Fermat's Last Theorem

Diophantine equation

$$x^n + y^n = z^n$$

does not have a solution in positive integers for integer $n > 2$.

- Conjectured by Pierre de Fermat in 1637 in the margin of a copy of Arithmetica where he claimed he had a proof that was too large to fit in the margin.
- $n = 4$ Fermat + several equivalent proofs
- $n = 3$ Leonhard Euler (1770)
- $n = 5$ Legendre / Dirichlet (1825)
- $n = 7$ Lamé (1839)
- $n = 6, 10, 14$
  ⋮
- any n Andrew Wiles (1994)
  – Elliptic curves $y^2 = x^3 + ax + b$
  – Modular forms $\mathbb{C}^2 \to \mathbb{C}^2$ with "much symmetry"

$n = 2$ (Euclid's formula):
$x = m^2 - n^2$
$y = 2mn$
$z = m^2 + n^2$

Fermat's Little Theorem

For p = prime: gcd = greatest common divisor

$$a^p \equiv a \pmod p \qquad a^{p-1} \equiv 1 \pmod p, a \text{ not multiple of } p$$

Proof: Consider p-tuples of a objects; there are a^p of them. We remove 111..1, 222..2,...; there are $a^p - a$ left. These can be grouped to p-cyclically shifted groups; e.g., 21111, 12111, 11211, 11121, 11112.
Also: $\{a, a^2, a^3, \ldots, a^{p-1}\} = \{1, 2, 3, \ldots, p-1\} \pmod p$ (i.e., except order)

Extension: for a, n co-primes

$$a^{\phi(n)} \equiv 1 \pmod n$$

numbers a, b so that $\gcd(a, b) = 1$ are called co-primes

where $\phi(n)$ = Euler's totient function = number of co-primes to n in interval $[1, n-1]$.
NB: $\phi(p) = p - 1$.

Example: calculate $3^7 \pmod 7$ by the square-and-multiply algorithm

(mod 7): $3^2 \equiv 2,\ 3^4 \equiv 4,\ 3^9 \equiv 1,\ 3^7 \equiv 3$

Inversion: If $a^{n-1} \not\equiv 1$ for a co-prime a, then n is composite

Probabilistic test: If $a^{n-1} \equiv 1$ for several co-primes a, then n is a prime with a high probability

Modular inversion (division in general)

Let a, b are co-primes and $a < b$. We want to solve

$$ax \equiv 1 \pmod b \quad \text{or} \quad ax + by = 1$$

Extended Euclidean algorithm:

	a	b
$r_0 := b$	$s_0 = 0$	$t_0 = 1$
$r_1 := a$	$s_1 = 1$	$t_1 = 0$
$r_2 := r_0 - q_1 r_1$	$s_2 := s_0 - q_1 s_1$	$t_2 := t_0 - q_1 t_1$
$r_3 := r_1 - q_2 r_2$	$s_3 := s_1 - q_2 s_2$	$t_3 := t_1 - q_2 t_2$
	⋮	
1	x	y

where q_i = reminder after $r_{i-1} : r_i$ (: = integer division)

Proof: based on $r_i = as_i + bt_i$ for every line, proof by induction.

Example: solve $6x \equiv 1 \pmod{17}$

ε

RSA cryptosystem

Rivest–Shamir–Adleman (1978) lcm = least common multiple

- Choose 2 distinct primes p, q (not too close)
- Calculate $n = pq$ (the modulo, part of the public key)
- Calculate $\lambda = (p-1)(q-1)$ (better: $\text{lcm}(p-1, q-1)$)
- Public key: e, $1 < e < \lambda$, co-prime to λ (often $e = 65537$)
- Private key: d so that $de \equiv 1 \pmod \lambda$ (easy if you know pq)

Encrypt m: $c \equiv m^e \pmod n$
Decrypt c: $c^d \equiv m \pmod n$

? Can integer factorization be solved in polynomial time on a classical computer?

