update: 2023

Some of the most famous open problems in number theory

Michel Waldschmidt

Sorbonne Université
Institut de Mathématiques de Jussieu – Paris Rive Gauche
http://www.imj-prg.fr/~michel.waldschmidt

Abstract

Problems in number theory are sometimes easy to state and often very hard to solve. We survey some of them.

Extended abstract

We start with prime numbers. The twin prime conjecture and the Goldbach conjecture are among the main challenges.

The largest known prime numbers are Mersenne numbers. Are there infinitely many Mersenne (resp. Fermat) prime numbers?
Mersenne prime numbers are also related with perfect numbers, a problem considered by Euclid and still unsolved.

One the most famous open problems in mathematics is Riemann's hypothesis, which is now more than 150 years old.

Extended abstract (continued)

Diophantine equations conceal plenty of mysteries. Fermat's Last Theorem has been proved by A. Wiles, but many more questions are waiting for an answer. We discuss a conjecture due to S.S. Pillai, as well as the abc-Conjecture of Oesterlé–Masser.

Kontsevich and Zagier introduced the notion of *periods* and suggested a far reaching statement which would solve a large number of open problems of irrationality and transcendence.

Finally we discuss open problems (initiated by E. Borel in 1905 and then in 1950) on the decimal (or binary) expansion of algebraic numbers. Almost nothing is known on this topic.

Hilbert's 8th Problem

August 8, 1900

David Hilbert (1862 - 1943)

Second International Congress of Mathematicians in Paris.

Twin primes,

Goldbach's Conjecture,

Riemann Hypothesis

The seven Millennium Problems

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

7 million US$ prize fund for the solution to these problems, with 1 million US$ allocated to each of them.

Paris, May 24, 2000:
Timothy Gowers, John Tate and Michael Atiyah.

- Birch and Swinnerton-Dyer Conjecture
- Hodge Conjecture
- Navier-Stokes Equations
- P vs NP
- Poincaré Conjecture
- Riemann Hypothesis
- Yang-Mills Theory

Numbers

Numbers $=$ real or complex numbers $\mathbb{R}$, $\mathbb{C}$.

Natural integers: $\mathbb{N} = \{0, 1, 2, \ldots\}$.

Rational integers: $\mathbb{Z} = \{0, \pm 1, \pm 2, \ldots\}$.

Prime numbers

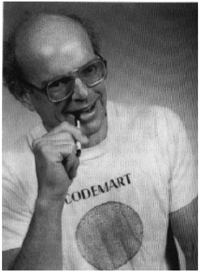
Numbers with exactly two divisors.

There are 25 prime numbers less than 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



Neil J. A. Sloane

Composite numbers

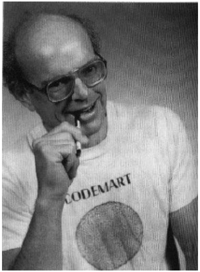
Numbers with more than two divisors:

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

http://oeis.org/A002808

The composite numbers: numbers n of the form $x \cdot y$ for $x > 1$ and $y > 1$.

There are 73 composite numbers less than 100.



Euclid of Alexandria

(about 325 BC – about 265 BC)

Given any finite collection $p_1, \ldots, p_n$ *of primes, there is one prime which is not in this collection.*

Euclid numbers *primorial* primes, *factorial* primes

Set $p_n^{\#} = 2 \cdot 3 \cdot 5 \cdots p_n$.
Euclid numbers are the numbers of the form $p_n^{\#} + 1$.
$p_n^{\#} + 1$ is prime for $n = 0, 1, 2, 3, 4, 5, 11, \ldots$ (sequence A014545 in the OEIS).
The largest known prime Euclid number is $p_{33\,237}^{\#} + 1$ with $169\,966$ digits.

Kummer numbers are the numbers of the form $p_n^{\#} - 1$.
$p_n^{\#} - 1$ is prime for $n = 2, 3, 5, 6, 13, 24, \ldots$ (sequence A057704 in the OEIS).

Primorial primes are prime numbers of the form $p_n^{\#} \pm 1$. The largest known is $p_{3\,267\,113}^{\#} - 1$ with $1\,418\,398$ digits.

Factorial primes are prime numbers of the form $n! + 1$. The largest known is $4\,224\,29! + 1$ with $2\,193\,027$ digits (February 2022).

Largest explicitly known prime numbers

January 2019: $2^{82\,589\,933} - 1$ decimal digits $24,862,048$

January 2018: $2^{77\,232\,917} - 1$ decimal digits $23\,249\,425$

January 2016: $2^{74\,207\,281} - 1$ decimal digits $22\,338\,618$

February 2013: $2^{57\,885\,161} - 1$ decimal digits $17\,425\,170$

August 2008: $2^{43\,112\,609} - 1$ decimal digits $12\,978\,189$

June 2009: $2^{42\,643\,801} - 1$ decimal digits $12\,837\,064$

September 2008: $2^{37\,156\,667} - 1$ decimal digits $11\,185\,272$

Large prime numbers

One knows (as of *February 2023*)

- 8 prime numbers with 10^8 decimal digits
- 1821 prime numbers with more than 10^7 decimal digits
- 3211 prime numbers with more than 10^6 decimal digits

List of the $5\,000$ largest explicitly known prime numbers :
http://primes.utm.edu/largest.html

Mersenne primes

If a number of the form $a^k - 1$ is prime, then $a = 2$ and k is prime.

A prime number of the form $2^p - 1$ is called a Mersenne prime.

http://www.mersenne.org/

Marin Mersenne
1588 – 1648

Mersenne prime numbers

The smallest Mersenne primes are

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

51 Mersenne primes are known, among them 9 of the 12 largest explicitly known primes.

The ninth currently known largest explicit prime is $10\,223 \cdot 2^{31172165} + 1$, it has 9383761 decimal digits.

