October 12, 2012

Delhi University, South Campus
Department of Mathematics

Number theory:
Challenges of the twenty–first century

Michel Waldschmidt

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

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. Are there infinitely many Mersenne (resp. Fermat) prime numbers ? The largest known prime numbers are Mersenne numbers. Mersenne prime numbers are also related with perfect numbers, a problem considered by Euclid and still unsolved. One the main challenges for specialists of number theory is Riemann's hypothesis, which is now more than 150 years old.

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) development of algebraic numbers. Almost nothing is known on this topic.

Hilbert's 8th Problem

August 8, 1900

Second International Congress of Mathematicians in Paris.

David Hilbert (1862 - 1943)

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 $\mathbf{R}$, $\mathbf{C}$.

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

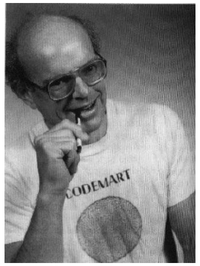
Rational integers : $\mathbf{Z} = \{0, \pm 1, \pm 2, \ldots\}$.

Prime numbers

Numbers with exactly two divisors :

$2,\ 3,\ 5,\ 7,\ 11,\ 13,\ 17,\ 19,\ 23,\ 29,\ 31,\ 37,\ 41,\ 43,\ 47,\ 53, \ldots$

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

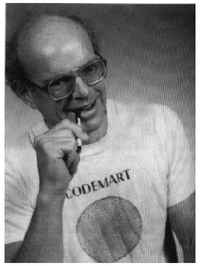


Composite numbers

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 $y > 1$.



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.

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 (October 2012) with $200\,700$ decimal digits :

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

http://oeis.org/A001097
http://primes.utm.edu/

Goldbach's Conjecture

Leonhard Euler
(1707 – 1783)

Letter of Christian Goldbach (1690 – 1764) to Euler, 1742 : *any integer ≥ 5 is sum of at most 3 primes.*

Euler : Equivalent to : *any even integer greater than 2 can be expressed as the sum of two primes.*

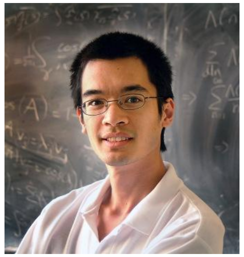
Proof :
$2n-2 = p+p' \Longleftrightarrow 2n = p+p'+2 \Longleftrightarrow 2n+1 = p+p'+3$.

Sums of two primes

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

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.*
- H. A. Helfgott, May 23, 2012, `arXiv:1205.5252v1` *Minor arcs for Goldbach's problem.*



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

Circle method

Hardy and Littlewood

Ivan Matveevich Vinogradov (1891 – 1983)

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

Largest explicitly known prime numbers

August 23, 2008 $12\,978\,189$ decimal digits

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

June 13, 2009 $12\,837\,064$ decimal digits

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

September 6, 2008 $11\,185\,272$ decimal digits

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

Large prime numbers

The nine largest explicitly known prime numbers are of the form $2^p - 1$.

One knows (as of *October 12, 2012*)
- 54 prime numbers with more than $1\,000\,000$ decimal digits
- 262 prime numbers with more than $500\,000$ decimal digits

List of the $5\,000$ largest explicitly known prime numbers :
`http://primes.utm.edu/largest.html`
47 prime numbers of the form of the form $2^p - 1$ are known
`http://www.mersenne.org/`

Marin Mersenne

1588 – 1648

Mersenne prime numbers

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

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

47 of them are known, among them the 9 largest are also the largest explicitly known primes.

The smallest Mersenne primes are

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

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 if perfect if it is equal to the sum of it 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 : all even perfect numbers are of this form.

Sequence of perfect numbers : 6, 28, 496, $8\,128$, $33\,550\,336$, ...
http://oeis.org/A000396

Are there infinitely many even perfect number ?