Proof. Since $de - 1$ is a multiple of λ, $\exists g, h, k$ so that

$$ed - 1 = g\lambda = h(p-1) = k(q-1)$$

Using Fermat's little theorem (except $m \equiv 0 \pmod p$, which is trivial)

$$m^{ed} = m^{ed-1}m = (m^{p-1})^h m \equiv 1^h m \equiv m \pmod p$$

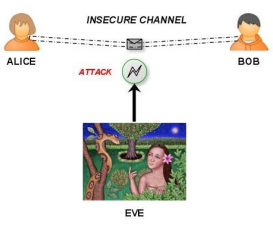
And similarly for q: $m^{ed} \equiv m \pmod q$. Since p, q are co-primes,

$$(m^e)^d \equiv m \pmod{pq}$$ q.e.d.

How it works

Message sent via insecure channel (https, ssh)

- Alice calculates n, e and sends it openly to Bob.
- Bob encrypts a message using n, e and sends it to Alice.
- Alice decrypts the mesage using her private n, d.



Digital signature

- Alice publishes n, e.
- Alice encrypts a file (better: a hash) using n, d.
- Bob can verify the encrypted hash using n, e.

SSH login without password

- Generate a private/public key pair on your HOME computer:
  ssh-keygen -t rsa
  your PRIVATE key is .ssh/id_rsa
  your PUBLIC key is .ssh/id_rsa.pub
- copy your PUBLIC key to .ssh/authorized_keys on the REMOTE machine

The Enormous Theorem

Every finite simple group is isomorphic to one of the following groups:

1. A cyclic group with prime order;
2. An alternating group (group of even permutations) of degree at least 5;
3. A simple group of Lie type (over a finite field) (quite rich...)†
4. The 26 sporadic simple groups.

The biggest sporadic group = "Monster", number of elements

$$= 2^{46} \cdot 3^{20} \cdot 5^9 \cdot 7^6 \cdot 11^2 \cdot 13^3 \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \cdot 41 \cdot 47 \cdot 59 \cdot 71$$
$$= 808017424794512875886459904961710757005754368000000000$$

Proof finished 2004 – hundreds of papers...

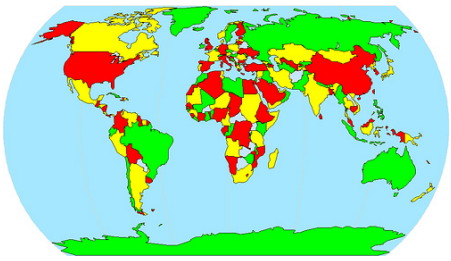
Group is a set G with "multiplication" and "division":

- $\forall a, b \in G$: $ab \in G$ (closure)
- $\forall a, b, c \in G$: $(ab)c = a(bc)$ (associativity)
- $\exists e \in G : \forall a \in G$ it holds $ea = ae = a$ (identity element)
- $\forall a \in G\ \exists a^{-1} : aa^{-1} = a^{-1}a = e$ (inverse element)

† Incl. both the classical Lie groups, namely the simple groups related to the projective special linear, unitary, symplectic, or orthogonal transformations over a finite field; the exceptional and twisted groups of Lie type (incl. the Tits group, sometimes classified as sporadic).

Four color theorem

Every map (on sphere or plane) can be colored by 4 colors



credit: http://www.artsrn.ualberta.ca/mengel/2015huco617/files/2015/04/Map.jpg

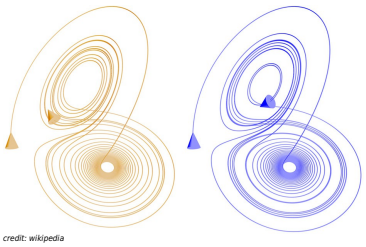
Computer-assisted proof in 1976 by Kenneth Appel and Wolfgang Haken, based on 1,936 submaps.

Easier for torus etc.