Are there infinitely many Mersenne primes?

Mersenne prime numbers

In 1536, Hudalricus Regius noticed that $2^{11} - 1 = 2\,047$ is not a prime number: $2\,047 = 23 \cdot 89$.

In the preface of *Cogitata Physica-Mathematica* (1644), Mersenne claimed that the numbers $2^n - 1$ are prime for

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

and that they are composite for all other values of $n < 257$.

The correct list is

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

http://oeis.org/A000043

Perfect numbers

A number is called perfect if it is equal to the sum of its divisors, excluding itself.
For instance 6 is the sum $1+2+3$, and the divisors of 6 are 1, 2, 3 and 6.
In the same way, the divisors of 28 are 1, 2, 4, 7, 14 and 28.
The sum $1+2+4+7+14$ is 28, hence 28 is perfect.

Notice that $6 = 2 \cdot 3$ and 3 is a Mersenne prime $2^2 - 1$.
Also $28 = 4 \cdot 7$ and 7 is a Mersenne prime $2^3 - 1$.

Other perfect numbers:

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

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

Perfect numbers

Euclid, Elements, Book IX: numbers of the form $2^{p-1} \cdot (2^p - 1)$ with $2^p - 1$ a (Mersenne) prime (hence p is prime) are perfect.

Euler (1747): all even perfect numbers are of this form.

Sequence of perfect numbers:

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

http://oeis.org/A000396

Are there infinitely many even perfect numbers?

Do there exist odd perfect numbers?

Fermat numbers

Fermat numbers are the numbers $F_n = 2^{2^n} + 1$.

Pierre de Fermat (1601 – 1665)

Fermat primes

$F_0 = 3$, $F_1 = 5$, $F_2 = 17$, $F_3 = 257$, $F_4 = 65537$ are prime
http://oeis.org/A000215

They are related with the construction of regular polygons with ruler and compass.

Fermat suggested in 1650 that all F_n are prime

Euler : $F_5 = 2^{32} + 1$ is divisible by 641

$$4294967297 = 641 \cdot 6700417$$

Fermat primes

$F_5 = 2^{32} + 1$ is divisible by 641

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

$$\begin{aligned} &5^4 \equiv -2^4 \pmod{641}, \\ &5 \cdot 2^7 \equiv -1 \pmod{641}, \\ &5^4 2^{28} \equiv 1 \pmod{641}, \\ &2^{32} \equiv -1 \pmod{641}. \end{aligned}$$

Are there infinitely many Fermat primes? Only five are known.

Twin primes

Conjecture: *there are infinitely many primes p such that $p+2$ is prime.*

Examples: $3, 5$, $5, 7$, $11, 13$, $17, 19$,...

More generally: *is every even integer (infinitely often) the difference of two primes? of two consecutive primes?*

Largest known example of twin primes (found in Sept. 2016) with $388\,342$ decimal digits:

$$2\,996\,863\,034\,895 \cdot 2^{1\,290\,000} \pm 1$$

http://primes.utm.edu/

Conjecture (Hardy and Littlewood, 1915)

Twin primes

The number of primes $p \le x$ such that $p+2$ is prime is

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

where

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

Circle method

Srinivasa Ramanujan
(1887 – 1920)

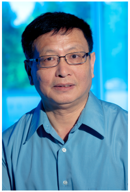
G.H. Hardy
(1877 – 1947)

J.E. Littlewood
(1885 – 1977)

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

Small gaps between primes

In 2013, Yitang Zhang proved that infinitely many gaps between prime numbers do not exceed $70 \cdot 10^6$.



Yitang Zhang
(1955 -)

http://en.wikipedia.org/wiki/Prime_gap

Polymath8a, July 2013: 4680

James Maynard, November 2013: 576

Polymath8b, December 2014: 246

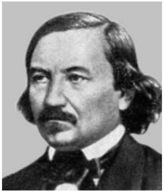
EMS Newsletter December 2014 issue 94 p. 13–23.

No large gaps between primes

Bertrand's Postulate. *There is always a prime between n and $2n$.*

Chebychev (1851):

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



Joseph Bertrand
(1822 - 1900)

Pafnuty Lvovich Chebychev
(1821 – 1894)

Legendre question (1808)

Question: Is there always a prime between n^2 and $(n+1)^2$?

Adrien–Marie Legendre
1752–1834

Louis Legendre
1755–1797

This caricature by J-L Boilly is the only known portrait of Adrien-Marie Legendre.
Louis Legendre was an active participant in the French Revolution.

https://mathshistory.st-andrews.ac.uk/Biographies/Legendre/
Peter Duren. Changing Faces: The Mistaken Portrait of Legendre.
www.ams.org/notices/200911/rtx091101440p.pdf

Leonhard Euler (1707 – 1783)

For $s > 1$,

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

For $s = 1$:

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

Johann Carl Friedrich Gauss (1777 – 1855)

Let p_n be the n-th prime.

