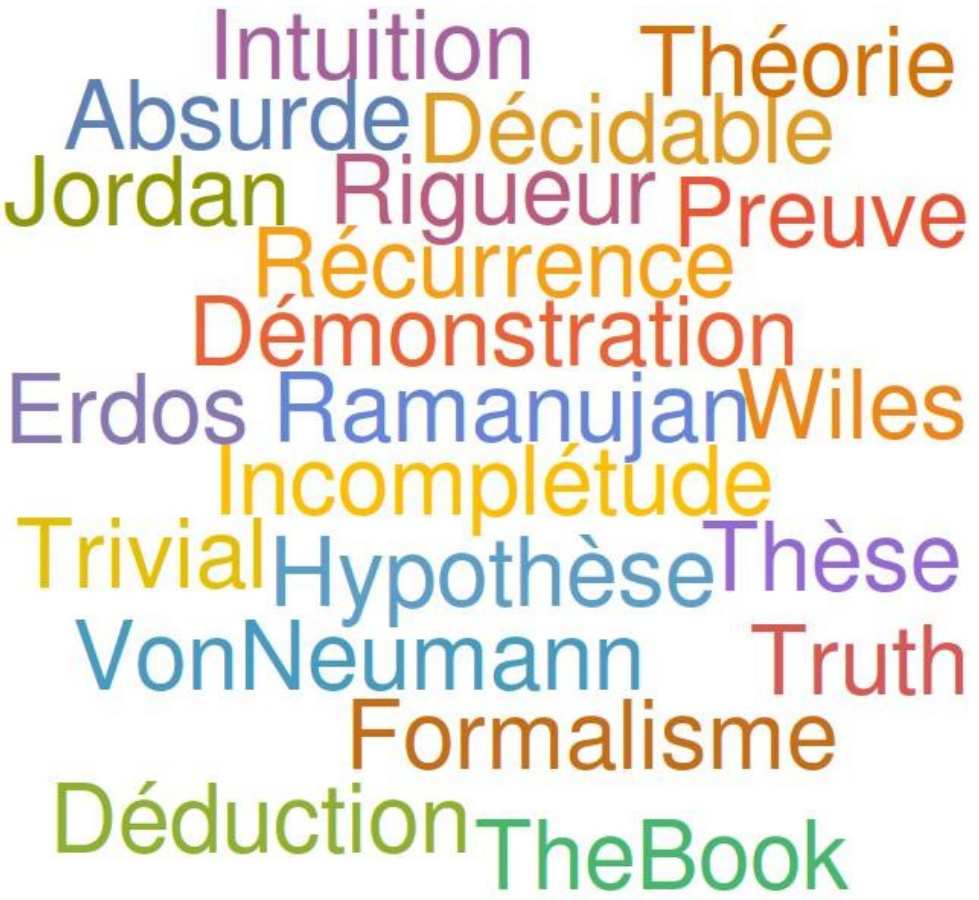
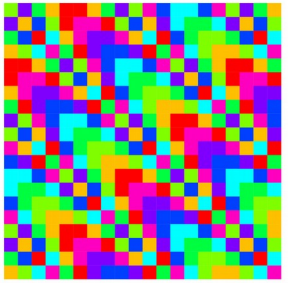
Des preuves ?

Où, quand, comment ?



Michel RIGO
Département de Mathématique
http://www.math.ulg.ac.be/

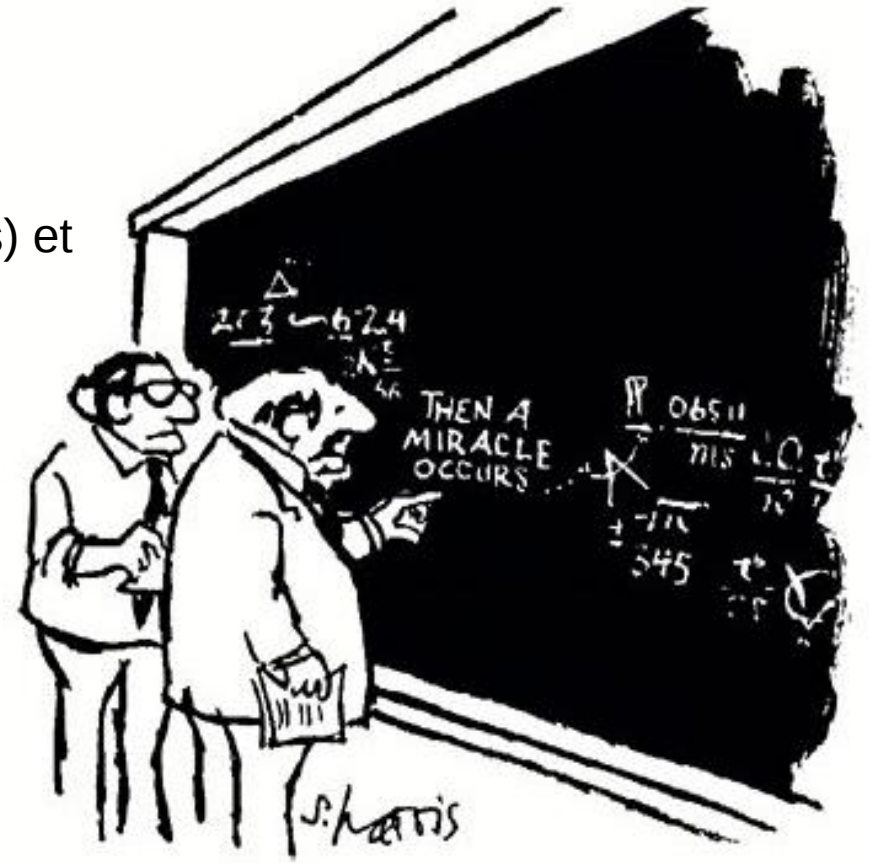


Preuve (Larousse) : Opération par laquelle on contrôle l'exactitude d'un calcul ou la justesse de la solution d'un problème.

Démonstration (Wikipédia) : En mathématiques, une démonstration est une rédaction argumentée qui établit la véracité d'un énoncé mathématique.

Une démonstration s'appuie sur

- des hypothèses,
- des énoncés précédemment démontrés,
- des énoncés supposés évidents (appelés axiomes) et
- des règles de déduction



"I THINK YOU SHOULD BE MORE EXPLICIT HERE IN STEP TWO."

Le point culminant !

Mathematicians are not normally content to guess, or assume, or assert that something is true; they must prove it, or feel they have, or as Hardy put it, "*exhibit the conclusion as the climax of a conventional pattern of propositions, a sequence of propositions whose truth is admitted and which are arranged in accordance with rules*".

The man who knew infinity, R. Kanigel

La notion de preuve *dépend* de l'époque, de l'environnement, de l'éducation reçue,...

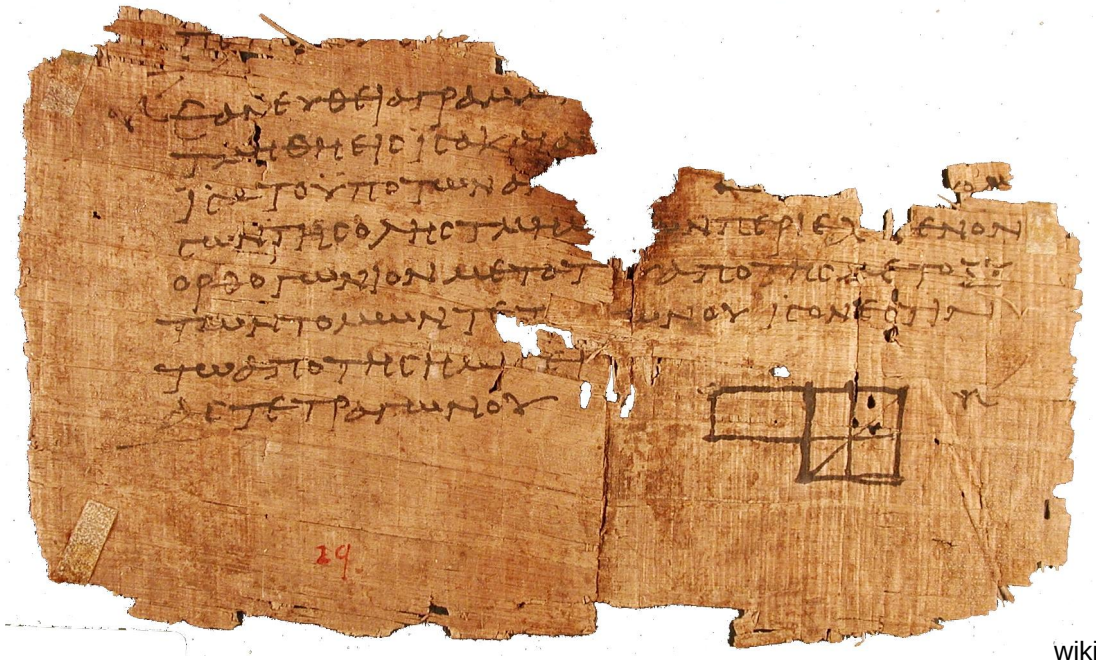
- le *formalisme* et les *notations* évoluent
- on donnait une preuve sur un *exemple* ou par une *construction particulière*
- la notion "moderne" d'*infini* a mis du temps à apparaître
- utilise les standards/la rigueur de l'*époque*

La multiplication chez les égyptiens et les mésopotamiens :
ils disposaient d'une forme implicite de raisonnement

wikipedia.org

Le papyrus de Rhind (British Museum, +/- 1500 Av J.C.)