Deterministic chaos

Weather, oil on pan ...
Lorentz attractor:

$$\begin{aligned} \dot{x} &= \sigma y - \sigma x, \\ \dot{y} &= \rho x - xz - y, \\ \dot{z} &= xy - \beta z \end{aligned}$$

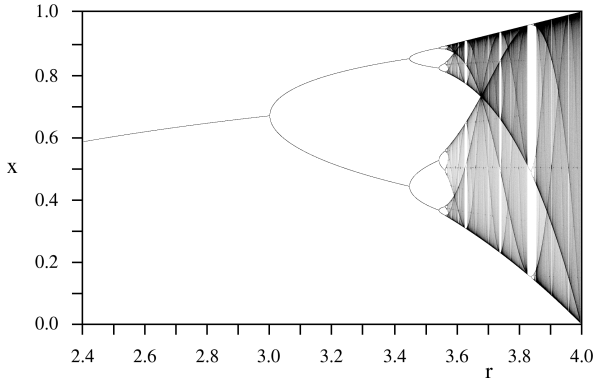


credit: wikipedia

Simpler model: $x := a - x^2$ (see mmpc7.mw)

- universal properties; Feigenbaum:
  4.669201609102990671853203821578...
  2.502907875095892822283902873218...
- self-similarity (fractal)

Bifurcation map $x := rx(1-x)$



Fractals

Problem: what is the length of the borderline?
Answer: it depends on the meter m:

$$l = \text{const}\, m^{1-D}$$

$D = 1.02$ South Africa
$D = 1.25$ west GB

Fractal: geometric set, which resembles a part of itself (after a continuous transformation, usually shrinking)
Random fractal: self-similarity in a statistical-sense

(Almost) definition of the **fractal dimension**:

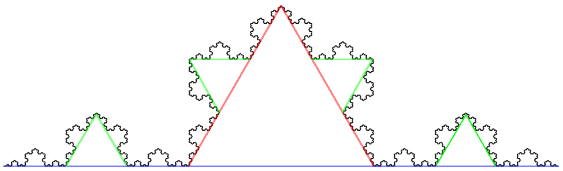
$$D = \lim_{m \to 0} \frac{\log N_m}{\log(1/m)}$$

where N_m = # of line segments/squares/cubes ... of length/edge... m needed to cover the set ($1/m$ = # of line segments of length m to cover a unit line segment, $D = 1$)

Fractal dimension

cd show;mz Kochsim.gif 11/24 mmpc7

Example. Calculate the fractal dimension of a line segment.
Answer: $N_m = l/m$, $D = \lim \log(l/m)/\log(1/m) = 1$



Example. Calculate the fractal dimension of the Koch curve

$\ln 4/\ln 3 \doteq 1.26$

Example. Calculate the fractal dimension of the trajectory of the Brownian motion (polymer in a θ-solvent)

1 step of random walk by 1 ($\overset{1/2}{\leftarrow}$, $\overset{1/2}{\rightarrow}$): $\langle R^2\rangle = 1$, $m = 1$, $l = 1$, $N_m = 1$
2 steps of random walk: $\langle R^2\rangle = 1$, $m = 1/\sqrt{2}$, $l = \sqrt{2}$, $N_m = l/m = 2$

$D = 2$ (does not depend on the space dimension)

Poincaré hypothesis

cd show;mz MugTorus.gif 12/24 mmpc7

Every simply-connected, closed 3-manifold is homeomorphic to the 3-sphere.

- 3-sphere = $\{\vec{r}, |\vec{r}| = 1\}$ in $\mathbb{R}^4$
- simply-connected = path-connected + any circle can be be contracted to a point
- path-connected = ∃ a continuouos path between points
- closed = compact + without boundary
- compact = any open cover has a finite subcover;
  any infinite sequence has a converging subsequence
- 3-manifold = locally as 3D Euclidean
- homeomorphism = continuous function between topological spaces that has a continuous inverse function

Proven by Grigori Perelman 2002, 2003
He rejected the Millennium Prize ($1M) and the Fields medal

Cf. Poincaré homology sphere (glued dodekahedron, binary icosahedral group, $n = 120$)

The Rectangular Peg Problem

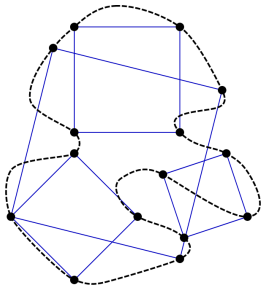
mz movies/RectangularPegProblem.gif 13/24 mmpc7

aka Inscribed Square Problem, Toeplitz' conjecture

Does any (smooth) Jordan curve admit an inscribed square?