Gauss introduces

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

He observes numerically

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

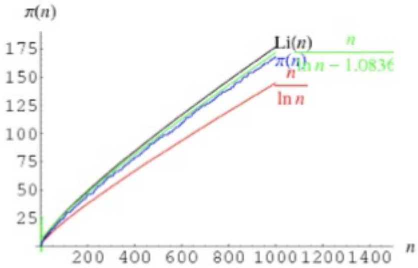
Define the density $\mathrm{d}\pi$ by

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

Problem: estimate from above

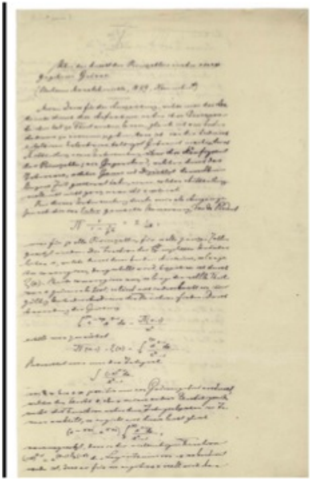
$$E(x) = \left| \pi(x) - \int_0^x \frac{\mathrm{d}t}{\log t} \right|.$$

Plot

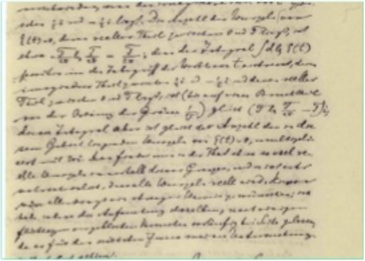


π(n)
175
150
125
100
75
50
25
200
400
600
800
1000
1200
1400
n
Li(n)
π(n)
n
ln n − 1.0836
n
ln n

Riemann 1859 Critical strip, critical line



$\zeta(s) = 0$
with $0 < \Re e(s) < 1$
implies
$\Re e(s) = 1/2$.



Riemann Hypothesis

> *Certainly one would wish for a stricter proof here; I have meanwhile temporarily put aside the search for this after some fleeting futile attempts, as it appears unnecessary for the next objective of my investigation.*

Über die Anzahl der Primzahlen unter einer gegebenen Grösse.

(Monatsberichte der Berliner Akademie, November 1859)

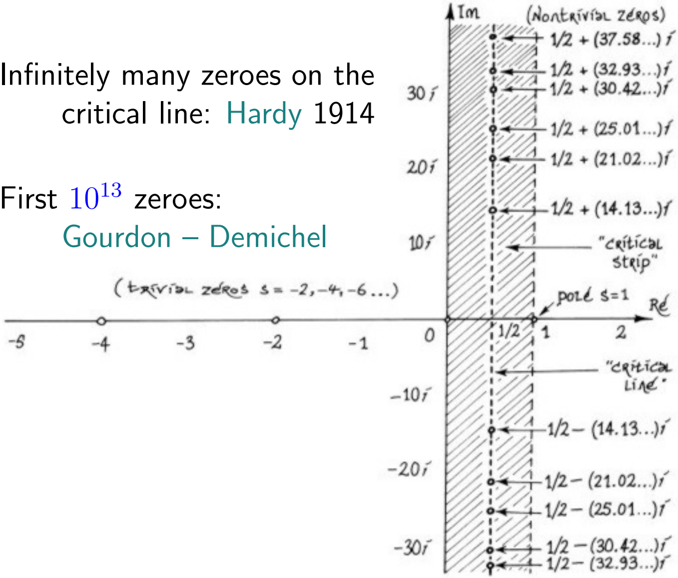
Bernhard Riemann's Gesammelte Mathematische Werke und Wissenschaftlicher Nachlass', herausgegeben under Mitwirkung von Richard Dedekind, von Heinrich Weber. (Leipzig: B. G. Teubner 1892). 145–153.

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

Small Zeros of Zeta

Infinitely many zeroes on the critical line: Hardy 1914

First 10^{13} zeroes:
Gourdon – Demichel



Riemann Hypothesis

Riemann Hypothesis is equivalent to :

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

for the remainder

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

Let $\mathrm{Even}(N)$ (resp. $\mathrm{Odd}(N)$) denote the number of positive integers $\leq N$ with an even (resp. odd) number of prime factors, counting multiplicities. Riemann Hypothesis is also equivalent to

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

Prime Number Theorem: $\pi(x) \simeq x/\log x$

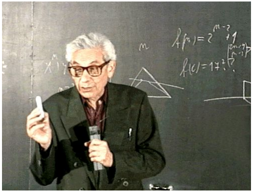
Jacques Hadamard
(1865 – 1963)

Charles de la Vallée Poussin
(1866 – 1962)

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

Prime Number Theorem: $p_n \simeq n \log n$

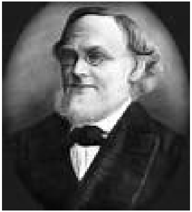
Elementary proof of the Prime Number Theorem (1949)



Paul Erdős
(1913 - 1996)

Atle Selberg
(1917 – 2007)

Goldbach's Conjecture



Christian Goldbach
(1690 – 1764)

Leonhard Euler
(1707 – 1783)

Letter of Goldbach to Euler, 1742: *any integer* ≥ 6 *is sum of* 3 *primes.*

Euler: Equivalent to :

Any even integer greater than 2 *can be expressed as the sum of two primes.*

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

Sums of two primes

$$
\begin{array}{cc}
4 = 2 + 2 & 6 = 3 + 3 \\
8 = 5 + 3 & 10 = 7 + 3 \\
12 = 7 + 5 & 14 = 11 + 3 \\
16 = 13 + 3 & 18 = 13 + 5 \\
20 = 17 + 3 & 22 = 19 + 3 \\
24 = 19 + 5 & 26 = 23 + 3 \\
\vdots & \vdots
\end{array}
$$

Circle method

Hardy and Littlewood

Ivan Matveevich Vinogradov (1891 – 1983)

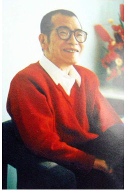
Every sufficiently large odd integer is the sum of at most three primes.

Sums of primes

Theorem – I.M. Vinogradov (1937)
Every sufficiently large odd integer is a sum of three primes.

Theorem – Chen Jing-Run (1966)
Every sufficiently large even integer is a sum of a prime and an integer that is either a prime or a product of two primes.

