Mardi 13 janvier 2015

USTHB, Alger

Quelques problèmes ouverts en théorie des nombres

Michel Waldschmidt

Institut de Mathématiques de Jussieu — Paris VI
http://www.math.jussieu.fr/∼miw/

Résumé

Les problèmes de théorie des nombres sont souvent faciles à énoncer et très difficiles à résoudre. Nous en donnons quelques exemples.

Résumé plus détaillé

Nous commençons en parlant des nombres premiers.

La conjecture des nombres premiers jumeaux et la conjecture de Goldbach font partie des principaux défis du sujet.

Les 10 plus grands nombres premiers connus explicitement sont des nombres de Mersenne. Y a-t-il une infinité de nombres premiers de Mersenne (resp. de Fermat) ? On ne sait pas. Les nombres premiers de Mersenne sont reliés aux nombres parfaits, considérés par Euclide, et qui posent un problème qu'on ne sait toujours pas résoudre.

Un des problèmes ouverts les plus célèbres est l'hypothèse de Riemann, qui résiste depuis 150 ans.

Résumé détaillé (suite)

Les équations diophantiennes recèlent plein de mystères. Le *Dernier Théorème de Fermat* a été démontré par A. Wiles, mais de nombreuses autres questions ne sont pas encore résolues. Nous parlerons d'une conjecture de S.S. Pillai, ainsi que de la conjecture abc proposée par Oesterlé et Masser.

Kontsevich et Zagier ont introduit la notion de *période* et ont suggéré un énoncé portant sur ces périodes qui fournirait un cadre adapté à une large classe de problèmes d'irrationalité et de transcendance.

Pour terminer, nous discuterons de questions provenant de travaux de E. Borel en 1905 puis en 1950 sur les développements (binaires ou décimaux par exemples) de nombres algébriques. On sait très peu de choses sur ces questions.

Le 8ème problème de Hilbert

8 Août 1900

David Hilbert (1862 - 1943)

Deuxième Congrès International des Mathématiciens (ICM1900) à Paris.

Nombres premiers jumeaux.

Conjecture de Goldbach,

Hypothèse de Riemann

Les 7 problèmes Clay du Millennium

Clay Mathematics Institute (CMI)
Cambridge, Massachusetts `http://www.claymath.org`

Prix de 7 million US$ pour la solution de ces problèmes,
1 million US$ pour chacun

24 mai 2000, Paris :
Timothy Gowers, John Tate et Michael Atiyah.

- Conjecture de Birch et Swinnerton-Dyer
- Conjecture de Hodge
- Équations de Navier-Stokes
- P vs NP
- Conjecture de Poincaré (*Grigory Perelman*)
- Hypothèse de Riemann
- Théorie de Yang-Mills

Nombres

Nombres = réels ou complexes $\mathbf{R}$, $\mathbf{C}$.

Entiers naturels : $\mathbf{N} = \{0, 1, 2, \ldots\}$.

Entiers rationnels : $\mathbf{Z} = \{0, \pm 1, \pm 2, \ldots\}$.

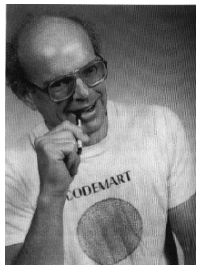
Nombres premiers

Un nombre premier est un entier positif ayant exactement deux diviseurs
Il y a 25 nombres premiers inférieurs à 100 :

$$2,\ 3,\ 5,\ 7,\ 11,\ 13,\ 17,\ 19,\ 23,\ 29,\ 31,\ 37,\ 41,$$

$$43,\ 47,\ 53,\ 59,\ 61,\ 67,\ 71,\ 73,\ 79,\ 83,\ 89,\ 97.$$

The On-Line Encyclopedia of Integer Sequences
`http://oeis.org/A000040`



Nombres composés

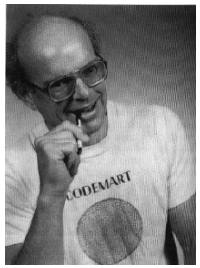
Nombres ayant au moins trois diviseurs :

$4,\ 6,\ 8,\ 9,\ 10,\ 12,\ 14,\ 15,\ 16,\ 18,\ 20,\ 21,\ 22,\ 24,\ 25,\ 26,\ 27, \ldots$

http://oeis.org/A002808

Les nombres composés sont les nombres n de la forme $x \cdot y$ avec $x > 1$ et $y > 1$.

Il y a 73 nombres composés inférieurs à 100.



Euclide d'Alexandrie

(vers 325 BC – vers 265 BC)

Étant donnée une collection finie $p_1, \ldots, p_n$ de nombres premiers, il existe un nombre premier qui n'est pas dans cette collection.

Premiers jumeaux

Le seul nombre premier p tel que $p + 1$ soit premier est $p = 2$.

Conjecture : *il y a une infinité de nombres premiers p tels que $p + 2$ soit premier.*

Exemples : $3, 5,\quad 5, 7,\quad 11, 13,\quad 17, 19, \ldots$

Plus généralement : *est-il vrai que tout entier pair est la différence de deux nombres premiers ?*

Est-vrai une infinité de fois ?

Tout entier pair est-il la différence de deux nombres premiers consécutifs ? Une infinité de fois ?

L'exemple le plus grand de nombres premiers jumeaux (trouvé en décembre 2011) a $200\,700$ chiffres décimaux :

$$3\,756\,801\,695\,685 \cdot 2^{666669} \pm 1$$

http://oeis.org/A001097

http://primes.utm.edu/

Conjecture de Goldbach

Christian Goldbach
(1690 – 1764)

Leonhard Euler
(1707 – 1783)

Lettre de Goldbach à Euler, 1742 :
tout entier ≥ 6 est somme de 3 nombres premiers.

Euler : c'est équivalent à :

tout entier pair supérieur à 2 est somme de deux nombres premiers.

Démonstration :
$2n = p + p' + 2 \Longleftrightarrow 2n + 1 = p + p' + 3$.

Somme de deux nombres premiers

$$4 = 2 + 2 \qquad 6 = 3 + 3$$
$$8 = 5 + 3 \qquad 10 = 7 + 3$$
$$12 = 7 + 5 \qquad 14 = 11 + 3$$
$$16 = 13 + 3 \qquad 18 = 13 + 5$$
$$20 = 17 + 3 \qquad 22 = 19 + 3$$
$$24 = 19 + 5 \qquad 26 = 23 + 3$$
$$\vdots \qquad \vdots$$

Somme de nombres premiers

Théorème – I.M. Vinogradov (1937)
Tout entier impair suffisamment grand est somme de trois nombres premiers.