Les *éléments d'Euclide* (+/- 300 Av. J.C.)



wikipedia.org

On se place dans un système axiomatique

HIERONYMI CAR

DANI, PRÆSTANTISSIMI MATHE-

MATICI, PHILOSOPHI, AC MEDICI,

ARTIS MAGNÆ,

SIVE DE REGVLIS ALGEBRAICIS,

Lib. unus. Qui & totius operis de Arithmetica, quod

OPVS PERFECTVM

inscripsit, est in ordine Decimus.

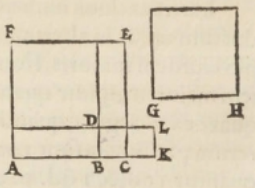
HAbes in hoc libro, studiose Lector, Regulas Algebraicas (Itali, de la Cosa uocant) nouis adinuentionibus, ac demonstrationibus ab Authore ita locupletatas, ut pro pauculis antea uulgò tritis, iam septuaginta euaserint. Neq; solum, ubi unus numerus alteri, aut duo uni, uerum etiam, ubi duo duobus, aut tres uni æquales fuerint, nodum explicant. Hunc aũt librum ideo seorsim edere placuit, ut hoc abstrusissimo, & planè inexhausto totius Arithmeticæ thesauro in lucem eruto, & quasi in theatro quodam omnibus ad spectandum expositò, Lectores incitarẽtur, ut reliquos Operis Perfecti libros, qui per Tomos edentur, tanto auidius amplectantur, ac minore fastidio perdiscant.

relinquitur prima 6 m: R̃ 30 6/7, hæ autem quantitates proportionales sunt, & quadratum secundæ est æquale duplo producti secundæ in primam, cum quadruplo primæ, ut proponebatur.

De cubo & rebus æqualibus numero. Cap. XI.

SCipio Ferreus Bononiensis iam annis ab hinc trigínta fermè capitulum hoc inuenit, tradidit uero Anthonio Mariæ Florido Veneto, qui cũ in certamen cũ Nicolao Tartalea Brixellense aliquando uenisset, occasionem dedit, ut Nicolaus inuenerit & ipse, qui cum nobis rogantibus tradidisset, suppressa demonstratione, freti hoc auxilio, demonstrationem quæsiuimus, eamq; in modos, quod difficillimum fuit, redactam sic subiecimus. DEMONSTRATIO.

Sit igitur exempli causa cubus G H & sexcuplum lateris G H æquale 20, & ponam duos cubos A E & C L, quorum differentia sit 20, ita quod productum A C lateris, in C K latus, sit 2, tertia scilicet numeri rerum pars, & abscindam C B, æqualem C K, dico, quod si ita fuerit, lineam A B residuum, esse æqualem G H, & ideo rei æstimationem, nam de G H iam supponebatur, quod ita esset, perficiam igitur per modum primi suppositi 6i capituli huius libri, corpora D A, D C, D E D F, ut per D C intelligamus cubum B C, per D F cubum A B, per D A triplum C B in quadratum A B, per D E triplum A B in quadratũ B C. quia igitur ex A C in C K fit 2, ex A C in C K ter, fiet 6 numerus rerum, igitur ex A B in triplum A C in C K fiunt 6 res A B, seu sexcuplum A B, quare triplum producti ex A B, B C, A C, est sexcuplum A B, at uero differentia cubi A C, à cubo C K, & existenti à cubo B C ei æq̃le ex supposito, est 20, & ex supposito primo 6i capituli, est aggregatum corporum D A, D E, D F, tria igitur hæc corpora sunt 20, posita uero B C m: cubus A B, æqualis est cubo A C, & triplo A C in quadratum C B, & cubo B C m: & triplo B C in quadratum A C m: per demonstrata illic, differentia autem tripli B C in quadratum A C, à triplo A C in quadratum B C est productum A B, B C, A C, quare cum hoc, ut demonstratum est, æquale sit sexcuplo A B, igitur addito sexcuplo A B, ad id quod fit ex A C in quadratum B C ter, fiet triplum B C in quadratum A C, cum igitur B C sit m: iam ostensum est, quod productum C B



in

Gerolamo Cardano, *Ars Magna* (1545)

A Synopsis of Elementary Results in Pure and Applied Mathematics, G. S. Carr (1886)

ANALYTICAL GEOMETRY OF THREE DIMENSIONS.

(25.) *The straight line.* The equations to a straight line referred to three rectangular co-ordinates, are

$$x = az + \alpha, \qquad y = bz + \beta:$$

which are the equations to its projections on the planes of xz, yz respectively.

The equations to a line passing through the point (x_1,y_1,z_1), are

$$x - x_1 = a(z - z_1), \qquad y - y_1 = b(z - z_1).$$

The equations to a line passing through two points (x_1,y_1,z_1), (x_2,y_2,z_2), are

$$x - x_1 = \frac{x_2 - x_1}{z_2 - z_1}(z - z_1), \qquad y - y_1 = \frac{y_2 - y_1}{z_2 - z_1}(z - z_1).$$

In order that the two lines

$$\begin{cases} x = a_1 z + \alpha_1, \\ y = b_1 z + \beta_1; \end{cases} \qquad \begin{cases} x = a_2 z + \alpha_2, \\ y = b_2 z + \beta_2, \end{cases}$$

may intersect each other, it is necessary that

$$\frac{\alpha_1 - \alpha_2}{a_1 - a_2} = \frac{\beta_1 - \beta_2}{b_1 - b_2}.$$

The co-ordinates of the point of intersection are

$$x = \frac{a_1\alpha_2 - a_2\alpha_1}{a_1 - a_2}, \quad y = \frac{b_1\beta_2 - b_2\beta_1}{a_1 - a_2}, \quad z = \frac{\alpha_2 - \alpha_1}{a_1 - a_2}.$$

The distance (d_1) of a point (x_1,y_1,z_1) from the origin;

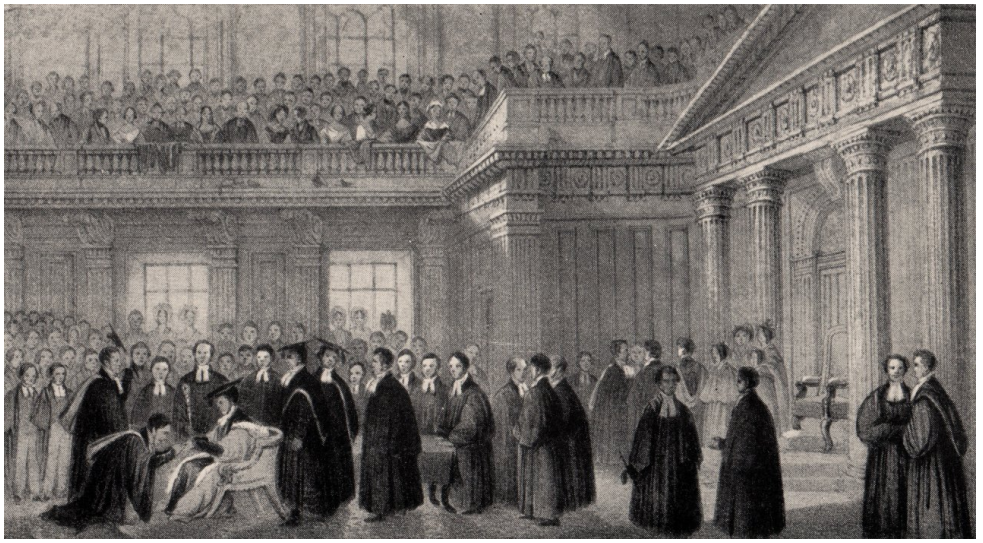
$$d_1 = (x_1^2 + y_1^2 + z_1^2)^{\frac{1}{2}} = z(1 + a^2 + b^2)^{\frac{1}{2}};$$

if $x = az$, $y = bz$ are the equations to the line passing through the given point, and the origin.

