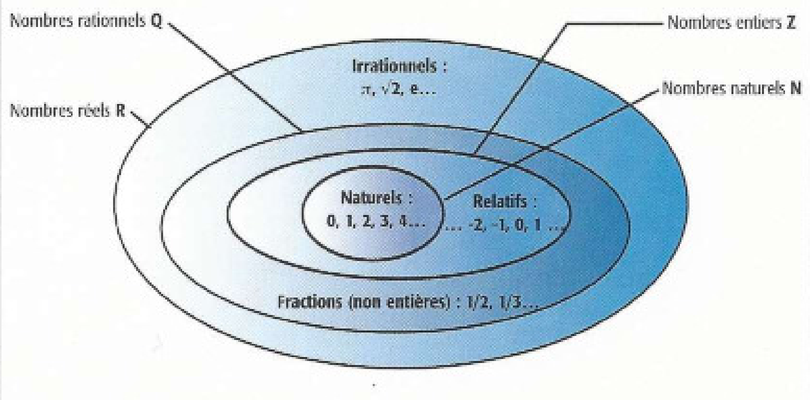
Parité et divisibilité

La propriété la plus simple d'un nombre est sa parité. La division par 2 fournit la première classification des naturels : ceux divisibles par 2 sont pairs, et ceux qui ne le sont pas sont impairs.
Autrement dit, un nombre est pair lorsqu'il est le double d'un autre, sinon, il est impair. Pour signifier que les pairs sont des « doubles », les mathématiciens les notent $2n$, n étant un entier naturel quelconque ; et les impairs sont notés $2n + 1$.

Opérations sur les nombres pairs et impairs

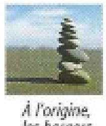
• Addition-soustraction :
pair ± pair = pair ;
pair ± impair = impair ;
impair ± impair = pair.
• Multiplication :
pair x pair = pair ;
pair x impair = pair ;
impair x impair = impair.
• Division :
La division de deux nombres entiers n'a pas nécessairement comme résultat un nombre entier. Par exemple, 1 divisé par 4 donne 1/4, qui n'est ni pair ou impair, les concepts pair et impair ne s'appliquant seulement que sur les entiers. Mais lorsque le quotient est un entier :
pair / impair = pair ;
impair / impair = impair ;
impair / pair n'est jamais un entier ;
pair / pair peut être soit pair soit impair.
La propriété de parité est en fait un cas particulier de la propriété de base de l'arithmétique : la divisibilité.

Les ensembles de nombres



Nombres et particularités

Des cailloux



À l'origine, les bergers représentaient chaque animal du troupeau par un cône d'argile. Ces cônes s'appelaient les « calculi » et sont à l'origine du mot « calcul ». En latin, calculus, calculi : un caillou, des cailloux.

Hôpital des Quinze-Vingts

L'hôpital parisien qui hébergeait 300 anciens combattants s'appelle toujours « Hôpital des Quinze-Vingts », vestige du système à base 20. En effet, 15 x 20 = 300.

6 ou 28

Tous les nombres parfaits pairs se terminent par 6 ou 28.

Nombre parfait impair ?

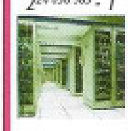
Il n'existe pas de nombre parfait impair inférieur à 10^{300}.

1 Gogol

1 Gogol = 10^{100} Mot inventé pour traduire un très grand nombre : « 1 suivi de 100 zéros ».

Le nombre premier le plus grand

mai 2004
$2^{24\,036\,583} - 1$



7 235 733
chiffres

Un nombre n est divisible par un autre nombre m lorsqu'il est le produit de ce dernier avec un troisième nombre : $n = m.p$.
Autrement dit, le reste de la division euclidienne de n par m est égal à 0.
Exemple : $8 = 4 \times 2 + 0$.
Le nombre m est alors un diviseur de n, et n est un multiple de m.

Critères de divisibilité

• Un nombre est divisible par 2 s'il se termine par un chiffre pair (0, 2, 4, 6, 8).
• Un nombre est divisible par 3 lorsque la somme de ses chiffres est divisible par 3. Exemple : 471, la somme de ses chiffres est $4 + 7 + 1 = 12$, qui est divisible par 3.
• Un nombre est divisible par 5 lorsqu'il se termine par 0 ou 5.
• Un nombre est divisible par 9 lorsque la somme de ses chiffres est divisible par 9. Exemple : 4 185, la somme de ses chiffres est $4 + 1 + 8 + 5 = 18$, qui est divisible par 9.