A Jordan curve is a plane curve which is topologically equivalent to (a homeomorphic image of) the unit circle, i.e., it is simple and closed.

Solved by Joshua Evan Greene and Andrew Lobb (2020) for smooth curves (even for every rectangle ∃ a similar rectangle on the the curve)



credits: Wikipedia, https://www.quantamagazine.org/new-geometric-perspective-cracks-old-problem-about-rectangles-20200625/

Gödel

14/24 mmpc7

Liar paradox: This sentence is false.

Paradox of 1000 words: Let us consider sentences in English, based on a well-defined syntax and vocabulary, that define a number. There are a finite number of words in English; therefore, there are a finite number of sentences shorter than 1000 words that define a number. Hence, there exists a highest such number. Now, consider the sentence: "The number equals one plus the highest number that can be defined by a sentence in English composed of less than 1000 words."

Language vs. metalanguage

First Incompleteness Theorem: Any consistent formal system F within which a certain amount of elementary arithmetic can be carried out is incomplete; i.e., there are statements of the language of F which can neither be proved nor disproved in F.

First Incompleteness Theorem: For each formal system F containing basic arithmetic, it is possible to canonically define a formula Cons(F) expressing the consistency of F. This formula expresses the property that "there does not exist a natural number coding a formal derivation within the system F whose conclusion is a syntactic contradiction;" loosely: "there is no natural number that codes a derivation of 0=1 from the axioms of F."

Gödel's second incompleteness theorem shows that, under general assumptions, this canonical consistency statement Cons(F) will not be provable in F.

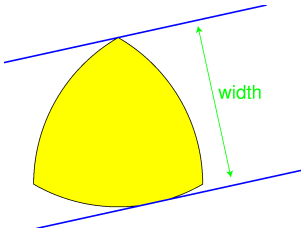
TO ADD: Axiom of choice

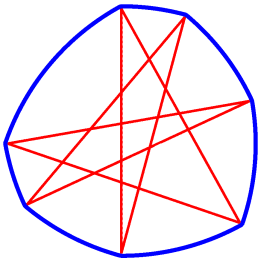
15/24 mmpc7

Curves/shapes of constant width

cd show; firefox ReuleauxTriangleAnimation.gif 16/24 mmpc7

A **curve of constant width** is a simple closed curve in the plane whose width (the distance between parallel supporting lines) is the same in all directions. Such curve is convex.

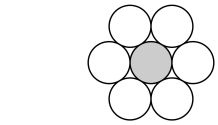


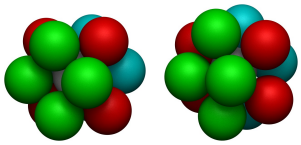


? Kissing numbers

cd ../simul/kissing; kiss.sh 17/24 mmpc7

The greatest number of non-overlapping unit spheres (in D-dimensional space) touching a central unit sphere.





D	Lower bound	Upper bound	proven
1	2		easy
2	6		easy
3	12		1953
4	24		2003
5	40	44	
6	72	78	
7	126	134	
8	$240 = 2^4 \cdot 3 \cdot 5$		1979
9	306	364	
10	500	554	
11	582	870	
12	840	1,357	
13	1,154	2,069	
14	1,606	3,183	
15	2,564	4,866	
16	4,320	7,355	
17	5,346	11,072	
18	7,398	16,572	
19	10,668	24,812	
20	17,400	36,764	
21	27,720	54,584	
22	49,896	82,340	
23	93,150	124,416	
24	$196{,}560 = 2^4 \cdot 3^3 \cdot 5 \cdot 7 \cdot 13$		1979

? Twin primes

18/24 mmpc7

are prime numbers p_1, p_2 so that $p_2 - p_1 = 2$.