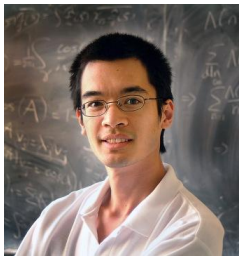
Théorème – Chen Jing-Run (1966)
Tout entier pair suffisamment grand est somme d'un nombre premier et d'un entier qui est soit premier, soit produit de deux nombres premiers.


Ivan Matveevich Vinogradov
(1891 – 1983)


Chen Jing Run
(1933 - 1996)

Somme de nombres premiers

- 27 n'est ni premier, ni somme de deux nombres premiers.
- Conjecture de Goldbach faible (ou ternaire) : *tout entier impair ≥ 7 est somme de trois nombres premiers.*
- Terence Tao, 4 février 2012, `arXiv:1201.6656` : *Tout entier impair supérieur à 1 est somme d'au plus cinq nombres premiers.*



Problème de Goldbach ternaire

Théorème – Harald Helfgott (2013).
Tout entier impair supérieur à 5 est somme de trois nombres premiers.
Tout entier impair supérieur à 7 est somme de trois nombres premiers impairs.

Harald Helfgott
(1977-)

Méthode du cercle

Srinivasa Ramanujan
(1887 – 1920)

G.H. Hardy
(1877 – 1947)

J.E. Littlewood
(1885 – 1977)

Hardy, ICM Stockholm, 1916
Hardy et Ramanujan (1918) : partitions
Hardy et Littlewood (1920 – 1928) :
Some problems in Partitio Numerorum

Méthode du cercle

Hardy et Littlewood

Ivan Matveevich Vinogradov
(1891 – 1983)

Tout entier impair suffisamment grand est la somme d'au plus trois nombres premiers.

Conjecture (Hardy et Littlewood, 1915)

Le nombre de premiers $p \leq x$ tels que $p+2$ soit premier est

$$\sim C \frac{x}{(\log x)^2}$$

où

$$C = \prod_{p \geq 3} \frac{p(p-2)}{(p-1)^2} \sim 0.660\,16\ldots$$

Nombres premiers les plus grands explicitement connus

2 mai 2013 $17\,425\,170$ chiffres décimaux

$$2^{57\,885\,161} - 1$$

23 août 2008 $12\,978\,189$ chiffres décimaux

$$2^{43\,112\,609} - 1$$

13 juin 2009 $12\,837\,064$ chiffres décimaux

$$2^{42\,643\,801} - 1$$

6 septembre 2008 $11\,185\,272$ chiffres décimaux

$$2^{37\,156\,667} - 1$$

Grands nombres premiers

Les dix plus grands nombres premiers explicitement connus sont de la forme $2^p - 1$.

Le *13 janvier 2015*, on connaît
- 121 nombres premiers ayant plus de $1\,000\,000$ chiffres décimaux,
- 1155 nombres premiers ayant plus de $500\,000$ chiffres décimaux.

Liste des $5\,000$ nombres premiers les plus grands explicitement connus :
http://primes.utm.edu/largest.html
48 nombres premiers de la forme $2^p - 1$ sont connus
http://www.mersenne.org/

Marin Mersenne

1588 – 1648

Nombres premiers de Mersenne

Si un nombre de la forme $2^k - 1$ est premier, alors k lui-même est premier.

Un nombre premier de la forme $2^p - 1$ est appelé *nombre premier de Mersenne*.

On en connaît 48, incluant les 10 plus grands nombres premiers explicitement connus.

Les plus petits nombres premiers de Mersenne sont

$$3 = 2^2 - 1, \quad 7 = 2^3 - 1 \quad 31 = 2^5 - 1, \quad 127 = 2^7 - 1.$$

Y a-t-il une infinité de nombres premiers de Mersenne ?

Nombres premiers de Mersenne

En 1536, Hudalricus Regius a remarqué que $2^{11} - 1 = 2\,047$ n'est pas premier : $2\,047 = 23 \cdot 89$.

Dans la préface de *Cogitata Physica-Mathematica* (1644), Mersenne affirme que les nombres de la forme $2^n - 1$ sont premiers pour

$$n = 2,\ 3,\ 5,\ 7,\ 13,\ 17,\ 19,\ 31,\ 67,\ 127 \quad \text{et} \quad 257$$

et qu'ils sont composés pour toutes les autres valeurs de $n < 257$.

La liste correcte est

$$2,\ 3,\ 5,\ 7,\ 13,\ 17,\ 19,\ 31,\ 61,\ 89,\ 107 \quad \text{et} \quad 127.$$

http://oeis.org/A000043

Nombres parfaits

Un nombre est dit parfait s'il est égal à la somme de ses diviseurs sans le compter lui-même.
Par exemple 6 est égal à la somme $1+2+3$, et les diviseurs de 6 sont 1, 2, 3 et 6.
De même, les diviseurs de 28 sont 1, 2, 4, 7, 14 et 28. La somme $1+2+4+7+14$ est égale à 28, donc 28 is parfait.

Remarquer que $6 = 2 \cdot 3$ et que 3 est un nombre de Mersenne $2^2 - 1$.
De même $28 = 4 \cdot 7$ et 7 est encore un nombre premier de Mersenne $2^3 - 1$.

Quelques autres exemples de nombres parfaits :

$$496 = 16 \cdot 31 \quad \text{avec} \quad 16 = 2^4, \quad 31 = 2^5 - 1,$$

$$8128 = 64 \cdot 127 \quad \text{et} \quad 64 = 2^6, \quad 127 = 2^7 - 1, \ldots$$

Nombres parfaits

Éléments d'Euclide, Livre IX : les nombres de la forme $2^{p-1} \cdot (2^p - 1)$ avec $2^p - 1$ nombre premier de (Mersenne) (donc p lui-même est premier) sont parfaits.

Euler : tous les nombres parfaits pairs sont de cette forme.

Suite des nombres parfaits :

$$6,\ 28,\ 496,\ 8\,128,\ 33\,550\,336,\ \ldots$$

http://oeis.org/A000396

Y a-t-il une infinité de nombres parfaits ?

Existe-t-il des nombres parfaits impairs ?

Nombres de Fermat

Les nombres de Fermat sont les nombres de la forme $F_n = 2^{2^n} + 1$.

Pierre de Fermat (1601 – 1665)

Nombres premiers de Fermat

$F_0 = 3$, $F_1 = 5$, $F_2 = 17$, $F_3 = 257$, $F_4 = 65537$ sont des nombres premiers.
http://oeis.org/A000215

Ils sont reliés à la construction de polygones réguliers avec la règle et le compas.

En 1650, Fermat a suggéré que tous les nombres F_n sont premiers.