The distance (D) between two points (x_1,y_1,z_1), (x_2,y_2,z_2);

$$D = \left|(x_1 - x_2)^2 + (y_1 - y_2)^2 + (z_1 - z_2)^2\right|^{\frac{1}{2}}:$$
$$= \left|d_1^2 + d_2^2 - 2(x_1x_2 + y_1y_2 + z_1z_2)\right|^{\frac{1}{2}},$$

d_2 being the distance of (x_2,y_2,z_2) from the origin.



Senior Wrangler (Cambridge) wikipedia.org

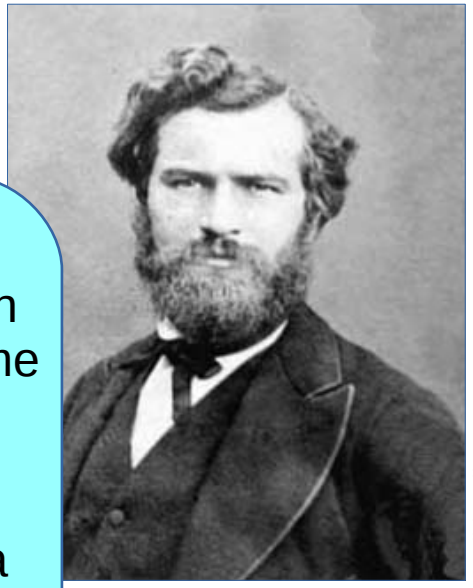
Un des seuls ouvrages à disposition de Srinivasa Ramanujan...

G. Hardy parle de “*rigueur*” :

...read Jordan’s famous *Cours d’analyse*; and I shall never forget the astonishment with which I read that remarkable work, the first inspiration for so many mathematicians of my generation, and learnt for the first time as I read it what mathematics really meant.

Ramanujan was self-taught: *he knew nothing of the modern **rigour***: in a sense he didn't know what a proof was.

A Mathematician's Apology (1940)



wikipedia.org

Camille Jordan
(1838-1922)

wikipedia.org

Godfrey Harold Hardy (1877-1947)

“... his purpose was to bring **rigour** into English mathematical analysis.”

De Hardy à Bertrand Russell :

“If I could prove by logic that you would die in five minutes, I should be sorry you were going to die, but my sorrow would be very much mitigated by pleasure in the **proof**.”

Lettre de Hardy à Ramanujan :

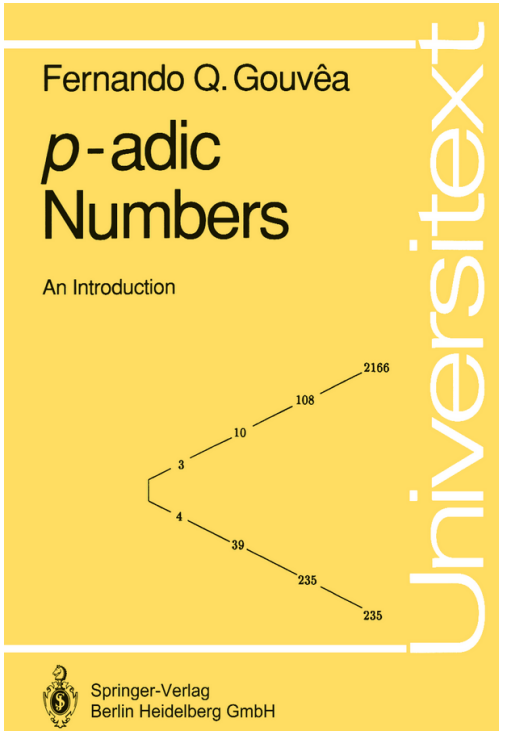
“I want particularly to see your proofs of your assertions here. You will understand that, in this theory, everything depends on **rigorous exactitude of proof**.”

The man who knew infinity, R. Kanigel

Jusqu'où la rigueur peut-elle nous mener ?

"Thus, we proceed without worrying too much about mathematical rigor [1] or precision, but rather emphasizing the ideas that are behind what we are trying to accomplish."

[1] which always runs the risk of becoming mathematical *rigor mortis*...



http://www.foxtrot.com/

Preuve vs. intuition... “*Power of thinking vaguely*”

31	est premier
331	est premier
3331	est premier
33331	est premier
333331	est premier
3333331	est premier
33333331	est premier

Parmi les nombres de Fermat
(une puissance de 2 plus 1)

5	est premier
17	est premier
257	est premier
65537	est premier

Preuve vs. intuition... “*Power of thinking vaguely*”

31	est premier
331	est premier
3331	est premier
33331	est premier
333331	est premier
3333331	est premier
33333331	est premier

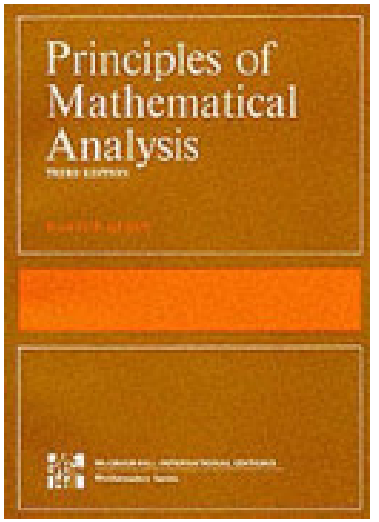
333333331 = 17 x 19607843

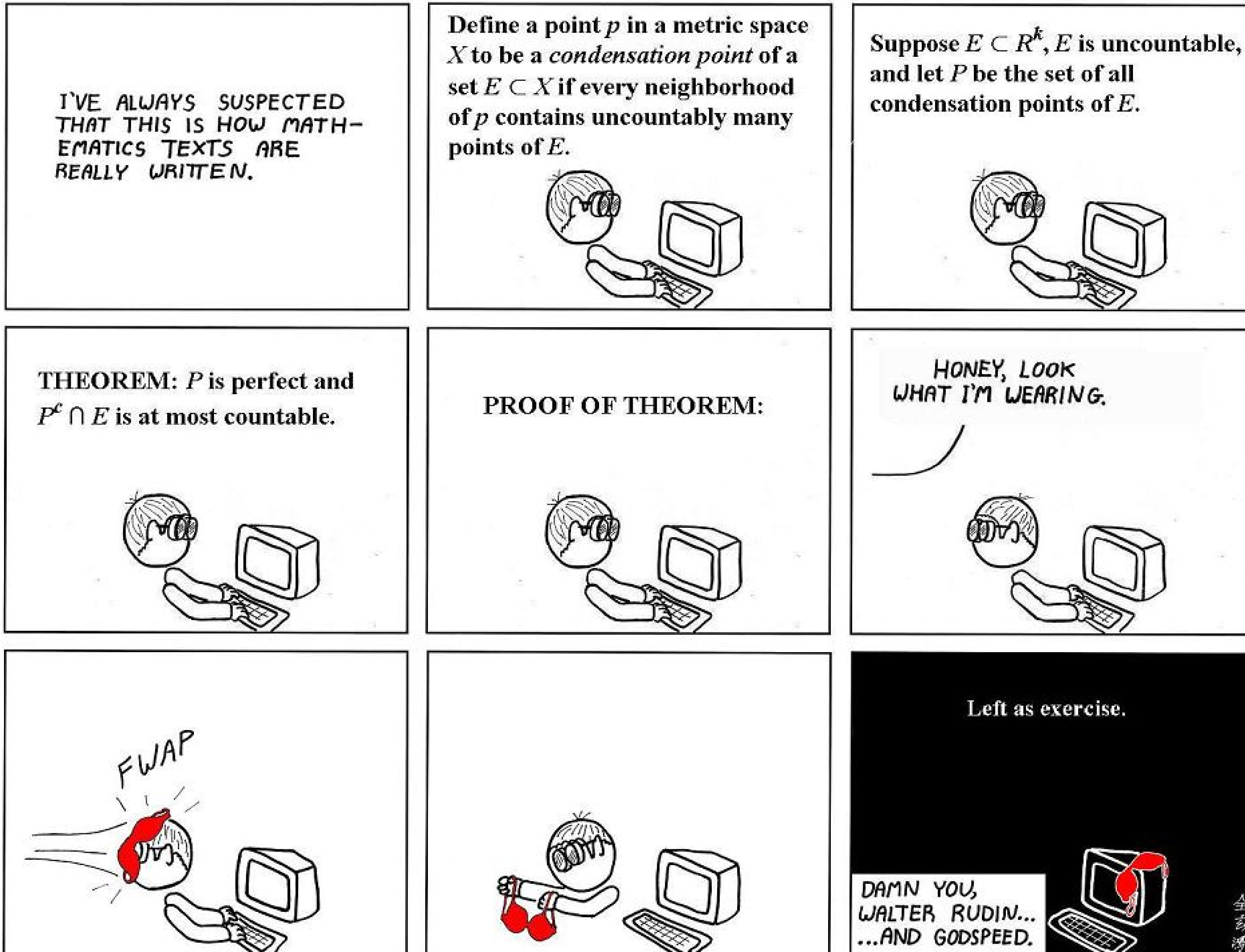
Parmi les nombres de Fermat
(une puissance de 2 plus 1)

5	est premier
17	est premier
257	est premier
65537	est premier

4294967297 = 641 x 6700417

- “C’est trivial !”
- “Il s’agit d’un simple exercice !”

