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


Twin primes,

Goldbach’s Conjecture,

David Hilbert (1862 - 1943) 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 : \( \mathbb{Z} = \{0, \pm1, \pm2, \ldots\} \).

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, ...

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 and Primorial 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).

23 prime Euclid numbers are known, the largest known of which is $p_{33237}^\# + 1$ with 169,966 digits.

Primorial primes are prime 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).

20 primorial prime are known, the largest known of which is $p_{55586}^\# - 1$ with 476,311 digits.

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: $2^{47\,156\,667} - 1$ decimal digits 11,185,272
Large prime numbers

Among the 13 largest explicitly known prime numbers, 12 are of the form $2^p - 1$. The 9th is $10\,223 \cdot 2^{81\,172\,165} + 1$ found in 2016.

One knows (as of January 2019)
- 428 prime numbers with more than 1,000,000 decimal digits
- 2296 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

51 prime numbers of the form of the form $2^p - 1$ are known
http://www.mersenne.org/

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.

50 of them are known, among them 11 of the 12 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?

Marin Mersenne

In 1536, Hudalricus Regius noticed that $2^{11} - 1 = 2047$ is not a prime number: 2047 = 23 · 89.

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

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

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

The correct list is

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

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:

- $496 = 16 \cdot 31$ with $16 = 2^4$, $31 = 2^5 - 1$,
- $8128 = 64 \cdot 127$ and $64 = 2^6$, $127 = 2^7 - 1$.

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, 8128, 33550336, ...

http://oeis.org/A000396

Are there infinitely many even perfect numbers?

Do there exist odd perfect numbers?

Fermat numbers

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

Fermat suggested in 1650 that all $F_n$ are prime

$F_0 = 3$, $F_1 = 5$, $F_2 = 17$, $F_3 = 257$, $F_4 = 65537$ are prime

http://oeis.org/A000215

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

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

$4294967297 = 641 \cdot 6700417$

Pierre de Fermat (1601 – 1665)
Fermat primes

\[ F_5 = 2^{32} + 1 \] is divisible by 641

\[ 641 = 5^4 + 2^4 = 5 \cdot 2^7 + 1 \]

\[ 5^4 \equiv -2^4 \pmod{641}, \]
\[ 5 \cdot 2^7 \equiv -1 \pmod{641}, \]
\[ 5^{128} \equiv 1 \pmod{641}, \]
\[ 2^{32} \equiv -1 \pmod{641}. \]

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, 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:

\[ 2^{996,863,034,895} \cdot 2^{1,290,000} + 1 \]

http://primes.utm.edu/

Conjecture (Hardy and Littlewood, 1915)

Twin primes

The number of primes \( p \leq x \) such that \( p + 2 \) is prime is

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

where

\[ C = \prod_{p \geq 3} \frac{p(p - 2)}{(p - 1)^2} \sim 0.66016 \ldots \]

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

No large gaps between primes
Bertrand’s Postulate. There is always a prime between $n$ and $2n$.
Chebychev (1851):

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

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 - 1833)

http://www.numericana.com/answer/record.htm

This caricature is the only known portrait of Adrien-Marie Legendre.

Louis Legendre (ca. 1755–1797)
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
\[ \pi(t + dt) - \pi(t) \sim \frac{dt}{\log t} \]

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

Riemann 1859

Critical strip, critical line

\[ \zeta(s) = 0 \]

with $0 < \Re(s) < 1$ implies
\[ \Re(s) = 1/2. \]
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)


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

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 $t \in \mathbb{R} \setminus \{0\}$. 

Let $\text{Even}(N)$ (resp. $\text{Odd}(N)$) 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

$$|\text{Even}(N) - \text{Odd}(N)| \leq CN^{1/2}.$$
Prime Number Theorem: \( p_n \sim n \log n \)

Elementary proof of the Prime Number Theorem (1949)

Paul Erdős (1913 - 1996)

Atle Selberg (1917 – 2007)

Goldbach’s Conjecture

Letter of Goldbach to Euler, 1742:

any integer \( \geq 6 \) is sum of \( 3 \) primes.