Ivan Matveevich Vinogradov
(1891 – 1983)



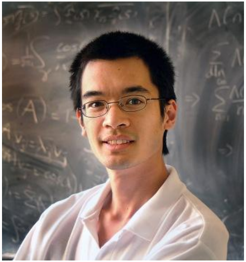
Chen Jing Run
(1933 - 1996)

Sums of primes

- 27 is neither prime nor a sum of two primes

- Weak (or ternary) Goldbach Conjecture: *every odd integer ≥ 7 is the sum of three odd primes.*

- Terence Tao, February 4, 2012, `arXiv:1201.6656`: *Every odd number greater than 1 is the sum of at most five primes.*



Ternary Goldbach Problem

Theorem – Harald Helfgott (2013).
Every odd number greater than 5 *can be expressed as the sum of three primes.*
Every odd number greater than 7 *can be expressed as the sum of three odd primes.*

Harald Helfgott
(1977-)

Earlier results due to Hardy and Littlewood (1923), Vinogradov (1937), Deshouillers et al. (1997), and more recently Ramaré, Kaniecki, Tao ...

Lejeune Dirichlet (1805 – 1859)

Prime numbers in arithmetic progressions.

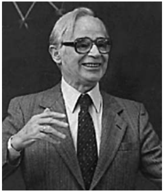
$$a,\ a+q,\ a+2q,\ a+3q,\ \ldots$$

1837:
For $\gcd(a,q)=1$,

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

Arithmetic progressions: van der Waerden

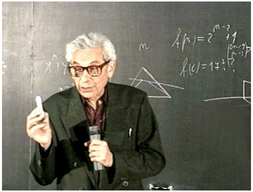
Theorem – B.L. van der Waerden (1927).
If the integers are coloured using finitely many colours, then one of the colour classes must contain arbitrarily long arithmetic progressions.



Bartel Leendert van der Waerden
(1903 - 1996)

Arithmetic progressions: Erdős and Turán

Conjecture – P. Erdős and P. Turán (1936).
Any set of positive integers for which the sum of the reciprocals diverges should contain arbitrarily long arithmetic progressions.



Paul Erdős
(1913 - 1996)

Paul Turán
(1910 - 1976)

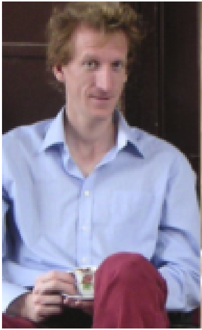
Arithmetic progressions: E. Szemerédi

Theorem – E. Szemerédi (1975).
Any subset of the set of integers of positive density contains arbitrarily long arithmetic progressions.

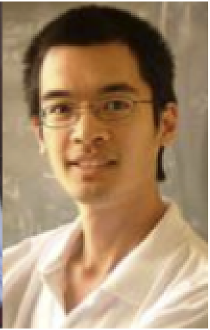
Endre Szemerédi
(1940 -)

Primes in arithmetic progression

Theorem – B. Green and T. Tao (2004).
The set of prime numbers contains arbitrarily long arithmetic progressions.



Barry Green



Terence Tao

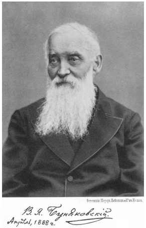
Further open problems on prime numbers

Euler: are there infinitely many primes of the form $x^2 + 1$? also a problem of Hardy – Littlewood and of Landau.

Conjecture of Bunyakovsky : prime values of one polynomial.

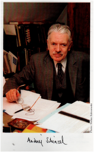
Schinzel hypothesis H: simultaneous prime values of several polynomial.

Bateman – Horn conjecture: quantitative refinement (includes the density of twin primes).



Viktor Bunyakovsky

(1804 – 1889)

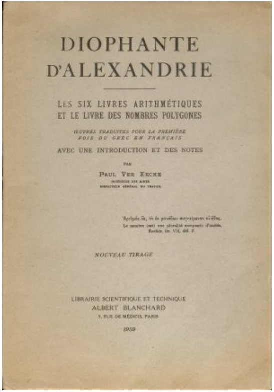


Andrzej Schinzel

(1937 – 2021)

Diophantine Problems

Diophantus of Alexandria (250 $\pm$50)



DIOPHANTE
D'ALEXANDRIE

LES SIX LIVRES ARITHMÉTIQUES
ET LE LIVRE DES NOMBRES POLYGONES

ŒUVRES TRADUITES POUR LA PREMIÈRE
FOIS DU GREC EN FRANÇAIS

AVEC UNE INTRODUCTION ET DES NOTES

PAR

PAUL VER EECKE

NOUVEAU TIRAGE

LIBRAIRIE SCIENTIFIQUE ET TECHNIQUE
ALBERT BLANCHARD
9, RUE DE MÉDICIS, PARIS

1959

Fermat's Last Theorem $x^n + y^n = z^n$

Pierre de Fermat
1601 – 1665

Andrew Wiles
1953 –

Solution in June 1993 completed in 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

Square, cubes. . .

- A perfect power is an integer of the form a^b where $a \geq 1$ and $b > 1$ are positive integers.
- Squares:

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

- Cubes:

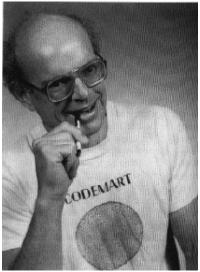
$$1,\ 8,\ 27,\ 64,\ 125,\ 216,\ 343,\ 512,\ 729,\ 1\,000,\ 1\,331,\ldots$$

- Fifth powers:

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

Perfect powers

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, ...