Euler : $F_5 = 2^{32} + 1$ est divisible par 641

$$4294967297 = 641 \cdot 6700417$$

$$641 = 5^4 + 2^4 = 5 \cdot 2^7 + 1$$

Y a-t-il une infinité de nombres premiers de Fermat ? On n'en connaît que cinq.

Leonhard Euler (1707 – 1783)

Pour $s > 1$,

$$\zeta(s) = \sum_{n \geq 1} \frac{1}{n^s} = \prod_p (1 - p^{-s})^{-1}.$$

Pour $s = 1$:

$$\sum_p \frac{1}{p} = +\infty.$$

Johann Carl Friedrich Gauss (1777 – 1855)

Soit p_n le n-ème nombre premier.

Problème : majorer le reste

$$E(x) = \left| \pi(x) - \int_0^x \frac{dt}{\log t} \right|.$$

Gauss introduit

$$\pi(x) = \sum_{p \leq x} 1$$

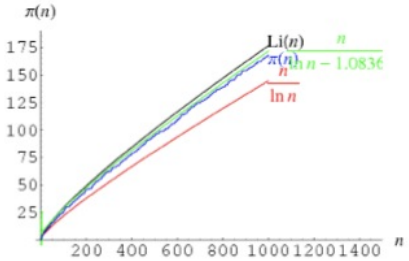
Il observe numériquement

$$\pi(t + dt) - \pi(t) \sim \frac{dt}{\log t}$$

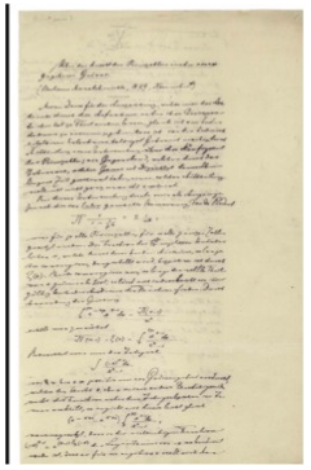
On définit la densité $d\pi$ par

$$\pi(x) = \int_0^x d\pi(t).$$

Graphes

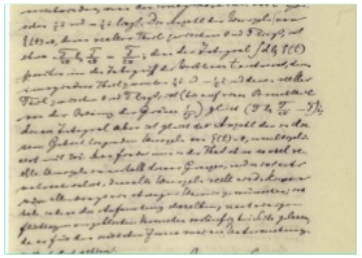


Riemann 1859



Bande critique, droite critique

$\zeta(s) = 0$
pour $0 < \Re e(s) < 1$
implique
$\Re e(s) = 1/2$.



Hypothèse de Riemann

On souhaiterait certainement avoir une démonstration rigoureuse ici. Après quelques essais infructueux, j'ai mis de côté cette recherche provisoirement, car cela ne semble pas indispensable pour la suite de ce travail.

Über die Anzahl der Primzahlen unter einer gegebenen Grösse. (Monatsberichte der Berliner Akademie, November 1859)

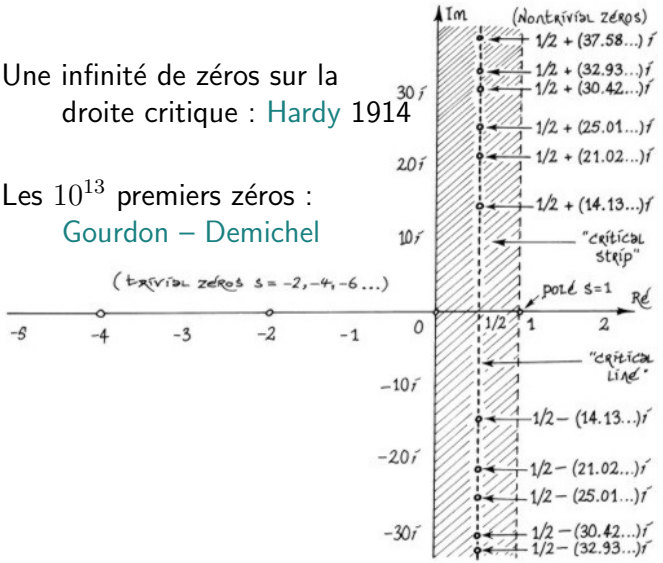
Bernhard Riemann's Gesammelte Mathematische Werke und Wissenschaftlicher Nachlass', herausgegeben under Mitwirkung von Richard Dedekind, von Heinrich Weber. (Leipzig : B. G. Teubner 1892). 145–153.

http://www.maths.tcd.ie/pub/HistMath/People/Riemann/Zeta/

Petits zéros de la fonction zêta

Une infinité de zéros sur la droite critique : Hardy 1914

Les 10^{13} premiers zéros : Gourdon – Demichel



Hypothèse de Riemann

L'hypothèse de Riemann est équivalente à la majoration

$$E(x) \leq Cx^{1/2} \log x$$

pour le reste

$$E(x) = \left| \pi(x) - \int_0^x \frac{dt}{\log t} \right|.$$

Notons $\mathrm{Even}(N)$ (resp. $\mathrm{Odd}(N)$) le nombre d'entiers positifs $\leq N$ ayant un nombre pair (resp. impair) de diviseurs premiers, comptés avec multiplicités. L'hypothèse de Riemann est encore équivalente à

$$|\mathrm{Even}(N) - \mathrm{Odd}(N)| \leq CN^{1/2}.$$

Le théorème des nombres premiers :

$\pi(x) \simeq x/\log x$

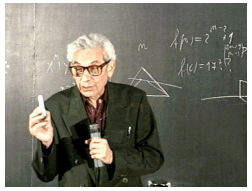
Jacques Hadamard (1865 – 1963)

Charles de la Vallée Poussin (1866 – 1962)

1896 : $\zeta(1+it) \neq 0$ pour $t \in \mathbf{R} \setminus \{0\}$.

Le théorème des nombres premiers : $p_n \simeq n \log n$

Démonstrations élémentaires du théorème des nombres premiers (1949)



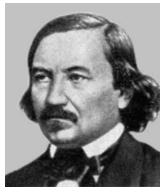
Paul Erdős
(1913 - 1996)

Atle Selberg
(1917 – 2007)

Petits trous dans la suite des nombres premiers

Postulat de Bertrand. *Il y a toujours un nombre premier entre* n *et* $2n$.
Chebyshev (1851) :

$$0.8\frac{x}{\log x} \leq \pi(x) \leq 1.2\frac{x}{\log x}.$$



Joseph Bertrand
(1822 - 1900)

Pafnuty Lvovich Chebyshev
(1821 – 1894)

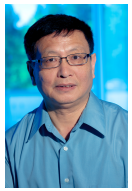
Legendre (1808)

Question : Y a-t-il toujours un nombre premier entre n^2 et $(n+1)^2$?