Algorithme d'Euclide et PGCD

À partir de la notion de divisibilité, on introduit naturellement les notions très utiles en théorie des nombres de plus grand diviseur commun (PGCD) et plus petit multiple commun (PPCM) de deux nombres.
Le PGCD de a et de b est le plus grand nombre qui divise à la fois a et b.
Le PPCM de a et de b est le plus petit nombre qui est divisé à la fois par a et par b.
L'algorithme d'Euclide, basé sur l'utilisation de la division euclidienne permet de déterminer le PGCD de deux nombres a et b.
Soient $a = 540$ et $b = 231$.

LA NUMÉRATION DANS UNE BASE

L'adoption d'une base de numération est un moyen pour n'utiliser qu'un petit nombre de symboles dans la représentation des nombres. Au lieu de compter uniquement par unités ($n = 1 + 1 + 1 + 1\ldots$), on compte par « paquets ».
On sait que les Babyloniens utilisaient le système sexagésimal (base 60), les Grecs se servaient des lettres de l'alphabet, les Mayas utilisaient un système vicésimal (base 20).
Actuellement la numération décimale (base 10) est la plus largement répandue. Elle fait intervenir dix symboles distincts, ou chiffres, pour représenter des nombres : 0, 1, 2, 3, 4, 5, 6, 7, 8, 9.
Dans le système décimal, la quantité représentée par n'importe lequel des dix symboles en usage dépend de sa position dans le nombre. Par exemple, le nombre 123 456 est une notation abrégée pour :

$1 \times 10^5 +$
$2 \times 10^4 +$
$3 \times 10^3 +$
$4 \times 10^2 +$
$5 \times 10^1 +$
6×10^0

Pour certains usages, on utilise toujours d'autres nombres que 10 comme base car ils possèdent plus de diviseurs.
Par exemple, la base 60 et son sous-multiple 12 s'avèrent très utiles pour subdiviser le temps.
Par ailleurs, le système binaire (base 2), avec le système de numération de base 16, est utilisé en informatique.

540 divisé par 231 donne 2, reste 78 ;
$540 = 231 \times 2 + 78$.
231 divisé par 78 donne 2, reste 75 ;
$231 = 78 \times 2 + 75$
78 divisé par 75 donne 1, reste 3 ;
$78 = 75 \times 1 + 3$
75 divisé par 3 donne 25, reste 0 ;
$75 = 3 \times 25 + 0$.
Le dernier reste, 3, est le PGCD de 540 et 231.
On peut alors en déduire le PPCM de 540 et 231. Il suffit de diviser le produit des deux nombres a et b par le PGCD.
Le PPCM de 540 et 231 est donc 41 580.
Une propriété intéressante du PGCD est l'identité de Bézout :
Si $d = \mathrm{PGCD}(a, b)$, il existe deux nombres u et v tels que $d = a.u + b.v$.
Par exemple, le PGCD de 14 et 10 est 2, donc il existe deux nombres tels que $2 = 14 \times u + 10 \times v$, ce qui n'est pas évident a priori. Par exemple : $u = 2$ et $v = -3$.
Si le PGCD de deux nombres est égal à 1, on dit que ces deux nombres sont premiers entre eux. Ils n'ont alors aucun diviseur commun autre que 1 et eux-même.

Nombres parfaits et nombres amiables

Introduits par Pythagore, les nombres parfaits et amiables sont parmi les premières notions arithmétiques inventées.
Un nombre est parfait s'il est égal à la somme de ses diviseurs. Ainsi, 6 est un nombre parfait. En effet, les diviseurs de 6 sont 1, 2, 3 et $6 = 1 + 2 + 3$.
Il n'existe pas de nombre parfait impair inférieur à 10^{300}, mais on ignore s'il en existe ou non au-delà. Le plus grand nombre parfait connu est
$2^{756838}(2^{756839} - 1)$ et il est pair.
Si la somme des diviseurs d'un nombre est supérieure à ce nombre, on dit qu'il est abondant. On sait qu'il existe une infinité de nombres abondants (12, 18, 20…). Par exemple, les diviseurs de 12 sont 1, 2, 3, 4, 6 et $12 < 1 + 2 + 3 + 4 + 6 = 16$.
Dans le même esprit, deux nombres sont amiables si la somme des diviseurs de l'un est égale à l'autre. Les grecs ne connaissaient que les deux plus petits nombres amiables : 220 et 284. Les diviseurs de 220 sont 1, 2, 4, 5, 10, 11, 20, 22, 44, 55, 110, dont la somme est 284. Quant aux diviseurs de 284, qui sont 1, 2, 4, 71 et 142, leur somme n'est autre que 220.

LES NOMBRES PREMIERS

Les nombres premiers sont les nombres les plus importants en arithmétique. Un nombre est premier lorsqu'il n'est pas le produit de deux nombres plus petits, c'est-à-dire que ses seuls diviseurs sont 1 et lui-même.