Neil J. A. Sloane's encyclopaedia
http://oeis.org/A001597

Consecutive elements in the sequence of perfect powers

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

Two conjectures

Subbayya Sivasankaranarayana Pillai (1901-1950)

Eugène Charles Catalan (1814 – 1894)

• Catalan's Conjecture: In the sequence of perfect powers, $8, 9$ is the only example of consecutive integers.

• Pillai's Conjecture: In the sequence of perfect powers, the difference between two consecutive terms tends to infinity.

Pillai's Conjecture:

- Pillai's Conjecture: In the sequence of perfect powers, the difference between two consecutive terms tends to infinity.

- Alternatively: Let k be a positive integer. The equation

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

where the unknowns x, y, p and q take integer values, all ≥ 2, has only finitely many solutions (x, y, p, q).

Pillai's conjecture

Pillai, S. S. – *On the equation* $2^x - 3^y = 2^X + 3^Y$, Bull. Calcutta Math. Soc. 37, (1945). 15–20.

I take this opportunity to put in print a conjecture which I gave during the conference of the Indian Mathematical Society held at Aligarh.

Arrange all the powers of integers like squares, cubes etc. in increasing order as follows:

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

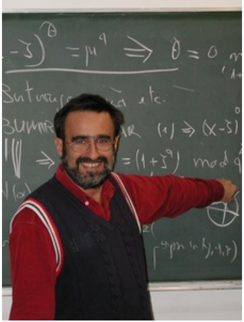
Let a_n *be the* n*-th member of this series so that* $a_1 = 1$, $a_2 = 4$, $a_3 = 8$, $a_4 = 9$, *etc. Then*

Conjecture:

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

Results

P. Mihăilescu, 2002.



Catalan was right: *the equation* $x^p - y^q = 1$ *where the unknowns* x, y, p *and* q *take integer values, all* ≥ 2, *has only one solution* $(x, y, p, q) = (3, 2, 2, 3)$.

Previous partial results: J.W.S. Cassels, R. Tijdeman, M. Mignotte,. . .

Higher values of k

There is no value of $k > 1$ for which one knows that Pillai's equation $x^p - y^q = k$ has only finitely many solutions.

Pillai's conjecture as a consequence of the abc conjecture:

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

with

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

The abc Conjecture

- For a positive integer n, we denote by

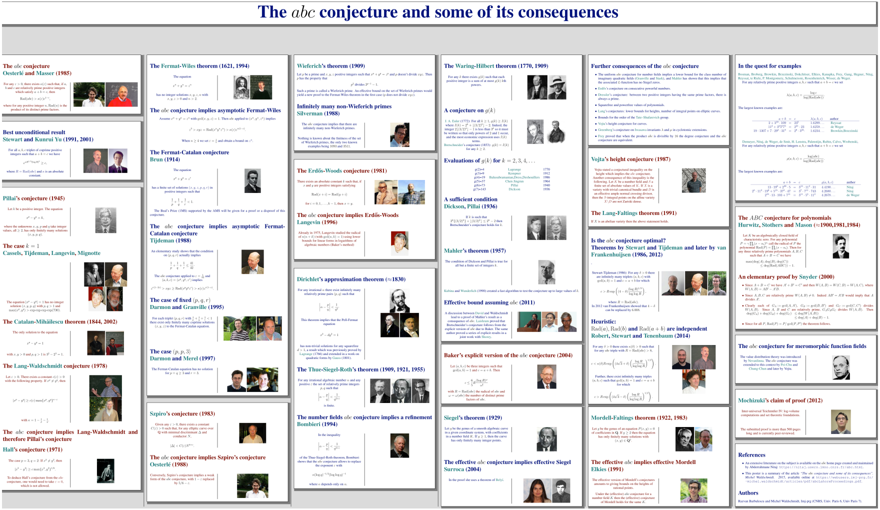
$$R(n) = \prod_{p|n} p$$

the *radical* or *the square free part* of n.

- Conjecture (abc Conjecture). *For each $\varepsilon > 0$ there exists $\kappa(\varepsilon)$ such that, if a, b and c in $\mathbb{Z}_{>0}$ are relatively prime and satisfy $a + b = c$, then*

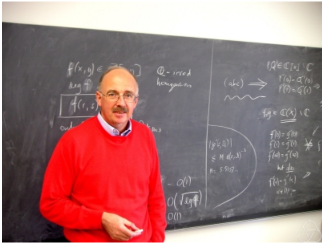
$$c < \kappa(\varepsilon) R(abc)^{1+\varepsilon}.$$

Poster with Razvan Barbulescu — Archives HAL



https://hal.archives-ouvertes.fr/hal-01626155

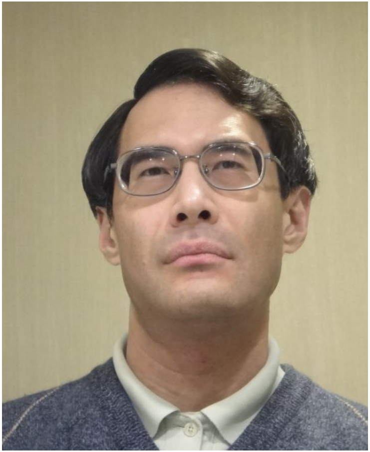
The *abc* Conjecture of Œsterlé and Masser



The *abc* Conjecture resulted from a discussion between J. Œsterlé and D. W. Masser around 1980.

M.W. On the *abc* conjecture and some of its consequences.
Mathematics in 21st Century, 6th World Conference, Lahore, March 2013,
(P. Cartier, A.D.R. Choudary, M. Waldschmidt Editors),
Springer Proceedings in Mathematics and Statistics **98** (2015), 211–230.