Adrien-Marie Legendre
(1752 - 1833)

Petits espaces entre nombres premiers

En 2013, Yitang Zhang a montré qu'il y avait une infinité de couples de nombres premiers dont la différence est au plus $70 \cdot 10^6$.



Yitang Zhang
(1955 -)

http://en.wikipedia.org/wiki/Prime_gap
Polymath8a, Juillet 2013 : 4680
James Maynard, Novembre 2013 : 576
Polymath8b, Décembre 2014 : 246
EMS Newsletter December 2014 N° 94 p. 13–23.

Lejeune Dirichlet (1805 – 1859)

Nombres premiers en progression arithmétique.

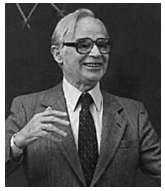
$$a,\ a+q,\ a+2q,\ a+3q,\ \ldots$$

1837 :
Pour $\mathrm{pgcd}(a,q)=1$, on a

$$\sum_{p\equiv a \pmod q} \frac{1}{p} = +\infty.$$

Progressions arithmétiques : van der Waerden

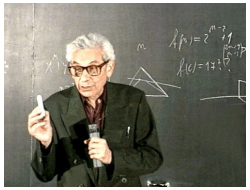
Théorème – B.L. van der Waerden (1927).
Si chaque entier est colorié en utilisant un nombre fini de couleurs, alors une au moins des suites de même couleur contient une progression arithmétique arbitrairement longue.



Bartel Leendert van der Waerden
(1903 - 1996)

Progressions arithmétiques : Erdős et Turán

Conjecture – P. Erdős et P. Turán (1936).
Tout ensemble d'entiers positifs dont la somme des inverses diverge contient des progressions arithmétiques arbitrairement longues.



Paul Erdős
(1913 - 1996)

Paul Turán
(1910 - 1976)

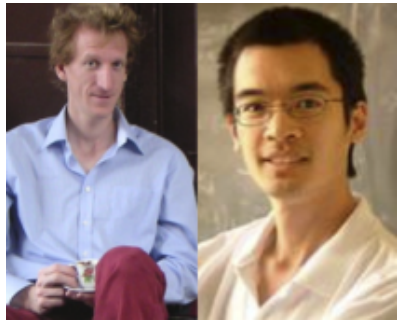
Progressions arithmétiques : E. Szemerédi

Théorème – E. Szemerédi (1975).
Tout sous-ensemble de l'ensemble des entiers ayant une densité positive contient des progressions arithmétiques arbitrairement longues.

Endre Szemerédi
(1940 -)

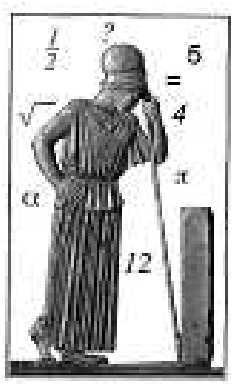
Nombres premiers en progression arithmétique

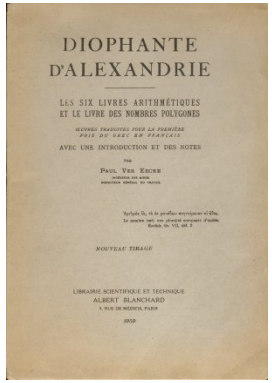
Théorème – B. Green et T. Tao (2004).
L'ensemble des nombres premiers contient des progressions arithmétiques arbitrairement longues.



Diophantine Problems

Diophantus of Alexandria (250 ±50)





Dernier théorème de Fermat $x^n + y^n = z^n$

Pierre de Fermat
1601 – 1665

Andrew Wiles
1953 –

Solution en 1994

S.Sivasankaranarayana Pillai (1901–1950)

Collected works of S. S. Pillai, ed. R. Balasubramanian and R. Thangadurai, 2010.

http ://www.geocities.com/thangadurai_kr/PILLAI.html

Carrés, cubes,...

- Une puissance parfaite est un entier de la forme a^b où $a \geq 1$ et $b > 1$ sont des entiers positifs.
- Carrés :

$1,\ 4,\ 9,\ 16,\ 25,\ 36,\ 49,\ 64,\ 81,\ 100,\ 121,\ 144,\ 169,\ 196, \ldots$

- Cubes :

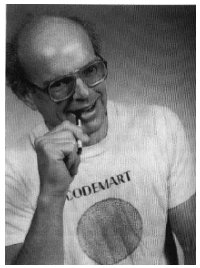
$1,\ 8,\ 27,\ 64,\ 125,\ 216,\ 343,\ 512,\ 729,\ 1\,000,\ 1\,331, \ldots$

- Puissances cinquièmes :

$1,\ 32,\ 243,\ 1\,024,\ 3\,125,\ 7\,776,\ 16\,807,\ 32\,768, \ldots$

Puissances parfaites

$1,\ 4,\ 8,\ 9,\ 16,\ 25,\ 27,\ 32,\ 36,\ 49,\ 64,\ 81,\ 100,\ 121,\ 125,$
$128,\ 144,\ 169,\ 196,\ 216,\ 225,\ 243,\ 256,\ 289,\ 324,\ 343,$
$361,\ 400,\ 441,\ 484,\ 512,\ 529,\ 576,\ 625,\ 676,\ 729,\ 784, \ldots$



Encyclopédie des suites d'entiers (Neil J. A. Sloane)
http://oeis.org/A001597

Entiers consécutifs dans la suite des puissances parfaites

- Difference 1 : $(8, 9)$
- Difference 2 : $(25, 27), \ldots$
- Difference 3 : $(1, 4)$, $(125, 128), \ldots$
- Difference 4 : $(4, 8)$, $(32, 36)$, $(121, 125), \ldots$
- Difference 5 : $(4, 9)$, $(27, 32), \ldots$

Deux conjectures

Eugène Charles Catalan (1814 – 1894)

Subbayya Sivasankaranarayana Pillai (1901-1950)

- Conjecture de Catalan : *Dans la suite des puissances parfaites, $8, 9$ est le seul exemple de deux entiers consécutifs.*
- Pillai's Conjecture : *Dans la suite des puissances parfaites, la différence entre deux termes consécutifs de la suite tend vers l'infini.*

Conjecture de Pillai :

• Pillai's Conjecture : *Dans la suite des puissances parfaites, la différence entre deux termes consécutifs de la suite tend vers l'infini.*

• Équivalent : Soit k un entier positif. L'équation

$$x^p - y^q = k,$$

où les inconnues x, y, p et q prennent des valeurs entières, toutes ≥ 2, n'a qu'un nombre fini de solutions (x, y, p, q).

