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
- $n = 3$ Leonhard Euler (1770)
- $n = 5$ Legendre / Dirichlet (1825)
- $n = 7$ Lamé (1839)

⋮

- general Andrew Wiles (1994)
  – Elliptic curves $y^2 = x^3 + ax + b$
  – Modular forms $\mathbb{C}^2 \to \mathbb{C}^2$ with "much symmetry"

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.

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

Extension: for a, n co-primes

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

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): $3^2 \equiv 2$, $3^4 \equiv 4$, $3^6 \equiv 1$, $3^7 \equiv 3$

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

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

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

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 $r_i = a s_i + b t_i$ for every line, proof by induction.

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

3

RSA cryptosystem

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

- Choose 2 distinct primes p, q (not too close)
- Calculate $n = pq$ (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 $de \equiv 1 \pmod{\lambda}$

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

Encrypt m: $c \equiv m^e \pmod{n}$

Decrypt c: $c^d \equiv m \pmod{n}$

Proof. $\exists g, h, k$ 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. 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 permut.) 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

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

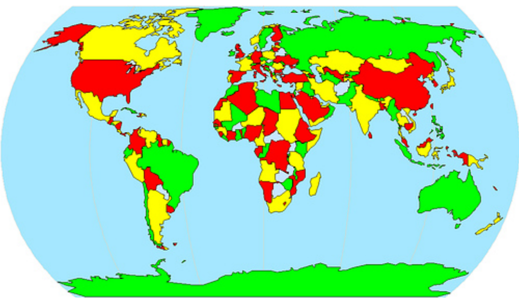
Proof finished 2004 – thousands of papers...

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)

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

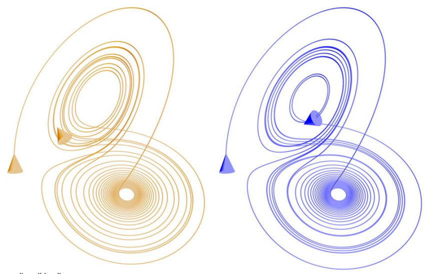
Computer-assisted proof in 1976 by Kenneth Appel and Wolfgang Haken, based on 1,936 sub-maps.

Easier for torus etc.

Deterministic chaos

Weather, oil on pan ...
Lorentz attractor:

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

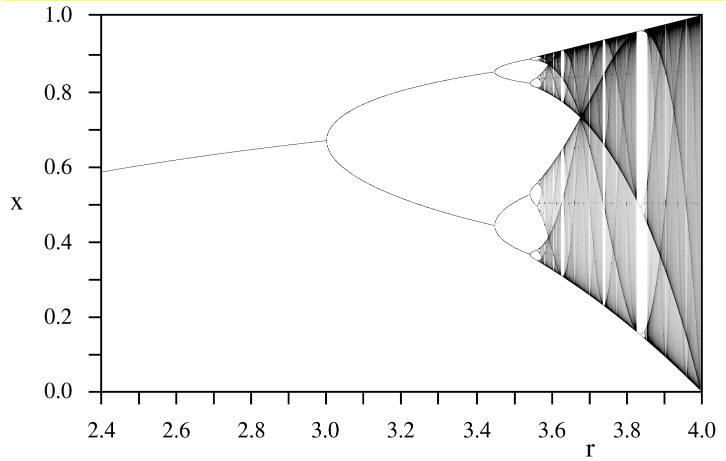


credit: wikipedia

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

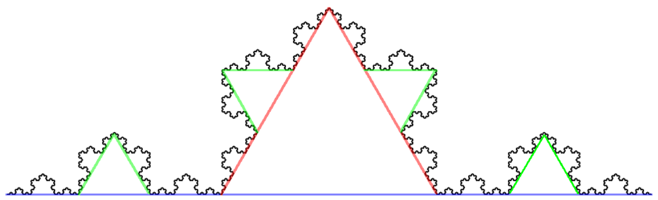
(Almost) definition of the **fractal dimension**:

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

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

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

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 Millennium Prize ($1M) and Fields medal

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

? Twin primes

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: 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

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

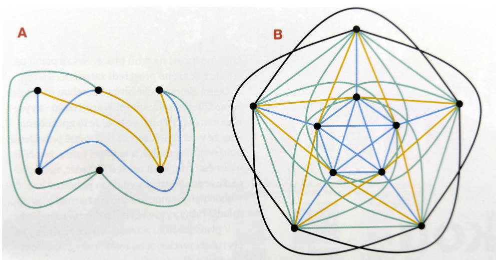
Euclid proved that $2^p1(2^p1)$ is an even perfect number whenever 2^p1 is prime (Mersenne prime).

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

It is unknown whether there is any odd perfect number N. I 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.

? Zarankiewicz and Hill conjectures



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)]

? Riemann hypothesis

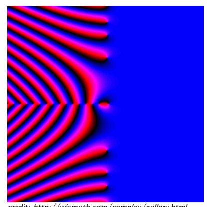
Riemann zeta function:

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

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

Euler:

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


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

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

? 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

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

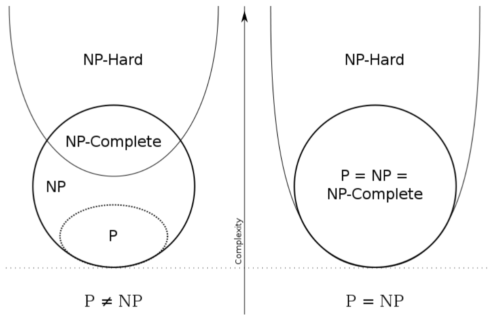
NP-hard = at least as hard as the hardest NP
H is NP-hard if every NP problem can be reduced in polynomial time to *H*
e.g., traveling salesman, quantum theory, . . .

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

*for numbers problem 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-complete_np-hard.svg