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/

Beal Equation $x^p + y^q = z^r$

Assume

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

and x, y, z are relatively prime

Only 10 solutions (up to obvious symmetries) are known

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

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

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

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

Beal Conjecture and prize problem

"Fermat-Catalan" Conjecture (H. Darmon and A. Granville) : *the set of solutions* (x, y, z, p, q, r) *to* $x^p + y^q = z^r$ *with* $\gcd(x, y, z) = 1$ *and* $(1/p) + (1/q) + (1/r) < 1$ *is finite.*

Consequence of the abc Conjecture. `Hint:`

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

Conjecture of R. Tijdeman, D. Zagier and A. Beal : *there is no solution to* $x^p + y^q = z^r$ *where* $\gcd(x, y, z) = 1$ *and each of* p, q *and* r *is* ≥ 3.

Beal conjecture and prize problem

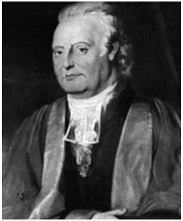
For a proof or a counterexample published in a refereed journal, A. Beal initially offered a prize of US $ 5,000 in 1997, raising it to $ 50,000 over ten years, but has since raised it to US $ 1,000,000.

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

Waring's Problem

In 1770, a few months before J.L. Lagrange solved a conjecture of Bachet and Fermat by proving that every positive integer is the sum of at most four squares of integers, E. Waring wrote:



Edward Waring
(1736 - 1798)

"Every integer is a cube or the sum of two, three, ... nine cubes; every integer is also the square of a square, or the sum of up to nineteen such; and so forth. Similar laws may be affirmed for the correspondingly defined numbers of quantities of any like degree."

Theorem. (D. Hilbert, 1909)

For each positive integer k, there exists an integer $g(k)$ such that every positive integer is a sum of at most $g(k)$ k-th powers.

Waring's function $g(k)$

- Waring's function g is defined as follows: *For any integer $k \geq 2$, $g(k)$ is the least positive integer s such that any positive integer N can be written $x_1^k + \cdots + x_s^k$.*

- Conjecture (The ideal Waring's Theorem): *For each integer $k \geq 2$,*

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

- This is true for $3 \leq k \leq 471\ 600\ 000$, and (K. Mahler) also for all sufficiently large k.

Evaluations of $g(k)$ for $k = 2, 3, 4, \ldots$

g(2)=4	Lagrange	1770
g(3)=9	Kempner	1912
g(4)=19	Balusubramanian,Dress,Deshouillers	1986
g(5)=37	Chen Jingrun	1964
g(6)=73	Pillai	1940
g(7)=143	Dickson	1936

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

Any positive integer is the sum of at most 19 *biquadrates*
R. Balasubramanian,
J-M. Deshouillers,
F. Dress
(1986).

$$79 = 4 \times 2^4 + 15 \times 1^5.$$

Waring's Problem and the abc Conjecture

S. David: the ideal Waring Theorem
$g(k) = 2^k + [(3/2)^k] - 2$
follows from an explicit solution of the abc Conjecture.

Baker's explicit abc conjecture

Alan Baker

Shanta Laishram

Waring's function $G(k)$

- Waring's function G is defined as follows: *For any integer $k \geq 2$, $G(k)$ is the least positive integer s such that any sufficiently large positive integer N can be written $x_1{}^k + \cdots + x_s{}^k$.*

- $G(k) \leq g(k)$.

- $G(k)$ is known only in two cases: $G(2) = 4$ and $G(4) = 16$

$G(2) = 4$

Joseph-Louis Lagrange
(1736–1813)

Solution of a conjecture of Bachet and Fermat in 1770:

Every positive integer is the sum of at most four squares of integers.

No integer congruent to -1 *modulo* 8 *can be a sum of three squares of integers.*

$G(k)$

Kempner (1912) $G(4) \geq 16$

$16^m \cdot 31$ needs at least 16 biquadrates

Hardy Littlewood (1920) $G(4) \leq 21$

circle method, singular series

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

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

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

Other estimates for $G(k)$, $k \geq 5$: Davenport, K. Sambasiva Rao, V. Narasimhamurti, K. Thanigasalam, R.C. Vaughan,. . .

Real numbers: rational, irrational

Rational numbers:
a/b with a and b rational integers, $b > 0$.

Irreducible representation:
p/q with p and q in $\mathbb{Z}$, $q > 0$ and $\gcd(p, q) = 1$.

Irrational number: a real number which is not rational.

Complex numbers: algebraic, transcendental

Algebraic number: a complex number which is a root of a non-zero polynomial with rational coefficients.

Examples:

rational numbers: a/b, root of $bX - a$.
$\sqrt{2}$, root of $X^2 - 2$.
i, root of $X^2 + 1$.
$e^{2\pi \mathrm{i}/n}$, root of $X^n - 1$.

The sum and the product of algebraic numbers are algebraic numbers. The set $\overline{\mathbb{Q}}$ of complex algebraic numbers is a field, the algebraic closure of $\mathbb{Q}$ in $\mathbb{C}$.

A transcendental number is a complex number which is not algebraic.

Inverse Galois Problem

Evariste Galois
(1811 – 1832)

A *number field* is a finite extension of $\mathbb{Q}$.

Is any finite group G the
Galois group over $\mathbb{Q}$ of a number field ?

Equivalently:
The *absolute Galois group of the field* $\mathbb{Q}$ is the group $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ of automorphisms of the field $\overline{\mathbb{Q}}$ of algebraic numbers. The previous question amounts to deciding whether any finite group G is a quotient of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$.