Conjecture de Pillai

Pillai, S. S. – *On the equation* $2^x - 3^y = 2^X + 3^Y$, Bull. Calcutta Math. Soc. 37, (1945). 15–20.
Je profite de l'occasion pour publier une conjecture que j'ai proposée durant la conference de l'Indian Mathematical Society qui s'est tenue à Aligarh.
Énumérons la liste des puissances parfaites : carrés, cubes, puissances cinquièmes, etc. en ordre croissant :

$$1,\ 4,\ 8,\ 9,\ 16,\ 25,\ 27,\ 32,\ 36,\ 49,\ 64,\ 81,\ 100,\ 121,\ 125,\ 128, \ldots$$

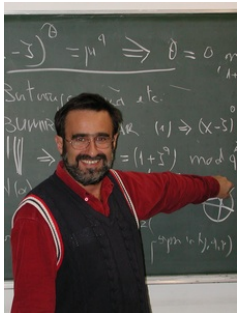
Soit a_n *le* n*-ème élément de cette suite :* $a_1 = 1$, $a_2 = 4$, $a_3 = 8$, $a_4 = 9$, *etc. Alors*
Conjecture :

$$\liminf(a_n - a_{n-1}) = \infty.$$

Résultats

P. Mihăilescu, 2002.

Catalan avait raison :
l'équation $x^p - y^q = 1$ *où les inconnues* x, y, p *et* q *prennent des valeurs entières, toutes* ≥ 2, *n'a que la solution* $(x, y, p, q) = (3, 2, 2, 3)$.



Résultats partiels antérieures : J.W.S. Cassels, R. Tijdeman, M. Mignotte,...

Valeurs supérieures de k

Il n'existe aucune valeur de $k > 1$ pour laquelle on sache démontrer que l'équation de Pillai $x^p - y^q = k$ n'a qu'un nombre fini de solutions.

La conjecture de Pillai est une conséquence de la conjecture abc :

$$|x^p - y^q| \geq c(\epsilon) \max\{x^p, y^q\}^{\kappa - \epsilon}$$

avec

$$\kappa = 1 - \frac{1}{p} - \frac{1}{q}.$$

La conjecture abc

- Quand n est un entier positif, on note

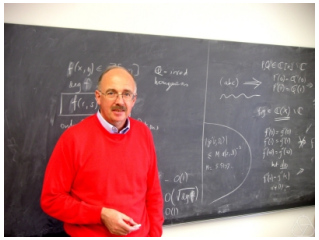
$$R(n) = \prod_{p|n} p$$

le *radical* ou *partie sans facteur carré* de n.

- Conjecture abc . *Pour tout $\varepsilon > 0$ il existe $\kappa(\varepsilon)$ tel que, si a, b et c dans $\mathbf{Z}_{>0}$ sont premiers entre eux et vérifient $a + b = c$, alors*

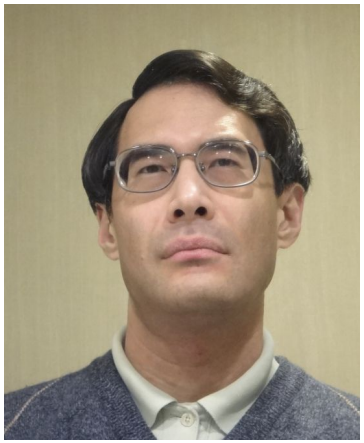
$$c < \kappa(\varepsilon) R(abc)^{1+\varepsilon}.$$

La conjecture abc de Œsterlé et Masser



La conjecture abc provient d'une discussion entre J. Œsterlé et D. W. Masser vers 1980.

Shinichi Mochizuki



INTER-UNIVERSAL TEICHMÜLLER THEORY IV : LOG-VOLUME COMPUTATIONS AND SET-THEORETIC FOUNDATIONS
by
Shinichi Mochizuki

http://www.kurims.kyoto-u.ac.jp/∼motizuki/

Textes de Shinichi Mochizuki

- General Arithmetic Geometry
- Intrinsic Hodge Theory
- p–adic Teichmuller Theory
- Anabelian Geometry, the Geometry of Categories
- The Hodge-Arakelov Theory of Elliptic Curves
- Inter-universal Teichmuller Theory

Shinichi Mochizuki

[1] Inter-universal Teichmuller Theory I : Construction of Hodge Theaters. PDF

[2] Inter-universal Teichmuller Theory II : Hodge-Arakelov-theoretic Evaluation. PDF

[3] Inter-universal Teichmuller Theory III : Canonical Splittings of the Log-theta-lattice. PDF

[4] Inter-universal Teichmuller Theory IV : Log-volume Computations and Set-theoretic Foundations. PDF

Équation de Beal $x^p + y^q = z^r$

Supposons

$$\frac{1}{p} + \frac{1}{q} + \frac{1}{r} < 1$$

et x, y, z premiers entre eux.

On connaît exactement 10 solutions (à symétrie évidente près) :

$$1 + 2^3 = 3^2, \quad 2^5 + 7^2 = 3^4, \quad 7^3 + 13^2 = 2^9, \quad 2^7 + 17^3 = 71^2,$$

$$3^5 + 11^4 = 122^2, \quad 17^7 + 76271^3 = 21063928^2,$$

$$1414^3 + 2213459^2 = 65^7, \quad 9262^3 + 15312283^2 = 113^7,$$

$$43^8 + 96222^3 = 30042907^2, \quad 33^8 + 1549034^2 = 15613^3.$$

Beal Conjecture and prize problem

"Conjecture de Fermat-Catalan" (H. Darmon et A. Granville) : *l'ensemble des solutions (x, y, z, p, q, r) de l'équation $x^p + y^q = z^r$ avec $(1/p) + (1/q) + (1/r) < 1$ est fini.*

C'est une conséquence de la conjecture abc.
`Indication:`

$$\frac{1}{p} + \frac{1}{q} + \frac{1}{r} < 1 \quad \text{implique} \quad \frac{1}{p} + \frac{1}{q} + \frac{1}{r} \leq \frac{41}{42}.$$

Conjecture de R. Tijdeman, D. Zagier et A. Beal : *il n'y a aucune solution à l'équation $x^p + y^q = z^r$ avec p, q et r tous ≥ 3.*

Beal conjecture and prize problem

Pour une démonstration ou un contre exemple publié dans un journal avec rapporteur, A. Beal a offert un prix de 5 000 US $ en 1997, l'augmentant jusqu'à 50 000 US $ sur 10 ans ; depuis il l'a monté à 1 000 000 US $.