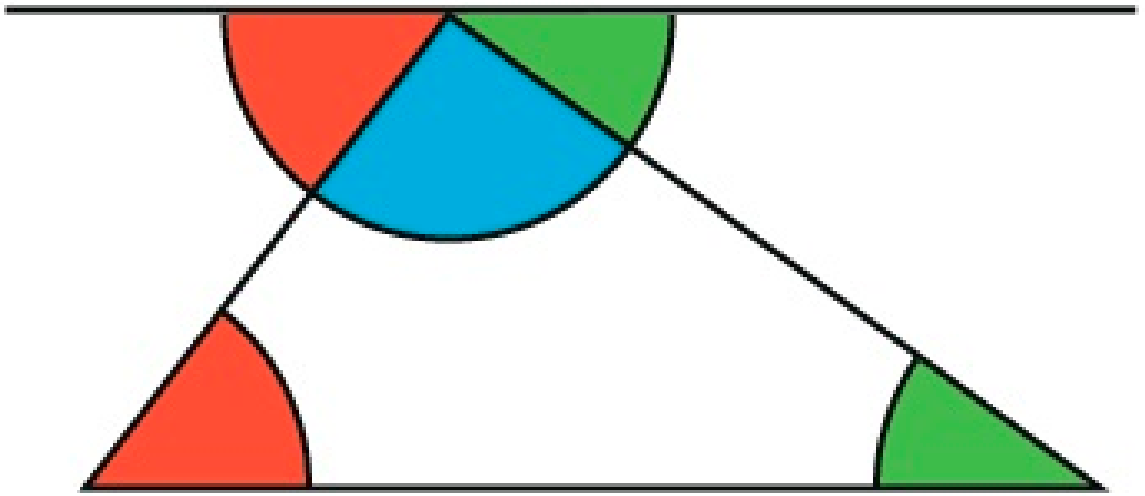



I'VE ALWAYS SUSPECTED THAT THIS IS HOW MATHEMATICS TEXTS ARE REALLY WRITTEN.
Define a point p in a metric space X to be a *condensation point* of a set $E \subset X$ if every neighborhood of p contains uncountably many points of E.
Suppose $E \subset R^k$, E is uncountable, and let P be the set of all condensation points of E.
THEOREM: P is perfect and $P^c \cap E$ is at most countable.
PROOF OF THEOREM:
HONEY, LOOK WHAT I'M WEARING.
FWAP
Left as exercise.
DAMN YOU, WALTER RUDIN... ...AND GODSPEED.

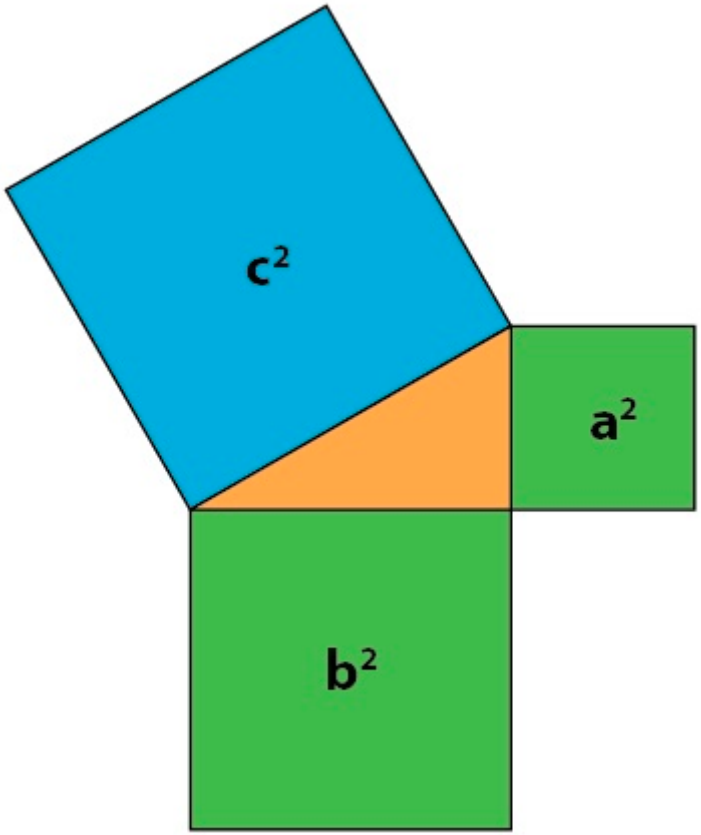
Différents types de preuves

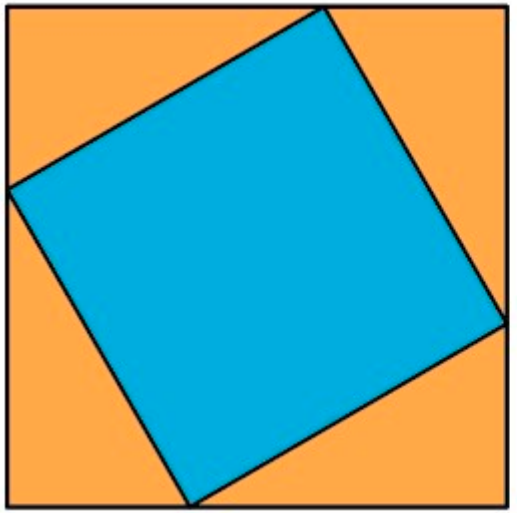
- par l’absurde,
- par récurrence,
- par récurrence forte,
- par disjonction des cas,
- par analyse/synthèse, ...