Christian Goldbach (1690 – 1764)

Leonhard Euler (1707 – 1783)

Euler: Equivalent to:

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

Proof:

\[
2n = p + p' + 2 \iff 2n + 1 = p + p' + 3.
\]

Sums of two primes

\[
\begin{align*}
4 &= 2 + 2 & 6 &= 3 + 3 \\
8 &= 5 + 3 & 10 &= 7 + 3 \\
12 &= 7 + 5 & 14 &= 11 + 3 \\
16 &= 13 + 3 & 18 &= 13 + 5 \\
20 &= 17 + 3 & 22 &= 19 + 3 \\
24 &= 19 + 5 & 26 &= 23 + 3 \\
\vdots & \quad \vdots
\end{align*}
\]

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.

27 is neither prime nor a sum of two primes

Weak (or ternary) Goldbach Conjecture: every odd integer \( \geq 7 \) is the sum of three odd primes.

Every odd number greater than 1 is the sum of at most five primes.

Ternary Goldbach Problem

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.

Lejeune Dirichlet (1805 – 1859)
Prime numbers in arithmetic progressions.

\[ a, a + q, a + 2q, a + 3q, \ldots \]

1837:
For \( \gcd(a, q) = 1 \),
\[ \sum_{p \equiv a \pmod{q}} \frac{1}{b} = +\infty. \]

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

*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 – )

Diophantine Problems

Diophantus of Alexandria (250 ±50)

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,

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, ...

- Cubes:
  
  1, 8, 27, 64, 125, 216, 343, 512, 729, 1000, 1331, ...

- Fifth powers:
  
  1, 32, 243, 1024, 3125, 7776, 16807, 32768, ...

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, ...

Consecutive elements in the sequence of perfect powers

- Difference 1 : (8, 9)

- Difference 2 : (25, 27), ...

- Difference 3 : (1, 4), (125, 128), ...

- Difference 4 : (4, 8), (32, 36), (121, 125), ...

- Difference 5 : (4, 9), (27, 32), ...

Two conjectures

- 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 \( \geq 2 \), has only finitely many solutions \((x, y, p, q)\).

Results


Catalan was right: the equation \( x^p - y^q = 1 \) where the unknowns \( x, y, p \) and \( q \) take integer values, all \( \geq 2 \), 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 $\mathbb{Z}_{>0}$ 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

https://hal.archives-ouvertes.fr/hal-01626155
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 \(\geq 3\).
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:

“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 \( k \geq 2 \), \( g(k) \) 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 \( k \geq 2 \),

  \[
g(k) = 2^k + \lfloor (3/2)^k \rfloor - 2.
\]

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

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.

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

<table>
<thead>
<tr>
<th>( k )</th>
<th>( g(k) )</th>
<th>Author/Year</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>4</td>
<td>Lagrange 1770</td>
</tr>
<tr>
<td>3</td>
<td>9</td>
<td>Kempner 1912</td>
</tr>
<tr>
<td>4</td>
<td>19</td>
<td>Balusubramanian, Dress, Deshouillers 1986</td>
</tr>
<tr>
<td>5</td>
<td>37</td>
<td>Chen Jingrun 1964</td>
</tr>
<tr>
<td>6</td>
<td>73</td>
<td>Pillai 1940</td>
</tr>
<tr>
<td>7</td>
<td>143</td>
<td>Dickson 1936</td>
</tr>
</tbody>
</table>
\[ n = x_1^4 + \cdots + x_g^4 : g(4) = 19 \]

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

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

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

\[ \text{Baker's explicit} \ \emph{abc} \ \text{conjecture} \]

\[ \text{Shanta Laishram} \]

\[ \text{Waring's function} \ G(k) \]

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

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

- \( G(k) \) \textit{is known only in two cases:} \( G(2) = 4 \) \textit{and} \( G(4) = 16 \)
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.