Are there infinitely many twin primes?

Probably yes, but not proven...

Brun's theorem: the sum of reciprocal twin primes converges:

$$\sum_{p,p+2 \text{ are primes}} \left(\frac{1}{p} + \frac{1}{p+2}\right) = \left(\frac{1}{3}+\frac{1}{5}\right) + \left(\frac{1}{5}+\frac{1}{7}\right) + \left(\frac{1}{11}+\frac{1}{13}\right) + \cdots \approx 1.902160583104$$

Euler 1737: the sum of reciprocal primes diverges

Yitang Zhang 2015: $\liminf_{n\to\infty}(p_{n-1} - p_n) < 246$

? Goldbach's conjecture

Every even integer greater than 2 can be expressed as a sum of two primes.

The conjecture has been shown to hold for all integers less than 4×10^{18}

? Odd perfect number

19/24 mmpc7

Perfect number = positive integer that is equal to the sum of its positive divisors, excluding the number itself.

Euclid proved that $2^{p-1}(2^p - 1)$ is an even perfect number whenever $2^p - 1$ is prime (Mersenne prime).

$$6 = 110_2 \quad 28 = 11100_2 \quad 496 = 111110000_2$$

It is unknown whether there is any odd perfect number N. If yes:

- $N > 10^{1500}$
- The largest prime factor of N is greater than 10^8
- N has at least 101 prime factors and at least 10 distinct prime factors.

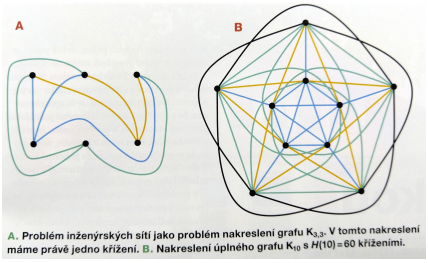
Catalan's conjecture → Mihăilescu's theorem

The only solution in natural numbers of $x^a - y^b = 1$ for $a, b > 1$, $x, y > 0$ is $3^2 - 2^3 = 1$.

Proven 2002 by Preda V. Mihăilescu

? Zarankiewicz and Hill conjectures

20/24 mmpc7



A. Problém inženýrských sítí jako problém nakreslení grafu $K_{3,3}$. V tomto nakreslení máme právě jedno křížení. B. Nakreslení úplného grafu K_{10} s $H(10) = 60$ kříženími.

To fully connect, algorithms exist for the number of crossing lines C:

$$C(K_{n,m}) = \lfloor \tfrac{n}{2} \rfloor \lfloor \tfrac{n-1}{2} \rfloor \lfloor \tfrac{m}{2} \rfloor \lfloor \tfrac{m-1}{2} \rfloor \quad C(K_n) = \tfrac{1}{4} \lfloor \tfrac{n}{2} \rfloor \lfloor \tfrac{n-1}{2} \rfloor \lfloor \tfrac{n-2}{2} \rfloor \lfloor \tfrac{n-3}{2} \rfloor$$

Are there better solutions?

[M. Balko, *Vesmír* **11**, 628 (2019)]

? Collatz conjecture aka $3n+1$ problem

$$f(n) := \begin{cases} n/2 & \text{for even } n \\ 3n+1 & \text{for odd n} \end{cases}$$

Conjecture: For any integer n, there exists a finite M

$$\text{so that } \overbrace{f(f(\ldots(n))}^{M\times} = 1$$

- proven for $n < 2^{68}$
- probabilistic arguments suggest it is true
- $27 \to 9232$
  $6631675 \to 60342610919632$
- The cycle length (except $1 \to 2 \to 1 \ldots$) of

$$f(n) := \begin{cases} n/2 & \text{for even } n \\ (3n+1)/2 & \text{for odd n} \end{cases}$$

  is at least 17087915 (Eliahou 1993). Based on continuum fraction expansion for $\ln 3/\ln 2 \to \to \to$