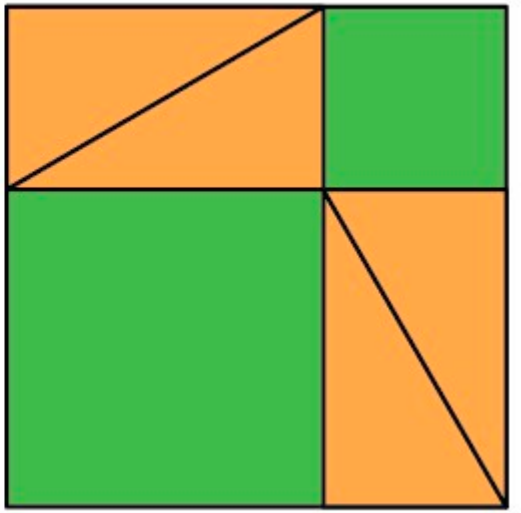
Des preuves sans mot



http://www.qedcat.com/misc/207.html

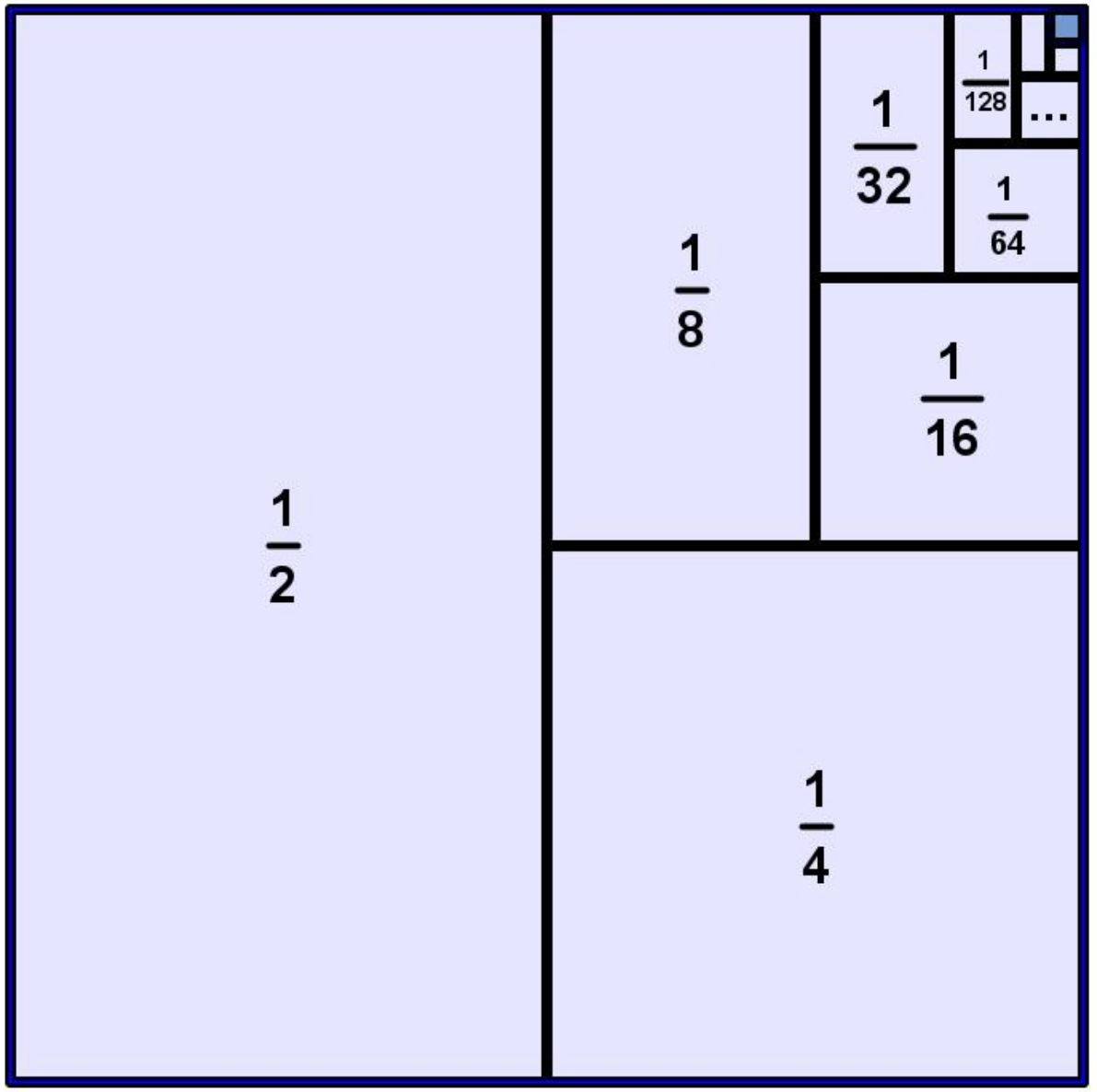






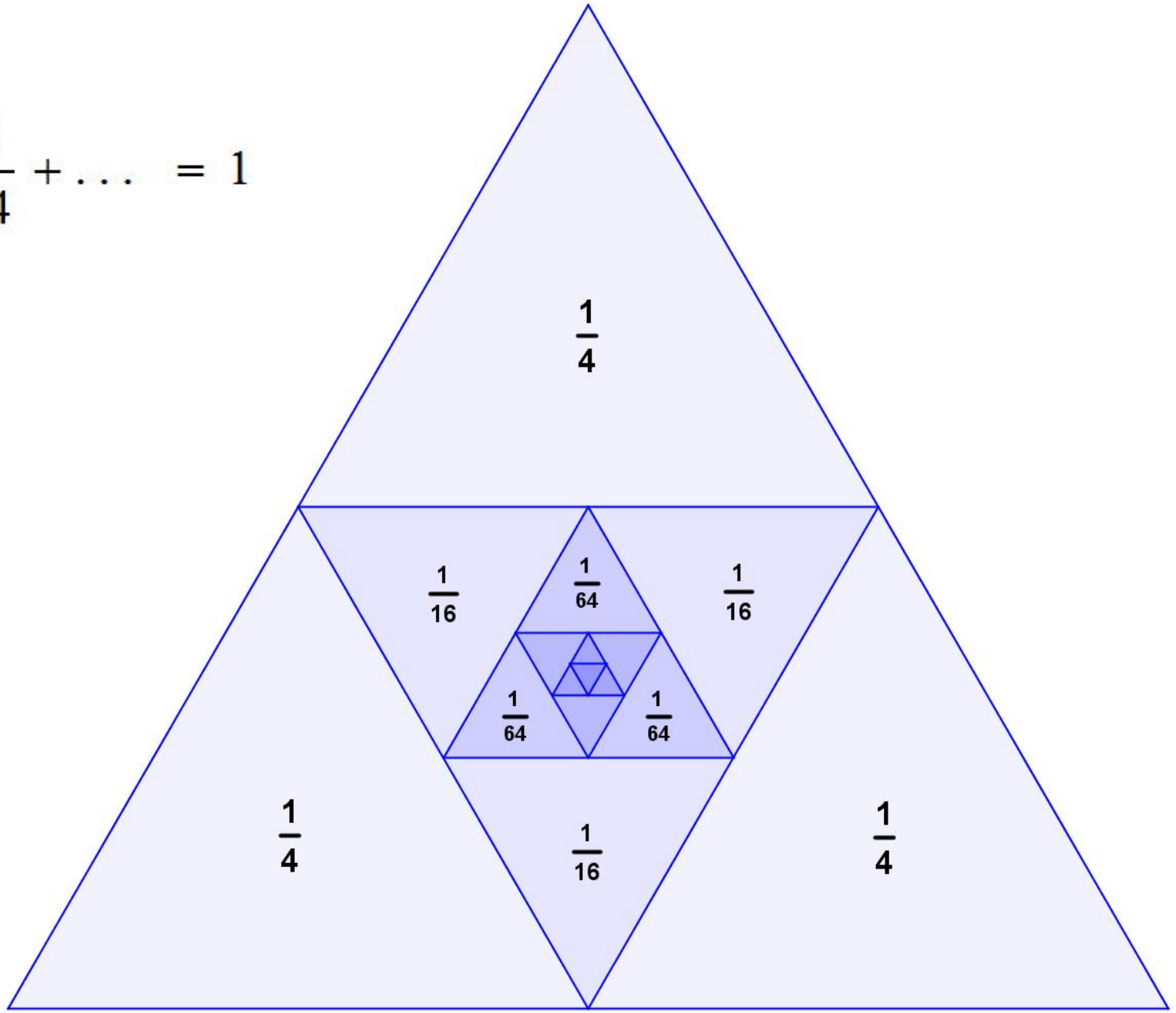
a b

http://www.qedcat.com/misc/207.html



$$\frac{1}{2} + \frac{1}{4} + \frac{1}{8} + \frac{1}{16} + \ldots = 1$$

$$\frac{3}{4} + \frac{3}{16} + \frac{3}{64} + \ldots = 1$$



Les preuves par récurrence

$1+2+3+\ldots+n = n.(n+1)/2$

$1 = 1.2/2 = 1$
$1+2 = 2.3/2 = 3$
$1+2+3 = 3.4/2 = 6$
$1+2+3+4 = 4.5/2 = 10$

ETAPE 1.
Vrai pour p=1 : 1=1.2/2

ETAPE 2.
Si la propriété est satisfaite pour p,
alors elle l'est encore pour p+1

Hyp : $1+2+3+\ldots+p = p.(p+1)/2$
Thèse : $1+2+3+\ldots+p+(p+1) = (p+1).(p+2)/2$

$1+2+3+\ldots+p+(p+1) = p.(p+1)/2 + p+1 = [p.(p+1)+2.(p+1)]/2$

Les preuves par récurrence

$1+2+3+\ldots+n = n.(n+1)/2$

$1 = 1.2/2 = 1$
$1+2 = 2.3/2 = 3$
$1+2+3 = 3.4/2 = 6$
$1+2+3+4 = 4.5/2 = 10$

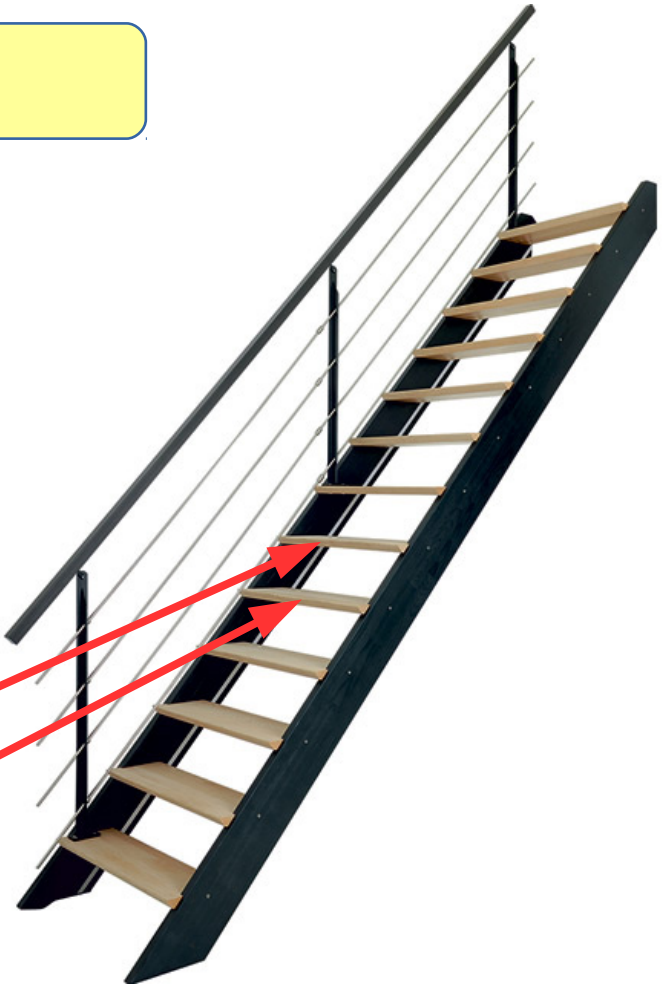
ETAPE 1.
Vrai pour p=1 : $1=1.2/2$

ETAPE 2.
Si la propriété est satisfaite pour p,
alors elle l'est encore pour p+1

Hyp : $1+2+3+\ldots+p = p.(p+1)/2$
Thèse : $1+2+3+\ldots+p+(p+1) = (p+1).(p+2)/2$