R. D. Mauldin, *A generalization of Fermat's last theorem : the Beal conjecture and prize problem*, Notices Amer. Math. Soc., 44 (1997), pp. 1436–1437.

http://www.ams.org/profession/prizes-awards/ams-supported/beal-prize

Problème de Waring

Edward Waring
(1736 - 1798)

En 1770, quelques mois avant que J.L. Lagrange résolve une conjecture de Bachet et Fermat en montrant que tout entier positif est somme d'au plus quatre carrés, E. Waring a écrit :

"Tout entier est un cube, ou la somme de deux, trois, . . . neuf cubes ; tout entier est aussi le carré d'un carré, ou la somme d'au plus 19 tels nombres ; et ainsi de suite. Des lois semblables peuvent être énoncées pour les nombres définis de manière similaire quelque soit le degré."

Théorème (D. Hilbert, 1909)

Pour tout entier positif k, il existe un entier $s(k)$ tel que tout entier positif est somme d'au plus $s(k)$ puissances k-èmes.

La fonction $g(k)$ de Waring

• La fonction $g(k)$ de Waring est définie de la manière suivante : *Pour tout entier $k \geq 2$, $g(k)$ est le plus petit entier s tel que tout entier positif N peut être écrit $x_1^k + \cdots + x_s^k$.*

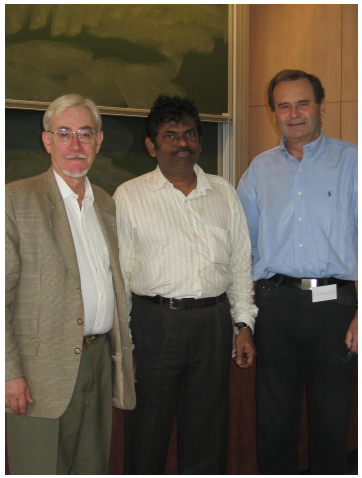
• Conjecture (Le théorème de Waring idéal) : *Pour chaque entier $k \geq 2$,*

$$g(k) = 2^k + [(3/2)^k] - 2.$$

• Cette formule est vraie pour $3 \leq k \leq 471\ 600\ 000$, et aussi, d'après K. Mahler, pour tout entier k suffisamment grand.

$n = x_1^4 + \cdots + x_g^4 : g(4) = 19$

Tout entier positif est somme eau plus 19 *bicarrés*
R. Balasubramanian,
J-M. Deshouillers,
F. Dress
(1986).



Le problème de Waring et la conjecture abc

S. David : la majoration

$$\left\| \left(\frac{3}{2}\right)^k \right\| \geq \left(\frac{3}{4}\right)^k,$$

(pour k suffisamment grand) résulte
non seulement des travaux de Mahler, mais aussi de la conjecture abc.

Par conséquent le théorème de Waring idéal
$g(k) = 2^k + [(3/2)^k] - 2$ résulterait d'une version explicite de la conjecture abc.

La fonction de Waring $G(k)$

• La fonction de Waring G est définie de la manière suivante : *Pour chaque entier* $k \geq 2$, $G(k)$ *est le plus petit entier positif* s *tel que tout entier* N *suffisamment grand puisse être écrit sous la forme* $x_1^k + \cdots + x_s^k$.

• Les deux seules valeurs connues de $G(k)$ sont $G(2) = 4$ et $G(4) = 16$

$G(2) = 4$

Joseph-Louis Lagrange
(1736–1813)

Démonstration d'une conjecture de Bachet et Fermat en 1770 :

Tout entier positif est la somme d'au plus quatre carrés.

Un entier congru à -1 *modulo* 8 *n'est pas la somme de trois carrés.*

$G(k)$

Kempner (1912) $G(4) \geq 16$
$16^m \cdot 31$ nécessite au moins 16 bicarrés

Hardy Littlewood (1920) $G(4) \leq 21$
méthode du cercle

Davenport, Heilbronn, Esterman (1936) $G(4) \leq 17$

Davenport (1939) $G(4) = 16$

Yu. V. Linnik (1943) $g(3) = 9$, $G(3) \leq 7$

Autres estimations pour $G(k)$, $k \geq 5$: Davenport, K. Sambasiva Rao, V. Narasimhamurti, K. Thanigasalam, R.C. Vaughan,...

Version explicite de la conjecture abc par Baker

Alan Baker

Shanta Laishram

Nombres réels : rationnels, irrationnels

Nombres rationnels :
a/b avec a et b entiers rationnels, $b > 0$.

Représentation irréductible :
p/q avec p et q dans $\mathbf{Z}$, $q > 0$ et $\mathrm{pgcd}(p, q) = 1$.

Nombre irrationnel : nombre (réel) qui n'est pas rationnel.

Nombres complexes : algébriques, transcendants

Nombre algébrique : nombre complexe racine d'un polynôme à coefficients rationnels.

Exemples :
nombres rationnels : a/b, racine de $bX - a$.
$\sqrt{2}$,racine de $X^2 - 2$.
i, racine de $X^2 + 1$.
$e^{2i\pi/n}$, racine de $X^n - 1$.

La somme et le produit de nombres algébriques sont des nombres algébriques. L'ensemble $\overline{\mathbf{Q}}$ des nombres complexes algébriques forme un corps, la clôture algébrique de $\mathbf{Q}$ dans $\mathbf{C}$.

Un nombre transcendant est un nombre complexe qui n'est pas algébrique.

Problème inverse de Galois

Evariste Galois
(1811 – 1832)

Un *corps de nombres* est une extension finie de $\mathbf{Q}$.

Est-il vrai que tout groupe fini G est le groupe de Galois sur $\mathbf{Q}$ d'un corps de nombres ?

Le *groupe de Galois absolu du corps* $\mathbf{Q}$ est le groupe $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ des automorphisms du corps $\overline{\mathbf{Q}}$ des nombres algébriques. Il s'agit de savoir si tout groupe fini G est un quotient de $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$.

Périodes : Maxime Kontsevich et Don Zagier

Periods,
Mathematics unlimited—2001 and beyond,
Springer 2001,
771–808.

Une *période* est un nombre complexe dont les parties réelles et imaginaires sont les valeurs d'intégrales absolument convergentes de fractions rationnelles à coefficients rationnels sur des domaines de $\mathbf{R}^n$ définis par des (in)égalités polynomiales à coefficients rationnels.

Le nombre π

Exemple fondamental d'une *période* :

$$e^{z+2i\pi} = e^z$$

$$2i\pi = \int_{|z|=1} \frac{dz}{z}$$

$$\begin{aligned} \pi &= \int\int_{x^2+y^2\le 1} dxdy &&= 2\int_{-1}^{1} \sqrt{1-x^2}dx \\ &= \int_{-1}^{1} \frac{dx}{\sqrt{1-x^2}} &&= \int_{-\infty}^{\infty} \frac{dx}{1-x^2}. \end{aligned}$$

Autres exemples de périodes

$$\sqrt{2} = \int_{2x^2\le 1} dx$$

et tous les nombres algébriques.

$$\log 2 = \int_{1<x<2} \frac{dx}{x}$$

et tous les logarithmes de nombres algébriques.

$$\pi = \int_{x^2+y^2\le 1} dxdy,$$

Un produit de périodes est une période (sous-algèbre de $\mathbf{C}$ sur $\overline{\mathbf{Q}}$), mais on s'attend à ce que $1/\pi$ ne soit pas une période.