Théorème fondamental de l'arithmétique

Depuis Euclide, on sait que tous les nombres peuvent être décomposés en un produit fini de nombres premiers.
Ainsi, si n désigne un nombre entier quelconque et « 2, 3, 5, 7… » la suite des nombres premiers, alors il existe des exposants (nombres entiers) i, j, k, l… tels que $n = p_1^i p_2^j \ldots = 2^i 3^j 5^k 7^l \ldots$
Par exemple, $540 = 2^2 3^3 5^1$, tous les exposants des autres nombres premiers étant nuls (un nombre élevé à la puissance 0 donne 1). Chaque exposant désigne donc le nombre de fois que le facteur premier correspondant apparaît dans la décomposition. Ce théorème montre que les nombres premiers sont comme les briques élémentaires des autres nombres.
On sait qu'il existe une infinité de nombres premiers mais leur apparition dans la suite des nombres entiers semble aléatoire. en outre, il n'existe aucune méthode pour en construire, bien que de nombreux mathématiciens s'y soient essayés.

Nombres de Fermat

Par exemple, Pierre de Fermat, en décrivant les nombres de Fermat qui sont de la forme $F_n = 2^{2^n} + 1$, croyait avoir une formule donnant les nombres premiers. Mais si $F_0 = 3$, $F_1 = 5$, $F_2 = 17$, $F_3 = 257$ et $F_4 = 65\,537$ sont premiers, F_5 ne l'est pas, ainsi que de nombreux autres. Il a fallu deux ans de calculs pour montrer que F_{17} n'est pas premier.
Ces nombres ont également d'autres applications, en particulier dans la construction des polygones réguliers.

Nombres de Mersenne

Mersenne (1588-1648) a également décrit les nombres de Mersenne de la forme $M = 2^p - 1$, dont il croyait qu'ils étaient premiers si p l'était, ce qui est faux. Par contre, si M est un nombre premier, alors p l'est également, mais la réciproque est fausse : par exemple, si $p = 11$, alors $M = 2\,047 = 23 \times 89$.
Néanmoins, les nombres premiers de Mersenne présentent certaines propriétés remarquables.
Une propriété énonce que si M est un nombre premier de Mersenne, alors le nombre $M(M + 1)/2$ est un nombre dit « parfait », c'est-à-dire égal à la somme de ses diviseurs propres.
Les nombres de Mersenne ont aussi permis de construire de nombreux grands nombres premiers.
Le plus grand nombre premier connu à ce jour est un nombre de Mersenne ($2^{24\,036\,583} - 1$), il possède 7 235 733 chiffres et a été découvert le 28 mai 2004 par le GIMPS (Great Internet Prime Search) grâce au calcul partagé sur Internet.

« Théorème de raréfaction des nombres premiers »

Même si la distribution des nombres premiers parmi les nombres entiers naturels semble aléatoire, les nombres premiers obéissent pourtant à des lois très précises. Ainsi, le théorème de raréfaction des nombres premiers affirme que pour un entier n donné, la quantité de nombres premiers

inférieurs à n est à peu près $n/\log(n)$. Conjecturé par ***Gauss*** et Legendre, ce théorème fut démontré indépendamment par Hadamard et de La Vallée-Poussin en 1896.

Indicateur d'Euler Φ

Pour un entier n, l'indicateur d'Euler $\varphi(n)$ est la quantité de nombres premiers avec n, inférieurs à n.
Il est égal à :
$\varphi(n) = n(1 - 1/p_1)(1 - 1/p_2)\ldots(1 - 1/p_r)$
où $n = p_1^i p_2^j \ldots$ est la décomposition de n en facteurs premiers.
Par exemple, pour $n = 10$:
$10 = 2 \times 5$; $p_1 = 2$ et $p_2 = 5$
$\varphi(n) = 10(1 - 1/2)(1 - 1/5) = 4$.
Cette fonction possède de nombreuses propriétés intéressantes, et son étude a donné lieu à de nombreux résultats.
Il existe également encore des questions ouvertes liées à φ, comme par exemple la conjecture de Carmichaël qui affirme que $\varphi(n) = n$ n'existe pas. Cette conjecture a été vérifiée jusqu'à $n = 10^{10\,000}$.

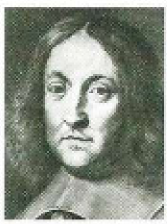
QUELQUES PROBLÈMES ARITHMÉTIQUES

Le petit théorème de Fermat

Si p est un nombre premier, le petit théorème de Fermat affirme que pour tout entier naturel a, le reste de la division de a^p par p est le même que le reste de la division de a par p. Ceci s'écrit en langage mathématique :
$a^p \equiv a \mod p$; qui se lit a^p est congru à a modulo p.
Un nombre n non premier qui vérifie cette propriété est appelé absolument pseudo-premier. Un tel nombre est nécessairement impair et sa décomposition en facteurs premiers comporte au moins trois facteurs et ne comporte aucun carré. On ignore s'il en existe une infinité.