$1+2+3+\ldots+p+(p+1) = p.(p+1)/2 + p+1 = [p.(p+1)+2.(p+1)]/2$

Les preuves par récurrence



$1+2+3+\ldots+n = n.(n+1)/2$

$1 = 1.2/2 = 1$
$1+2 = 2.3/2 = 3$
$1+2+3 = 3.4/2 = 6$
$1+2+3+4 = 4.5/2 = 10$

ETAPE 1.
Vrai pour p=1 : 1=1.2/2

ETAPE 2.
Si la propriété est satisfaite pour p,
alors elle l'est encore pour p+1

Hyp : $1+2+3+\ldots+p = p.(p+1)/2$
Thèse : $1+2+3+\ldots+p+(p+1) = (p+1).(p+2)/2$

$1+2+3+\ldots+p+(p+1) = p.(p+1)/2 + p+1 = [p.(p+1)+2.(p+1)]/2$

Les preuves par récurrence

$1+2+3+...+n = n.(n+1)/2$

$1 + 2 + 3 + \ldots + (n-2) + (n-1) + n$
$n + (n-1) + (n-2) + \ldots + 3 + 2 + 1$

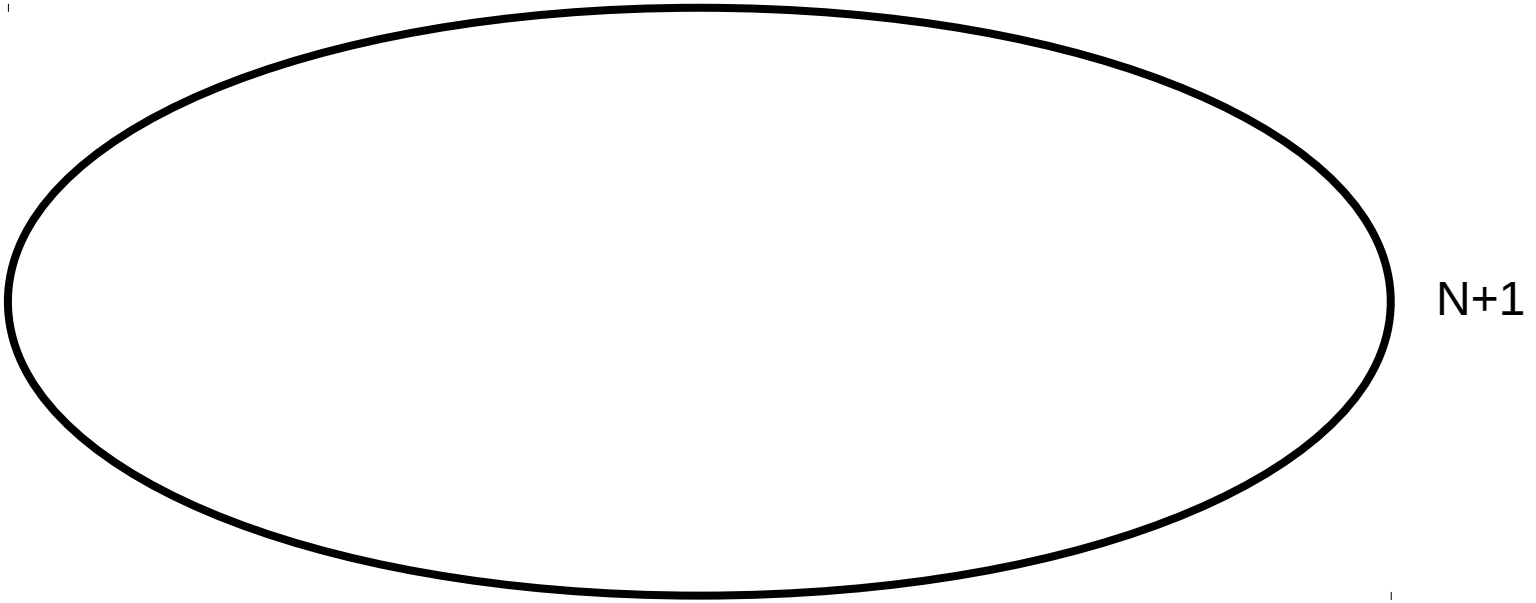
K. F. Gauss (1777-1855)

Théorème (FAKE NEWS !) : *Tous les chevaux ont la même couleur*.

Preuve par récurrence sur le nombre N de chevaux.

Si N=1 : tous les chevaux de l'ensemble ont la même couleur.

Si la propriété est vérifiée pour un ensemble de N chevaux,
l'est-elle encore pour un ensemble à N+1 chevaux ?

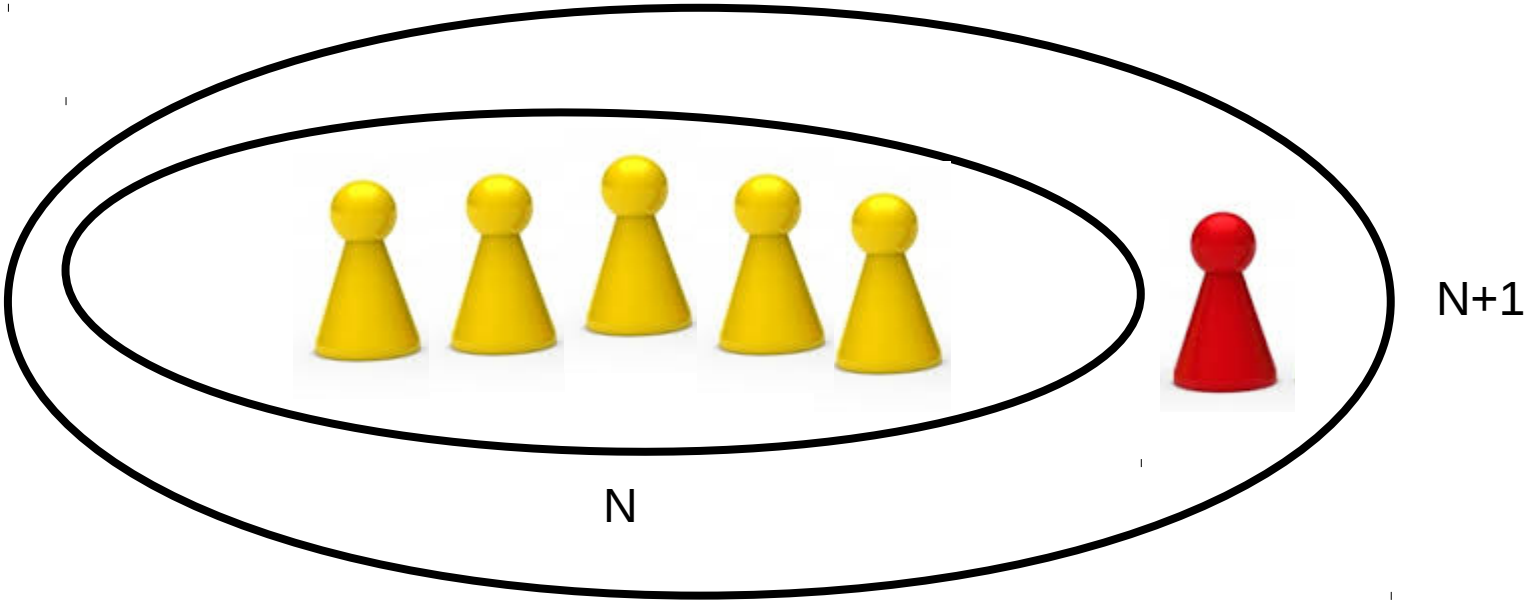


Théorème (FAKE NEWS !) : *Tous les chevaux ont la même couleur*.

Preuve par récurrence sur le nombre N de chevaux.

Si N=1 : tous les chevaux de l'ensemble ont la même couleur.

Si la propriété est vérifiée pour un ensemble de N chevaux,
l'est-elle encore pour un ensemble à N+1 chevaux ?