27 82 41 124 62 31 94 47 142 71 214 107 322 161
484 242 121 364 182 91 274 137 412 206 103 310
155 466 233 700 350 175 526 263 790 395 1186 593
1780 890 445 1336 668 334 167 502 251 754 377
1132 566 283 850 425 1276 638 319 958 479 1438
719 2158 1079 3238 1619 4858 2429 7288 3644
1822 911 2734 1367 4102 2051 6154 3077 9232
4616 2308 1154 577 1732 866 433 1300 650 325
976 488 244 122 61 184 92 46 23 70 35 106 53 160
80 40 20 10 5 16 8 4 2 1 4 2 1 4 2 1

1	1/1	-0.585
1	2/1	0.415
1	3/2	-0.08496
2	8/5	0.01504
2	19/12	-0.001629
3	65/41	0.0004034
1	84/53	-5.684e-05
5	485/306	4.82e-06
2	1054/665	-9.471e-08
23	24727/15601	1.683e-09
2	50508/31867	-3.289e-10
2	125743/79335	6.664e-11
1	176251/111202	-4.671e-11
1	301994/190537	4.883e-13
55	16785921/10590737	-7.243e-15
1	17087915/10781274	1.515e-15

? Riemann hypothesis

Riemann zeta function:

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = \frac{1}{1^s} + \frac{1}{2^s} + \frac{1}{3^s} + \cdots.$$

for $s \in \mathbb{C}$ and $\Re(s) > 1$, and its analytic continuation

Euler:

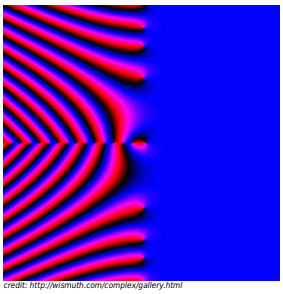
$$\zeta(s) = \prod_{p \text{ is prime}} \frac{1}{1-p^{-s}}$$

Single pole at $s = 1$ (res = 1)

Hypothesis (1859): roots = negative even integers (trivial) and complex numbers with real part 1/2.

Proven (2004) for the first 10^{13} roots, but not in general

Consequences to the distribution of primes



credit: http://wismuth.com/complex/gallery.html

? Complexity theory: $P = NP$

P = problem can be solved (on a computer) in a polynomial time (as a function of problem size)[*]
e.g.: sorting, square root

Subset sum problem: Having data set (numbers may repeat) of N integers and target sum T, find a data subset summing up to T

NP[†] = a known solution can be verified in a polynomial time
e.g., subset sum problem, sudoku

NP-complete = problems to which any other NP-problem can be reduced in polynomial time, and whose solution may still be verified in polynomial time
e.g., decide whether a solution of traveling salesman is indeed the shortest

NP-hard = at least as hard as the hardest NP
H is NP-hard if every NP problem can be reduced in polynomial time to *H*
e.g., traveling salesman, quantum theory, . . .

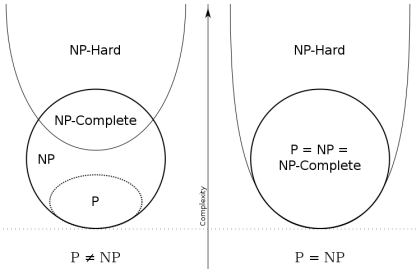
Connes embedding conjecture (about aproximating operators ≈ infinite matrices ≈ quantum world by a hirearachy of finite matrices) has been falsified

- likely but not proven: P ≠ NP
  ⇒ NP-hard problems cannot be solved in polynomial time

[*] for number problems: size = # of digits
[†] Nondeterministic Polynomial

? Probably $P \neq NP$

.. but not proven! And thus many problems are hard.



credit: "P np np-complete np-hard" by Behnam Esfahbod. Licensed under CC BY-SA 3.0 via Commons – https://commons.wikimedia.org/wiki/File:P,np,np-complete,np-hard.svg#/media/File:P,np,np-co