Periods: Maxime Kontsevich and Don Zagier

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

A *period* is a complex number whose real and imaginary parts are values of absolutely convergent integrals of rational functions with rational coefficients, over domains in $\mathbb{R}^n$ given by polynomial inequalities with rational coefficients.

The number π

Period of a function:

$$f(z+\omega) = f(z).$$

Basic example:

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

Connection with an integral:

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

The number π is a period:

$$\pi = \int\int_{x^2+y^2\leq 1} \mathrm{d}x\mathrm{d}y = \int_{-\infty}^{\infty} \frac{\mathrm{d}x}{1-x^2}.$$

Further examples of periods

$$\sqrt{2} = \int_{2x^2 \leq 1} \mathrm{d}x$$

and all algebraic numbers.

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

and all logarithms of algebraic numbers.

M. Kontsevich

$$\frac{\pi^2}{6} = \zeta(2) = \sum_{n\geq 1} \frac{1}{n^2} = \int_{1>t_1>t_2>0} \frac{\mathrm{d}t_1}{t_1} \cdot \frac{\mathrm{d}t_2}{1-t_2}.$$

A product of periods is a period (subalgebra of $\mathbb{C}$), but $1/\pi$ is expected not to be a period.

Relations among periods

1 Additivity

(in the integrand and in the domain of integration)

$$\int_a^b \big(f(x)+g(x)\big)\mathrm{d}x = \int_a^b f(x)\mathrm{d}x + \int_a^b g(x)\mathrm{d}x,$$

$$\int_a^b f(x)\mathrm{d}x = \int_a^c f(x)\mathrm{d}x + \int_c^b f(x)\mathrm{d}x.$$

2 Change of variables:

if $y = f(x)$ is an invertible change of variables, then

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

Relations among periods (continued)

$\boxed{3}$ Newton–Leibniz–Stokes Formula

$$\int_a^b f'(x)\mathrm{d}x = f(b) - f(a).$$

Conjecture of Kontsevich and Zagier

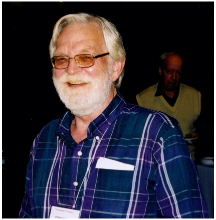
A widely-held belief, based on a judicious combination of experience, analogy, and wishful thinking, is the following

Conjecture (Kontsevich–Zagier). *If a period has two integral representations, then one can pass from one formula to another by using only rules* $\boxed{1}$, $\boxed{2}$, $\boxed{3}$ *in which all functions and domains of integration are algebraic with algebraic coefficients.*

Conjecture of Kontsevich and Zagier (continued)

In other words, we do not expect any miraculous coincidence of two integrals of algebraic functions which will not be possible to prove using three simple rules.
This conjecture, which is similar in spirit to the Hodge conjecture, is one of the central conjectures about algebraic independence and transcendental numbers, and is related to many of the results and ideas of modern arithmetic algebraic geometry and the theory of motives.

Conjectures by S. Schanuel, A. Grothendieck and Y. André



- Schanuel: *if* $x_1, \ldots, x_n$ *are* $\mathbb{Q}$*–linearly independent complex numbers, then at least* n *of the* $2n$ *numbers* $x_1, \ldots, x_n$, $e^{x_1}, \ldots, e^{x_n}$ *are algebraically independent.*

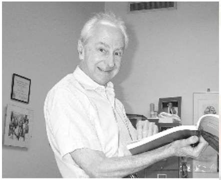
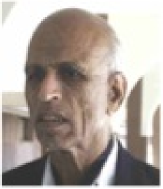
- Periods conjecture by Grothendieck: Dimension of the Mumford–Tate group of a smooth projective variety.

- Y. André: generalization to motives.

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

Ramanujan: Highly composite numbers.

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

Four exponentials conjecture

Let t be a positive real number. Assume 2^t and 3^t are both integers. Prove that t is an integer.

Equivalently:
If n is a positive integer such that

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

is an integer, then n is a power of 2:

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

First decimals of $\sqrt{2}$

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

1.41421356237309504880168872420969807856967187537694807317667973
799073247846210703885038753432764157273501384623091229702492483
605585073721264412149709993583141322266592750559275579995050115
278206057147010955997160597027453459686201472851741864088919860
955232923048430871432145083976260362799525140798968725339654633
180882964062061525835239505474575028775996172983557522033753185
701135437460340849884716038689997069900481503054402779031645424
782306849293691862158057846311159666871301301561856898723723528
850926486124949771542183342042856860601468247207714358548741556
570696776537202264854470158588016207584749226572260020855844665
214583988939443709265918003113882464681570826301005948587040031
864803421948972782906410450726368813137398552561173220402450912
277002269411275736272804957381089675040183698683684507257993647
290607629969413804756548237289971803268024744206292691248590521
810044598421505911202494413417285314781058036033710773091828693
1471017111168391658172688941975871658215212822951848847 . . .

First binary digits of $\sqrt{2}$ http://wims.unice.fr/wims/wims.cgi

1.011010100000100111100110011001111111001110111100110010010000
10001011001011111011000100110110011011101010100101010111110100
11111000111010110111101100000101110101000100100111011101010000
10011001110110100010111101011001000010110000011001100111001100
10001010101001010111111001000001100000100001110101011100010100
01011000011101010001011000111111110011011111101110010000011110
11011001110010000111101110100101010000101111001000011100111000
11110110100101001111000000001001000011100110110001111011111101
00010011101101000110100100010000000101110100001110100001010101
11100011111010011100101001100000101100111000110000000010001101
11100001100110111101111001010101100011011110010010001000101101
00010000100010110001010010001100000101010111100011100100010111
10111110001001110001100111100011011010101101010001010001110001
01110110111111010011101110011001011001010100110001101000011001
10001111100111100100001001101111101010010111100010010000011111
00000110110111001011000001011101110101010100100101000001000100
110010000010000001100101001001010100000010011100101001010 . . .