Relations entre périodes

1 Additivité

(quantité à intégrer et domaine d'intégration)

$$\int_a^b \big(f(x)+g(x)\big)dx = \int_a^b f(x)dx + \int_a^b g(x)dx,$$

$$\int_a^b f(x)dx = \int_a^c f(x)dx + \int_c^b f(x)dx.$$

2 Changement de variables :

Si $y = f(x)$ est un changement de variables inversible, alors

$$\int_{f(a)}^{f(b)} F(y)dy = \int_a^b F\big(f(x)\big)f'(x)dx.$$

Relations entre périodes (suite)

3 Formule de Newton–Leibniz–Stokes

$$\int_a^b f'(x)dx = f(b) - f(a).$$

Conjecture de Kontsevich et Zagier

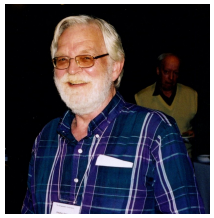
Une croyance répandue,
fondée sur
une combinaison judicieuse
d'expérience, d'analogie
et de prise de ses désirs
pour des réalités,
est la suivante

Conjecture (Kontsevich–Zagier). *Si une période a deux représentations, on peut passer d'une des deux formules à l'autre en utilisant seulement les trois règles 1, 2, 3 dans lesquelles toutes les fonctions et les domaines d'intégration sont algébriques avec des coefficients algébriques.*

Conjecture de Kontsevich et Zagier (suite)

En d'autres termes, on ne s'attend pas à ce qu'il existe des coïncidences miraculeuses entre deux intégrales de fonctions algébriques qu'il ne serait pas possible de démontrer à l'aide seulement de ces trois règles simples.
Cette conjecture, dont l'esprit est semblable à la conjecture de Hodge, est une des conjectures centrales sur l'indépendance algébrique et la transcendance de nombres, elle est liée à de nombreux résultats et de nombreuses idées de la géométrie algébrique arithmétique moderne et à la théorie des motifs.

Conjectures de S. Schanuel, A. Grothendieck et Y. André



• Schanuel : *si $x_1, \ldots, x_n$ sont des nombres complexes linéairement indépendants sur $\mathbf{Q}$, alors n au moins parmi les $2n$ nombres $x_1, \ldots, x_n$, $e^{x_1}, \ldots, e^{x_n}$ sont algébriquement indépendent.*

• Conjecture des périodes de Grothendieck sur la dimension du groupe de Mumford–Tate d'une variété projective lisse.

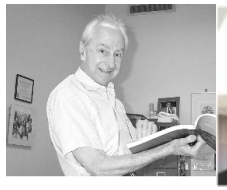
• Y. André : généralisations aux motifs.

S. Ramanujan, C.L. Siegel, S. Lang, K. Ramachandra

Ramanujan : Nombres hautement composés.

Alaoglu et Erdős (1944), Siegel, Schneider, Lang, Ramachandra






Conjecture des quatre exponentielles

Soit t un nombre réel positif. Supposons que les deux nombres 2^t et 3^t sont entiers. Montrer que t est entier.

De façon équivalente :
Si n est un entier positif tel que

$$n^{(\log 3)/\log 2}$$

est un entier, alors n est une puissance de 2 :

$$2^{k(\log 3)/\log 2} = 3^k.$$

Premières décimales de $\sqrt{2}$ http://wims.unice.fr/wims/wims.cgi

1.41421356237309504880168872420969807856967187537694807317667973
7990732478462107038850387534327641572735013846230912297024924836055850737212644121497099935831413222665927505592755799950501152782060571470109559971605970274534596862014728517418640889198609552329230484308714321450839762603627995251407989687253396546331808829640620615258352395054745750287759961729835575220337531857011354374603408498847160386899970699004815030544027790316454247823068492936918621580578463111596668713013015618568987237235288509264861249497715421833420428568606014682472077143585487415565706967765372022648544701585880162075847492265722600208558446652145839889394437092659180031138824646815708263010059485870400318648034219489727829064104507263688131373985525611732204024509122770022694112757362728049573810896750401836986836845072579936472906076299694138047565482372899718032680247442062926912485905218100445984215059112024944134172853147810580360337107730918286931471017111168391658172688941975871658215212822951848847 ...

Benoit Rittaud
http://www.math.univ-paris13.fr/~rittaud/RacineDeDeux

Premiers chiffres binaires de $\sqrt{2}$

http://wims.unice.fr/wims/wims.cgi

1.01101010000010011110011001100111111100111011110011001001000
10001011001011111011000100110110011011101010100101010111110100
11111000111010110111101100000101110101000100100111011101010000
10011001110110100010111101011001000010110000011001100111001100
10001010101001010111111001000001100000100001110101011100010100
01011000011101010001011000111111110011011111101110010000011110
11011001110010000111101110100101010000101111001000011100111000
11110110100101001111000000001001000011100110110001111011111101
00010011101101000110100100010000000101110100001110100001010101
11100011111010011100101001100000101100111000110000000010001101
11100001100110111011110011010101100011011110010010001000101101
00010000100010110001010010001100000101010111100011100100010111
10111110001001110001100111100011011010101101010001010001110001
01110110111111010011101110011001011001010100110001101000011001
10001111100111100100001001101111101010010111100010010000011111
00000110110111001011000001011101110101010100100101000001000100
11001000001000000110010100100101010000001001110010100101010 . . .

Calcul des décimales de $\sqrt{2}$

$1\,542$ décimales calculées à la main par Horace Uhler en 1951

$14\,000$ décimales calculées en 1967

$1\,000\,000$ décimales calculées en 1971

$137 \cdot 10^9$ décimales calculées par Yasumasa Kanada et Daisuke Takahashi en 1997 avec Hitachi SR2201 en 7 heures et 31 minutes.

- Motivation : calcul de π.