Does 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

$$4294967297 = 641 \cdot 6700417$$

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

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

Leonhard Euler (1707 – 1783)

For $s > 1$,

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

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

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

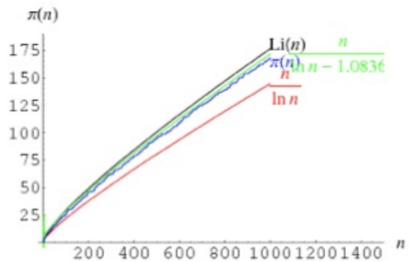
Define the density $d\pi$ by

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

Problem : estimate from above

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

Plot



Lejeune Dirichlet (1805 – 1859)

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

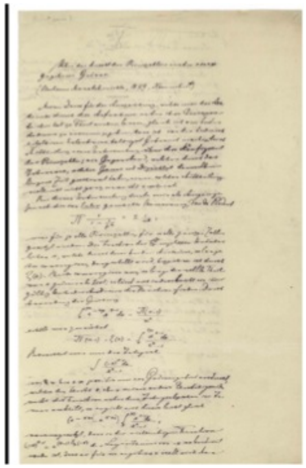
$$\sum_{p \equiv a \pmod q} \frac{1}{p} = +\infty.$$

Pafnuty Lvovich Chebyshev (1821 – 1894)

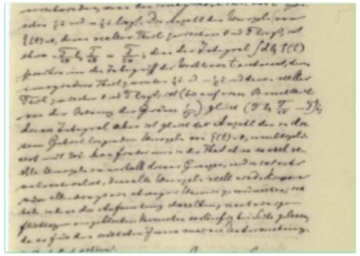
1851 :

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

Riemann 1859



$\zeta(s) = 0$
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)

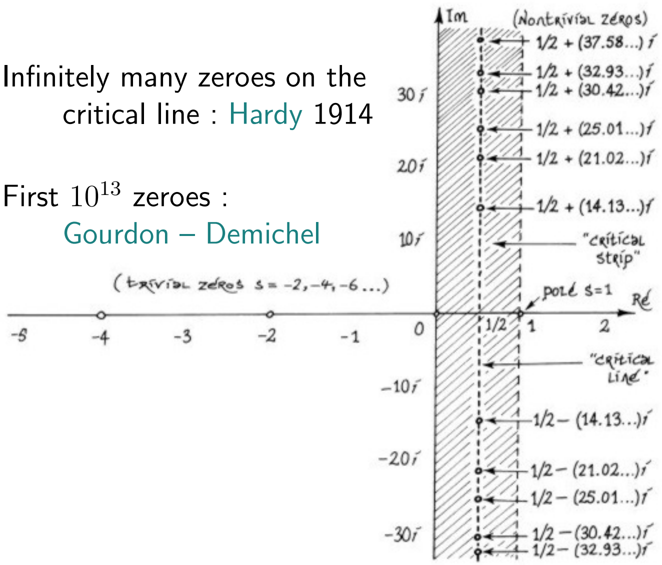
Bernhard Riemann's Gesammelte Mathematische Werke und Wissenschaftlicher Nachlass', herausgegeben under Mitwirkung von Richard Dedekind, von Heinrich Weber. (Leipzig : B. G. Teubner 1892). 145–153.

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

Small Zeros Zeta

Infinitely many zeroes on the critical line : Hardy 1914

First 10^{13} zeroes : Gourdon – Demichel



Riemann Hypothesis

Riemann Hypothesis is equivalent to :

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

for the remainder

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

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

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

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

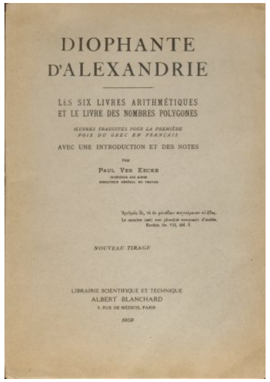
Jacques Hadamard
(1865 – 1963)

Charles de la Vallée Poussin
(1866 – 1962)

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

Diophantine Problems

Diophantus of Alexandria (250 $\pm$50)



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

Pierre de Fermat
1601 – 1665

Andrew Wiles
1953 –

Solution 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 :

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

- Cubes :

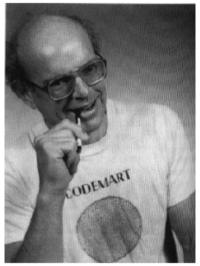
$$1,\ 8,\ 27,\ 64,\ 125,\ 216,\ 343,\ 512,\ 729,\ 1\,000,\ 1\,331, \dots$$

- Fifth powers :