$G(2) = 4$

$G(k)$

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 $X^2 + 1$.
- $e^{2i\pi/n}$, 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

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 $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ 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 $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$.

The number $\pi$

*Period* of a function:

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

Basic example:

$$e^{x+2i\pi} = e^x.$$ 

Connection with an integral:

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

The number $\pi$ is a period:

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

Further examples of periods

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

and all algebraic numbers.

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

and all logarithms of algebraic numbers.

M. Kontsevich

$$\frac{\pi^2}{6} = \zeta(2) = \sum_{n\geq 1} \frac{1}{n^2} = \int_{1>t_1>t_2>0} \frac{dt_1}{t_1} \cdot \frac{dt_2}{1-t_2}.$$

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)

\[ \int_a^b (f(x) + g(x)) \, dx = \int_a^b f(x) \, dx + \int_a^b g(x) \, dx, \]

\[ \int_a^b f(x) \, dx = \int_a^c f(x) \, dx + \int_c^b f(x) \, dx. \]

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

\[ \int_{f(a)}^{f(b)} F(y) \, dy = \int_a^b F(f(x)) f'(x) \, dx. \]

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.

Relation among periods (continued)

3 Newton–Leibniz–Stokes Formula

\[ \int_a^b f'(x) \, dx = f(b) - f(a). \]

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.

---

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

$$n \frac{(\log 3)}{\log 2}$$

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

$$2^k \frac{(\log 3)}{\log 2} = 3^k.$$
First binary digits of $\sqrt{2}$: 

```
1.01101010000101111111011110111101110110110010000
1010011010001011111111011110111101110110110010000
01001101001101101100110111101011101110101110100
10010000110100111000101111010011101110101110100
01101000111101011001101110110011001110101101100
1111011101111001100011011110100101101001110100
01110001111110111011101110111011101110111011101
0101100111101111111010110110111101001111011101
1011100111111111111010111101110100111111011111
01001101111001101111111111111111111111111111111
00110001111111111111111111111111111111111111111
11111111111111111111111111111111111111111111111
11111111111111111111111111111111111111111111111
```

Computation of decimals of $\sqrt{2}$:

- 1542 decimals computed by hand by Horace Uhler in 1951
- 14000 decimals computed in 1967
- 1000000 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 $\pi$.

---

**Émile Borel (1871–1956)**

- Jahrbuch Database: [JFM 40.0283.01](http://www.emis.de/MATH/JFM/JFM.html)


**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.

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 $\log \pi = 1.144 729 885 849 400 174 143 273 513 53 \ldots$ irrational?

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 $n$. 
Catalan’s constant

Is Catalan’s constant
\[
\sum_{n \geq 1} \frac{(-1)^n}{(2n + 1)^2} = 0.9159655941772190150 \ldots
\]
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 \( \pi^s \).

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

Coefficients : Bernoulli numbers.

Riemann zeta function

The number
\[
\zeta(3) = \sum_{n \geq 1} \frac{1}{n^3} = 1, 202056903159594285399738161511 \ldots
\]
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
\[
\zeta(5) = \sum_{n \geq 1} \frac{1}{n^5} = 1.036927755143369926331365486457 \ldots
\]
n 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
Euler–Mascheroni constant

Euler’s Constant is

\[ \gamma = \lim_{n \to \infty} \left( \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n} - \log n \right) \]

\[ = 0.5772156649015328606065120907282888617934885...

Is it a rational number?

\[ \gamma = \sum_{k=1}^{\infty} \left( \frac{1}{k} - \log \left( 1 + \frac{1}{k} \right) \right) = \int_{1}^{\infty} \left( \frac{1}{x} - \frac{1}{x} \right) dx \]

\[ = -\int_{0}^{1} \int_{0}^{1} \frac{(1-x)dx}{{(1-xy)\log(xy)}} \]

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 \( \theta = \theta_1, \theta_2, \cdots, \theta_d \) are the conjugates of \( \theta \). Is there a constant \( c > 1 \) such that \( M(\theta) < c \) implies that \( \theta \) 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

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

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