Computation of decimals of $\sqrt{2}$

$1\,542$ decimals computed by hand by Horace Uhler in 1951

$14\,000$ decimals computed in 1967

$1\,000\,000$ decimals in 1971

$137 \cdot 10^9$ decimals computed by Yasumasa Kanada and Daisuke Takahashi in 1997 with Hitachi SR2201 in 7 hours and 31 minutes.

• Motivation: computation of π.
March 21, 2022: 10^{14} decimals of π computed by Emma Haruka Iwao (Google).

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

Let $g \geq 2$ be an integer and x a real irrational algebraic number. *The expansion in base g of x should satisfy some of the laws which are valid for almost all real numbers (with respect to Lebesgue's measure).*

Conjecture of Émile Borel

Conjecture (É. Borel). *Let* x *be an irrational algebraic real number,* $g \geq 3$ *a positive integer and* a *an integer in the range* $0 \leq a \leq g-1$*. Then the digit* a *occurs at least once in the* g*–ary expansion of* x*.*
Corollary. *Each given sequence of digits should occur infinitely often in the* g*–ary expansion of any real irrational algebraic number.*
(consider powers of g).

- An irrational number with a *regular* expansion in some base g should be transcendental.

The state of the art

There is no explicitly known example of a triple (g, a, x), where $g \geq 3$ is an integer, a a digit in $\{0, \ldots, g-1\}$ and x an algebraic irrational number, for which one can claim that the digit a occurs infinitely often in the g–ary expansion of x.

A stronger conjecture, also due to Borel, is that algebraic irrational real numbers are *normal*: each sequence of n digits in basis g should occur with the frequency $1/g^n$, for all g and all n.

Complexity of the expansion in basis g of a real irrational algebraic number

Theorem (B. Adamczewski, Y. Bugeaud 2005; conjecture of A. Cobham 1968).
If the sequence of digits of a real number x is produced by a finite automaton, then x is either rational or else transcendental.

Open problems (irrationality)

- Is the number

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

  irrational?
- Is the number

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

  irrational?
- Is the number

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

  irrational?

Catalan's constant

Is Catalan's constant

$$\sum_{n\geq 1} \frac{(-1)^n}{(2n+1)^2} = 0.915\,965\,594\,177\,219\,015\,0\ldots$$

an irrational number?

Special values of the Riemann zeta function

Leonhard Euler
(1707 – 1783)

Introductio in analysin infinitorum (1748)

For any even integer value of $s \geq 2$, the number

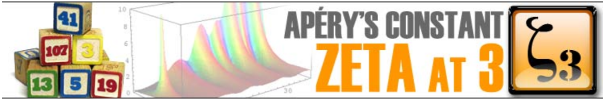
$$\zeta(s) = \sum_{n \geq 1} \frac{1}{n^s}$$

is a rational multiple of π^s.

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

Coefficients: Bernoulli numbers.

Riemann zeta function



The number

$$\zeta(3) = \sum_{n \geq 1} \frac{1}{n^3} = 1,202\,056\,903\,159\,594\,285\,399\,738\,161\,511\ \dots$$

is irrational *(Apéry 1978)*.

Recall that $\zeta(s)/\pi^s$ is rational for any even value of $s \geq 2$.

Open question: Is the number $\zeta(3)/\pi^3$ irrational?

Riemann zeta function

Is the number

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

irrational?

T. Rivoal (2000): infinitely many $\zeta(2n+1)$ are irrational.

F. Brown (2014): Irrationality proofs for zeta values, moduli spaces and dinner parties `arXiv:1412.6508`
Moscow Journal of Combinatorics and Number Theory, **6** 2–3 (2016), 102–165.

Euler–Mascheroni constant

Lorenzo Mascheroni
(1750 – 1800)

Euler's Constant is

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

Is it a rational number?

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

Artin's Conjecture

- Artin's Conjecture (1927): given an integer a which is not a square nor -1, there are infinitely many p such that a is a primitive root modulo p.
(+ Conjectural asymptotic estimate for the density).

(1967), C.Hooley : conditional proof for the conjecture, assuming the Generalized Riemann hypothesis.

(1984), R. Gupta and M. Ram Murty: Artin's conjecture is true for infinitely many a

(1986) R. Heath-Brown : there are at most two exceptional prime numbers a for which Artin's conjecture fails.

For instance one out of 3, 5, and 7 is a primitive root modulo p for infinitely many p.

There is not a single value of a for which the Artin conjecture is known to hold.

Other open problems

- Theory of partitions.

- Lehmer's problem: Let $\theta \neq 0$ be an algebraic integer of degree d, and $M(\theta) = \prod_{i=1}^{d} \max(1, |\theta_i|)$, where $\theta = \theta_1$ and $\theta_2, \cdots, \theta_d$ are the conjugates of θ. Is there a constant $c > 1$ such that $M(\theta) < c$ implies that θ is a root of unity?
$c < 1.176280\ldots$ (Lehmer 1933).

- Markoff conjecture.

- Leopoldt's conjecture.

- The Birch and Swinnerton–Dyer Conjecture

- Langlands program

Collatz equation (Syracuse Problem)

Iterate

$$n \longmapsto \begin{cases} n/2 & \text{if } n \text{ is even,} \\ 3n+1 & \text{if } n \text{ is odd.} \end{cases}$$

Is $(4, 2, 1)$ the only cycle?

update: 2023

Some of the most famous open problems in number theory

Michel Waldschmidt

Sorbonne Université
Institut de Mathématiques de Jussieu – Paris Rive Gauche
http://www.imj-prg.fr/~michel.waldschmidt