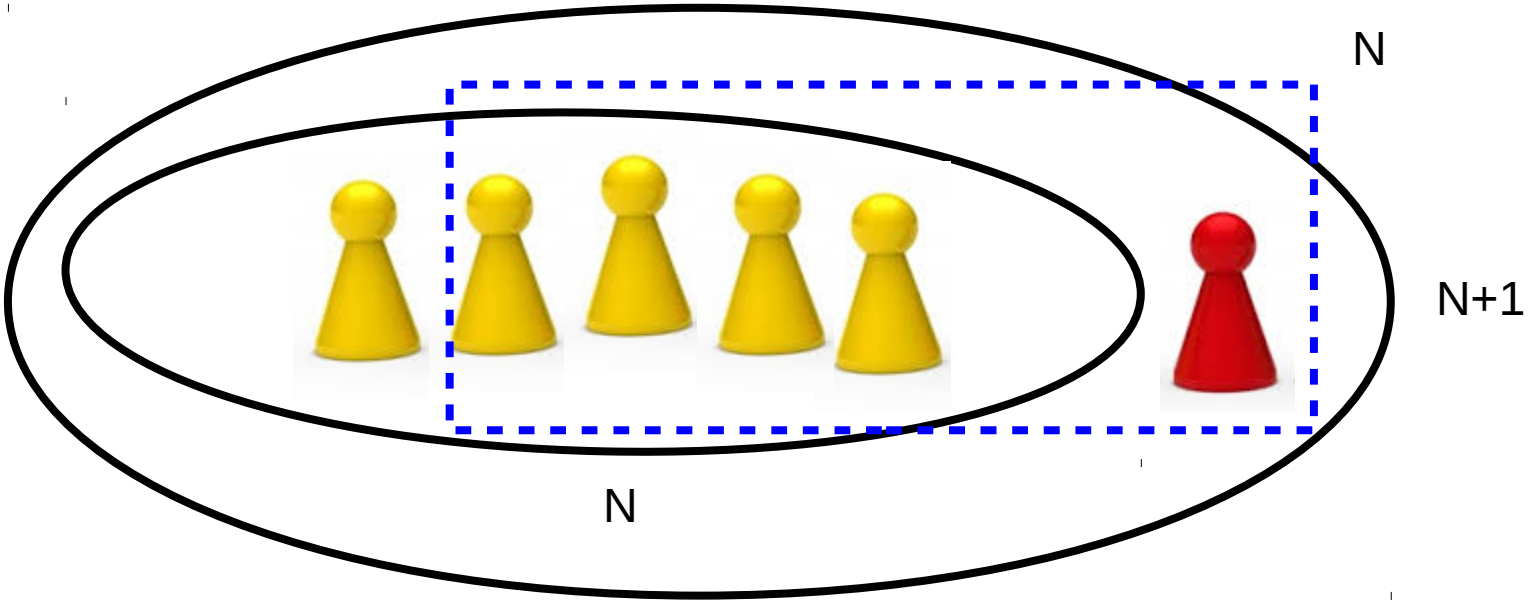


Théorème (FAKE NEWS !) : *Tous les chevaux ont la même couleur*.

Preuve par récurrence sur le nombre N de chevaux.

Si N=1 : tous les chevaux de l'ensemble ont la même couleur.

Si la propriété est vérifiée pour un ensemble de N chevaux,
l'est-elle encore pour un ensemble à N+1 chevaux ?

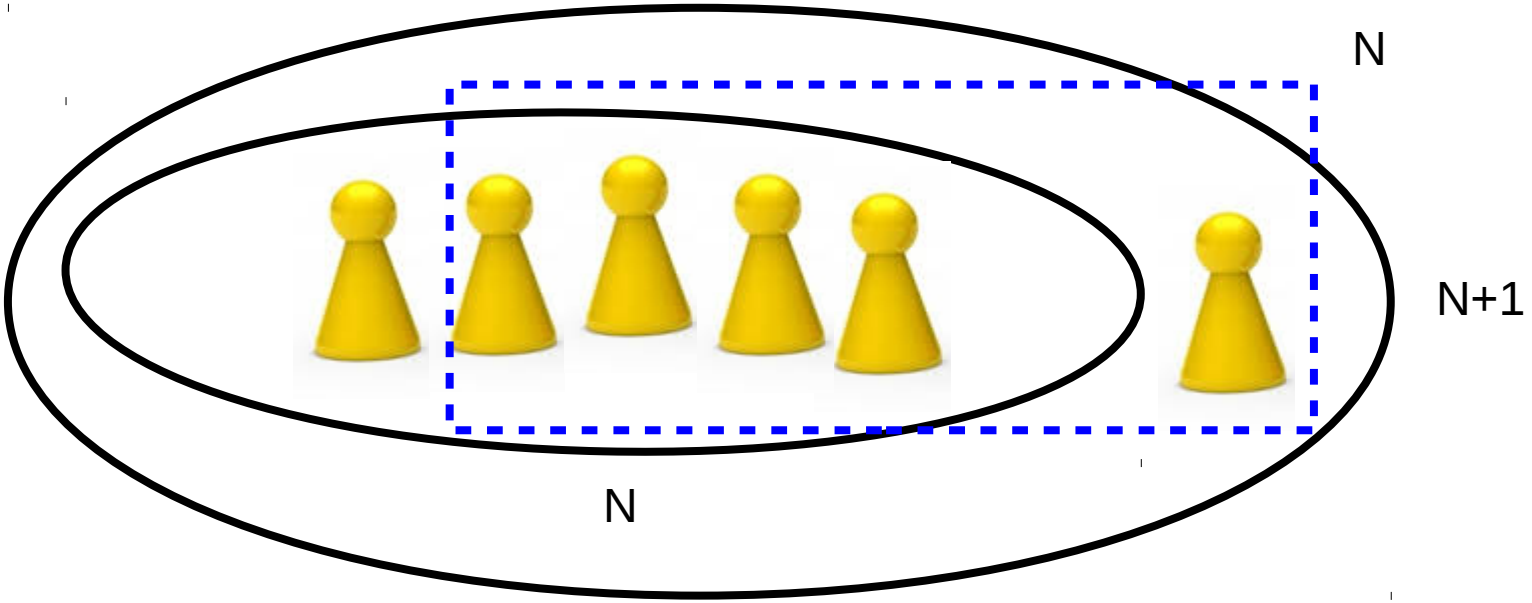


Théorème (FAKE NEWS !) : *Tous les chevaux ont la même couleur*.

Preuve par récurrence sur le nombre N de chevaux.

Si N=1 : tous les chevaux de l'ensemble ont la même couleur.

Si la propriété est vérifiée pour un ensemble de N chevaux,
l'est-elle encore pour un ensemble à N+1 chevaux ?



Faire une preuve permet de démontrer un résultat
MAIS
permet aussi de développer de nouveaux outils,
de nouvelles théories !

wikipedia.org

"*A large part of mathematics which becomes useful developed with absolutely no desire to be useful, and in a situation where nobody could possibly know in what area it would become useful*".

(John Von Neumann, 1903-1957)

The $3x+1$ Problem: An Annotated Bibliography (1963–1999) (Sorted by Author)

Jeffrey C. Lagarias
Department of Mathematics
University of Michigan
Ann Arbor, MI 48109–1109
lagarias@umich.edu

(January 1, 2011 version)

ABSTRACT. The $3x+1$ problem concerns iteration of the map $T : \mathbb{Z} \to \mathbb{Z}$ given by

$$T(x) = \begin{cases} \dfrac{3x+1}{2} & \text{if } x \equiv 1 \pmod 2 \ . \\ \\ \dfrac{x}{2} & \text{if } x \equiv 0 \pmod 2 \ . \end{cases}$$

The $3x+1$ Conjecture asserts that each $m \geq 1$ has some iterate $T^{(k)}(m) = 1$. This is an annotated bibliography of work done on the $3x+1$ problem and related problems from 1963 through 1999. At present the $3x+1$ Conjecture remains unsolved.

La beauté d’une preuve ?

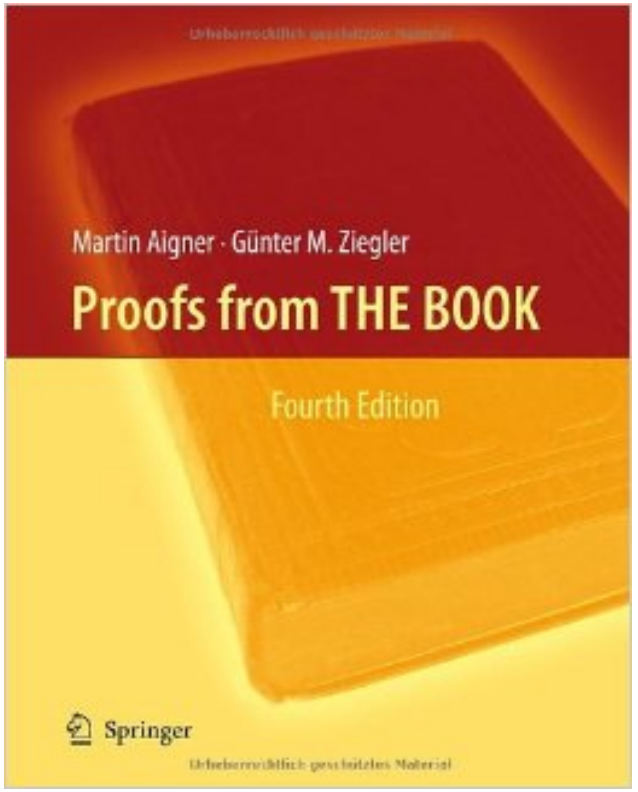
… because it is difficult, and because I have no qualifications for any serious discussion in aesthetics. The beauty of a mathematical theorem depends a great deal on its seriousness, as even in poetry the beauty of a line may depend to some extent on the significance of the ideas which it contains.