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

Perfect powers

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



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

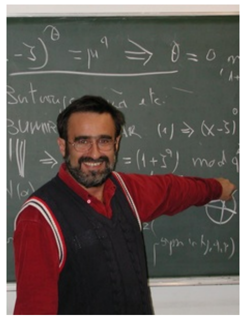
Conjecture :

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

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

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

The abc Conjecture

- For a positive integer n, we denote by

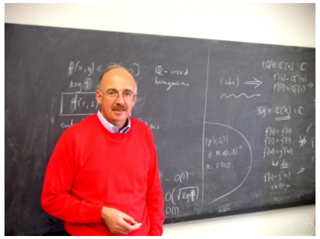
$$R(n) = \prod_{p|n} p$$

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 $\mathbf{Z}_{>0}$ are relatively prime and satisfy $a + b = c$, then*

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

The abc Conjecture of Œsterlé and Masser



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

Papers of 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

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 to $x^p + y^q = z^r$ with $(1/p) + (1/q) + (1/r) < 1$ is finite.*

Consequence of the abc Conjecture. `Hint`:

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

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

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.

Example related to the abc conjecture

$$109 \cdot 3^{10} + 2 = 23^5$$

Continued fraction of $109^{1/5}$: $[2; 1, 1, 4, 77733, \dots]$, approximation : $23/9$

$$109^{1/5} = 2.555\,555\,39\dots$$
$$\frac{23}{9} = 2.555\,555\,55\dots$$

N. A. Carella. *Note on the ABC Conjecture*
http://arXiv.org/abs/math/0606221

Waring's Problem

Edward Waring (1736 - 1798)

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 :

"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."

Waring's function $g(k)$

- Waring's function g is defined as follows : *For any integer $k \ge 2$, $g(k)$ 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 $k \ge 2$,*

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

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

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

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

Waring's Problem and the abc Conjecture

S. David : the estimate

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

(for sufficiently large k) follows not only from Mahler's estimate, but also from the abc Conjecture !

Hence the ideal Waring Theorem $g(k) = 2^k + [(3/2)^k] - 2.$ would follow from an explicit solution of the abc Conjecture.

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 $x_1^k + \cdots + x_s^k$.*

- $G(k)$ 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) $G(4) \geq 16$
$16^m \cdot 31$ need 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,. . .

Baker's explicit *abc* conjecture

Alan Baker

Shanta Laishram

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 $\mathbf{Z}$, $q > 0$ 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 $X^2 + 1$.

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

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 $\mathbf{Q}$.

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

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

Srinivasa Ramanujan

Some transcendental aspects of Ramanujan's work.
Proceedings of the Ramanujan Centennial International Conference
(Annamalainagar, 1987),
RMS Publ., **1**, Ramanujan Math. Soc., Annamalainagar, 1988, 67–76.

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 $\mathbf{R}^n$ given by polynomial inequalities with rational coefficients.

The number π

Basic example of a *period* :

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

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

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

Further examples of periods

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

and all algebraic numbers.

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

and all logarithms of algebraic numbers.

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

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

Relations among periods

1. Additivity
(in the integrand and in the domain of integration)

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

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

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

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

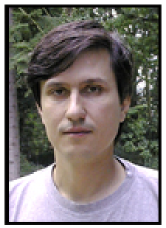
Relations among periods (continued)



3. Newton–Leibniz–Stokes Formula

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

Conjecture of Kontsevich and Zagier



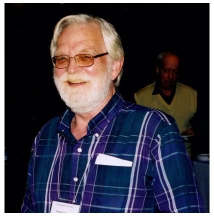
A widely-held belief, based on a
judicious combination
of experience, analogy,
and wishful thinking,
is the following

Conjecture (Kontsevich–Zagier). *If a period has two integral representations, then one can pass from one formula to another by using only rules* 1, 2, 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 coïncidence 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



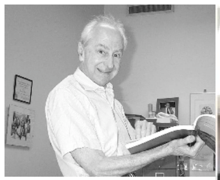
- Schanuel : *if $x_1, \ldots, x_n$ are $\mathbf{Q}$–linearly independent complex numbers, then n at least of the $2n$ numbers $x_1, \ldots, x_n$, $e^{x_1}, \ldots, e^{x_n}$ are algebraically independent.*
- Periods conjecture by Grothendieck : Dimension of the Mumford–Tate group of a smooth projective 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