Le théorème de Fermat-Wiles

Parmi les équations diophantiennes, le théorème de Fermat-Wiles, longtemps appelé la conjecture de Fermat est l'un des plus célèbres des mathématiques.
Il a été démontré en 1994 par Andrew



Wiles. Enoncé en 1641 par ***Pierre de Fermat***, ce problème d'apparence très simple a occupé de nombreux mathématiciens pendant deux siècles et demi.
Sa démonstration présentée par Wiles, qui n'est comprise dans sa totalité que par une poignée de mathématiciens, utilise un rapprochement des formes modulaires et des courbes elliptiques.
Deux concepts qui appartiennent à l'analyse et à la géométrie algébrique, et qui sont au départ très éloignés de l'arithmétique.
Le théorème de Fermat-Wiles s'énonce ainsi :
Il n'existe pas de solution autre que $x = 0$, $y = 0$, $z = 0$ à l'équation $x^n + y^n = z^n$ dès que n est supérieur à 2.

Conjectures de Goldbach

Les conjectures de Goldbach sont deux problèmes posés par Goldbach (1690-1764) à Euler en 1742.
Ces conjectures affirment que tout entier pair $n \geq 4$ est somme de deux nombres premiers et que tout entier impair $n \geq 9$ est somme de trois nombres premiers.
Elles sont encore non démontrées à ce jour, malgré des avancées importantes dues à Vinogradov (1937) et Vaughan (1975). On sait par exemple que la première conjecture est vérifiée pour $n \leq 33.10^6$, et que pour ces nombres, les deux nombres premiers concernés sont distincts.

Conjecture de Catalan

La conjecture de Catalan affirme que les seules puissances exactes consécutives sont 8 et 9. Autrement dit, la seule solution à l'équation diophantienne $x^n - y^m = 1$ est $x = 3$, $y = 2$, $n = 2$ et $m = 3$.
Posée par Catalan (1814-1894) en 1844, elle a été démontrée en 2002 par Mihailescu.

Infinité des couples de nombres premiers jumeaux

Deux nombres premiers p et q sont appelés jumeaux lorsque $q = p + 2$. Par exemple, (5 , 7), (17 , 19) ou (311 , 313) sont les premiers couples de nombres premiers jumeaux. On ignore s'il existe une infinité de tels couples.
On sait cependant que la série $\Sigma\, 1/p$, qui diverge lorsque l'on considère tous les nombres premiers, converge si l'on se restreint aux nombres premiers jumeaux.
On a dénombré 6 497 407 couples parmi les 100 premiers millions de nombres premiers.

Théorème de Waring

En 1770, Waring (1734-1798) émettait l'hypothèse que tout entier n peut s'écrire comme la somme de quatre carrés parfaits au plus, c'est-à-dire $n = a^2 + b^2 + c^2 + d^2$. Il supposait également que ce nombre pouvait s'écrire comme somme de 9 cubes parfaits au plus, comme somme de 19 puissances quatrièmes au plus, et d'une manière générale comme somme d'un nombre fini $g(k)$ de puissance k-ième au plus. Ce théorème fut démontré petit à petit par Lagrange pour $k = 2$ en 1770, par Wieferich pour $k = 3$ en 1909. Hilbert montra la même année l'existence de ce nombre fini $g(k)$, mais on ne sut le calculer pour $k \geq 6$ qu'après les travaux de Hardy et Littlewood en 1935.
Ce théorème fut démontré en 1985, 215 ans après.

La fonction ζ de Riemann

Pour un nombre s, on définit le nombre $\zeta(s)$ comme la somme infinie $\zeta(s) = \Sigma_{n>0}(1/n^s)$.
Ce nombre est défini si $s > 1$ (on dit que la somme infinie converge). Par exemple, $\zeta(2) = \Sigma_{n>0}(1/n^2) = \pi^2/6$.
Les mathématiciens ont étendu cette fonction aux nombres complexes sauf 1, c'est-à-dire qu'ils ont défini $\zeta(s)$ lorsque s est un nombre complexe $(a + ib)$ différent de 1.
La fonction ζ est appelée fonction ζ de Riemann. Elle intervient en arithmétique dans l'étude de la répartition des nombres premiers grâce à l'identité d'Euler. Cette identité exprime en effet $\zeta(s)$ comme un produit infini où apparaissent tous les nombres premiers.
L'étude de cette fonction a par exemple permis à Hadamard et de La Vallée-Poussin de démontrer le théorème de raréfaction des nombres premiers cité plus haut.
Enfin, la conjecture de Riemann, non encore démontrée, portant sur la nature des zéros (ou racines) de cette fonction permettrait d'affiner certains résultats concernant les nombres premiers.