Émile Borel (1871–1956)

- *Les probabilités dénombrables et leurs applications arithmétiques,*
Palermo Rend. **27**, 247-271 (1909).
Jahrbuch Database JFM 40.0283.01
http://www.emis.de/MATH/JFM/JFM.html

- *Sur les chiffres décimaux de $\sqrt{2}$ et divers problèmes de probabilités en chaînes,*
C. R. Acad. Sci., Paris **230**, 591-593 (1950).
Zbl 0035.08302

Émile Borel : 1950

Soient $g \geq 2$ un entier et x un nombre réel algébrique irrationnel. *Le développement en base g de x devrait satisfaire certaines des lois valables pour presque tous les nombres (pour la mesure de Lebesgue).*

Conjecture d'Émile Borel

Conjecture (É. Borel). *Soient x un nombre réel algébrique irrationnel, $g \geq 3$ un entier positif et a un entier dans l'intervalle $0 \leq a \leq g-1$. Alors le chiffre a apparaît au moins une fois dans le développement en base g de x.*
Corollaire. *Toute suite finie de chiffres devrait apparaître une infinité de fois dans le développement en base g de tout nombre réel algébrique irrationnel.*
(remplacer g par une puissance de g).

• Un nombre réel irrationnel dont le développement dans une base g possède une certaine régularité devrait être transcendant.

État de la question

On ne connaît aucun exemple explicite de triplet (g, a, x), où $g \geq 3$ est un entier, a un chiffre dans l'intervalle $\{0, \ldots, g-1\}$ et x un nombre réel algébrique irrationnel, pour lequel on puisse affirmer que le chiffre a apparaît une infinité de fois dans le développement en base g de x.

Une conjecture plus forte, également due à Borel, est qu'un nombre réel algébrique irrationnel est *normal* : toute suite finie de n chiffres en base g devrait apparaître avec la fréquence $1/g^n$, ceci pour tout g et tout n.

Complexité du développement en base g d'un nombre réel algébrique irrationnel

Théorème (B. Adamczewski, Y. Bugeaud 2005 ; conjecture de A. Cobham 1968).
si la suite des chiffres d'un nombre réel x peut être obtenue par un automate fini, alors x est soit rationnel, soit transcendant.

Problèmes ouverts (irrationalité)

• Le nombre

$$e + \pi = 5.859\,874\,482\,048\,838\,473\,822\,930\,854\,632\ldots$$

est-il irrationnel ?
• Le nombre

$$e\pi = 8.539\,734\,222\,673\,567\,065\,463\,550\,869\,546\ldots$$

est-il irrationnel ?
• Le nombre

$$\log \pi = 1.144\,729\,885\,849\,400\,174\,143\,427\,351\,353\ \ldots$$

est-il irrationnel ?

La constante de Catalan

La constante de Catalan
$$\sum_{n\geq 1} \frac{(-1)^n}{(2n+1)^2}$$
$$= 0.915\,965\,594\,177\,219\,015\,0\ldots$$
est-elle irrationnelle ?

Fonction zêta de Riemann

La fonction
$$\zeta(s) = \sum_{n\geq 1} \frac{1}{n^s}$$
a été étudiée par Euler (1707– 1783)
pour s entier
et par Riemann (1859) pour s complexe.

Euler : pour toute valeur paire de l'entier $s \geq 2$, le nombre $\zeta(s)$ est un multiple rationnel de π^s.

Exemples : $\zeta(2) = \pi^2/6$, $\zeta(4) = \pi^4/90$, $\zeta(6) = \pi^6/945$, $\zeta(8) = \pi^8/9450\cdots$

Coefficients : Nombres de Bernoulli.

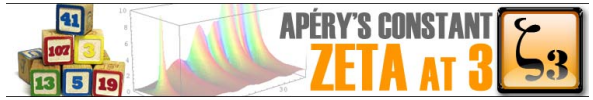
Introductio in analysin infinitorum

Leonhard Euler

(1707 – 1783)

Introductio in analysin infinitorum
(1748)

Fonction zêta de Riemann



Le nombre
$$\zeta(3) = \sum_{n\geq 1} \frac{1}{n^3} = 1,202\,056\,903\,159\,594\,285\,399\,738\,161\,511\ldots$$
est irrationnel *(Apéry 1978)*.

Rappelons que $\zeta(s)/\pi^s$ est rationnel pour toute valeur paire de $s \geq 2$.

Question ouverte : Le nombre $\zeta(3)/\pi^3$ est-il irrationnel ?

Fonction zêta de Riemann

Le nombre

$$\zeta(5) = \sum_{n\geq 1} \frac{1}{n^5} = 1.036\,927\,755\,143\,369\,926\,331\,365\,486\,457\ldots$$

est-il irrationnel ?

T. Rivoal (2000) : irrationalité d'une infinité de nombres de la forme $\zeta(2n+1)$.

F. Brown (2014) : Irrationality proofs for zeta values, moduli spaces and dinner parties arXiv:1412.6508

Constante d'Euler–Mascheroni

Lorenzo Mascheroni
(1750 – 1800)

La constante d'Euler est

$$\gamma = \lim_{n\to\infty} \left(1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n} - \log n\right)$$
$$= 0.577\,215\,664\,901\,532\,860\,606\,512\,090\,082\ldots$$

Est-ce un nombre irrationnel ?

$$\gamma = \sum_{k=1}^{\infty} \left(\frac{1}{k} - \log\left(1 + \frac{1}{k}\right)\right) = \int_1^{\infty} \left(\frac{1}{[x]} - \frac{1}{x}\right) dx$$
$$= -\int_0^1 \int_0^1 \frac{(1-x)dxdy}{(1-xy)\log(xy)}.$$

Autres problèmes ouverts

- Conjecture d'Artin (1927) : étant donné un entier a différent de -1 qui n'est pas un carré, il y a une infinité de p tels que a est une racine primitive modulo p.
(+ estimation conjecturale asymptotique pour la densité).
- Problème de Lehmer : Soit $\theta \neq 0$ un nombre algébrique de degré d. On pose $M(\theta) = \prod_{i=1}^{d} \max(1, |\theta_i|)$, où $\theta = \theta_1$ et $\theta_2, \cdots, \theta_d$ sont les conjugués de θ. Existe-t-il une constante $c > 1$ telle que la majoration $M(\theta) < c$ implique que θ est une racine de l'unité ?
$c < 1.176280\ldots$ (Lehmer 1933).
- Hypothèse H de Schinzel. Cas particulier : *existe-t-il une infinité de nombres premiers de la forme $x^2 + 1$?*
- La conjecture de Birch et Swinnerton–Dyer
- Le programme de Langlands

Équation de Collatz (Problème de Syracuse)

On itère

$$n \longmapsto \begin{cases} n/2 & \text{si } n \text{ est pair,} \\ 3n+1 & \text{si } n \text{ est impair.} \end{cases}$$

Est-il vrai que $(4, 2, 1)$est le seul cycle ?

Mardi 13 janvier 2015

USTHB, Alger

Quelques problèmes ouverts en théorie des nombres

Michel Waldschmidt

Institut de Mathématiques de Jussieu — Paris VI

http://www.math.jussieu.fr/∼miw/