1.4142135623730950488016887242096980785696718753769480731766797379907324784621070388503875343276415727350138462309122970249248360558507372126441214970999358314132226659275055927557999505011527820605714701095599716059702745345968620147285174186408891986095523292304843087143214508397626036279952514079896872533965463318088296406206152583523950547457502877599617298355752203375318570113543746034084988471603868999706990048150305440277903164542478230684929369186215805784631115966687130130156185689872372352885092648612494977154218334204285686060146824720771435854874155657069677653720226485447015858801620758474922657226002085584466521458398893944370926591800311388246468157082630100594858704003186480342194897278290641045072636881313739855256117322040245091227700226941127573627280495738108967504018369868368450725799364729060762996941380475654823728997180326802474420629269124859052181004459842150591120249441341728531478105803603371077309182869314710171111683916581726889419758716582152128229518488472089694633862891562882765952635140542267653239694617511291602408715510135150455381287560052631468017127402653969470240300517495318862925631385188163478001569369176881852378684052287837629389214300655869568685964595155501644724509836896036887323114389415576651040883914292338113206052433629485317049915771756228549741438999188021762430965206564211827316726257539594717255934637238632261482742622208671155839599926521176252698917540988159348640083457085181472231814204070426509056532333398436457865796796519267292399875366617215982578860263363617827495994219403777753681426217738799194551397231274066898329989895386728822856378697749662519966583525776198939322845344735694794962952168891485492538904755828834526096524096542889394538646625744927492684039 ...

First binary digits of $\sqrt{2}$

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

1.0110101000001001111001100110011111110011101111001100100100001000101100101111101100010011011001101110101010010101011111010011111000111010110111101100000101110101000100100111011101010000100110011101101000101111010110010000101100000110011001110011001000101010100101011111110010000001100000010000111010101110001010001011000011101010001011000111111110011011111101110010000011110110110011100100001111011101001010100001011110010000111001110001111011010010100111100000000100100001110011011000111101111110100010011101101000110100100010000000101110100001110100001010101111000111110100111001010011000000101100111000110000000001000110111100000110011011110111100101010110001101111001001000100010110100010000010001011000101001000110000010101011110001110010001011110111111000100111000110011110001101101010110101000101000111000101110110111111010011101110011001011001010100110001101000011001100011111001111001000010011011111010100101111000100100000111110000011011011100101100000101110111010101010010010100000010001001100100000010000000110010100100101010000000100111001010010 ...

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.

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 (for* 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 b 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 ?

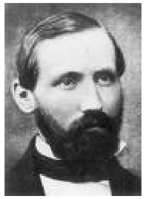
Catalan's constant

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 ?

Riemann zeta function



The function

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

was studied by Euler (1707– 1783)
for integer values of s
and by Riemann (1859) for complex values of s.

Euler : for any even integer value of $s \geq 2$, the number $\zeta(s)$ 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.

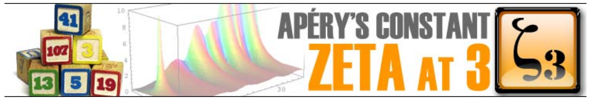
Introductio in analysin infinitorum

Leonhard Euler

(1707 – 1783)

Introductio in analysin infinitorum (1748)

Riemann zeta function



The number

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

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.

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 ?

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

Other open problems

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

- 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 is a constant $c > 1$ such that $M(\theta) < c$ implies that θ is a root of unity ?
$c < 1.176280\ldots$ (Lehmer 1933).

- Schinzel Hypothesis H. For instance : *are there infinitely many primes of the form $x^2 + 1$?*

- 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 ?

The Kerala School of Mathematics (KSoM)

February 4-8, 2013, Calicut = Kozhikode

Workshop on number theory and dynamical systems.

http://www.ksom.res.in/wntds.php

Pietro Corvaja, S.G. Dani, Michel Laurent, Michel Waldschmidt

apply for the workshop at KSOM through online registration on or before **15th December 2012**.

October 12, 2012

Delhi University, South Campus
Department of Mathematics

Number theory:
Challenges of the twenty–first century

Michel Waldschmidt

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