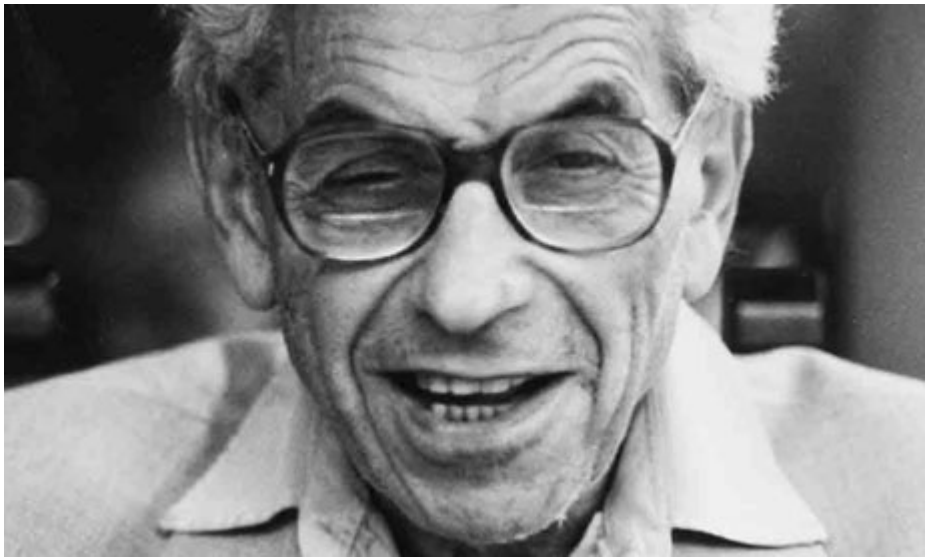
A Mathematician's Apology (1940)

Paul Erdős liked to talk about The Book, in which God maintains the *perfect proofs for mathematical theorems*, following the dictum of G. H. Hardy that there is *no permanent place for ugly mathematics*.

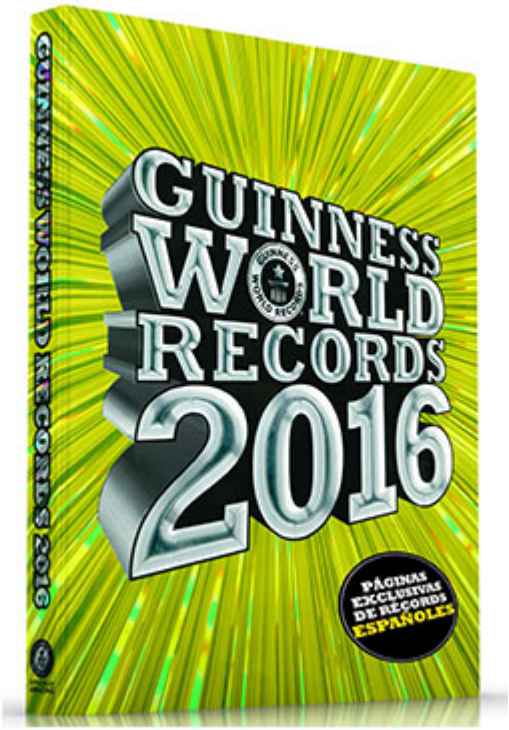
Erdős also said that :

you need not believe in God but,
as a mathematician, you should believe in The Book.





Quelques records...



- "*Boolean Pythagorean triples problem*" preuve : 200 Terabytes

Peut-on colorer les naturels avec 2 couleurs Rouge / Bleu
de telle sorte qu'aucun triplet pythagoricien ne soit *monochromatique*.
Aucune solution, pour plus que les 7824 premiers naturels.

Ex : 3, 4, 5

https://lejournal.cnrs.fr/articles/la-plus-grosse-preuve-de-lhistoire-des-mathematiques

- Andrew Wiles, *Modular elliptic curves and Fermat's Last Theorem* (1995) : 108 pages
7 ans de travail, preuve de plus de 150 pages, un "trou" comblé avec R. Taylor...

- Preuve de la "conjecture *abc*" Shinichi Mochizuki :
suite de 4 papiers (2016); la preuve s'étend sur plus 500 pages

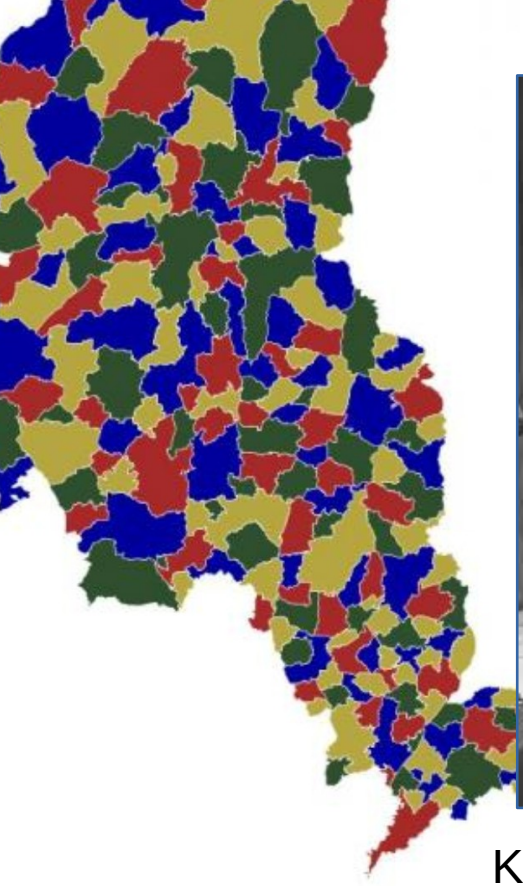
"Monumental proof to torment mathematicians for years to come" (Nature)

Qui fait des preuves ?

Depuis les grecs, les mathématiciens, les juristes, les ordinateurs … (preuves formelles)

“No, That's Not A Laptop On An Ancient Greek Grave Marker”

J. Paul Getty Museum, Malibu



K. Appel, W. Haken (1975)

Grand nombre (fini) de cas à traiter

Formal Proof—The Four-Color Theorem

Georges Gonthier

The Tale of a Brainteaser

Francis Guthrie certainly did it, when he coined his innocent little coloring puzzle in 1852. He managed to embarrass successively his mathematician brother, his brother's professor, Augustus de Morgan, and all of de Morgan's visitors, who couldn't solve it; the Royal Society, who only realized ten years later that Alfred Kempe's 1879 solution was wrong; and the three following generations of mathematicians who couldn't fix it [19].

Even Appel and Haken's 1976 triumph [2] had a hint of defeat: they'd had a computer do the proof for them! Perhaps the mathematical controversy around the proof died down with their book [3] and with the elegant 1995 revision [13] by Robertson, Saunders, Seymour, and Thomas. However something was still amiss: both proofs combined a textual argument, which could reasonably be checked by inspection, with computer code that could not. Worse, the empirical evidence provided by running code several times with the *same* input is weak, as it is blind to the most common cause of "computer" error: programmer error.

For some thirty years, computer science has been working out a solution to this problem: formal program proofs. The idea is to write code that describes not only *what* the machine should do, but also *why* it should be doing it—a formal proof of correctness. The validity of the proof is an objective mathematical fact that can be checked by a *different* program, whose own validity can be ascertained empirically because it does run on *many* inputs. The main technical difficulty is that formal proofs are very difficult to produce, even with a language rich enough to express all mathematics.

In 2000 we tried to produce such a proof for part of code from [13], just to evaluate how the field had progressed. We succeeded, but now a new question emerged: was the statement of the correctness proof (the *specification*) itself correct? The only solution to that conundrum was to formalize the *entire* proof of the Four-Color Theorem, not just its code. This we finally achieved in 2005.

While we tackled this project mainly to explore the capabilities of a modern formal proof system—at first, to benchmark speed—we were pleasantly surprised to uncover new and rather elegant nuggets of mathematics in the process. In hindsight this might have been expected: to produce a formal proof one must make explicit every single logical step of a proof; this both provides new insight in the structure of the proof, and forces one to use this insight to discover every possible symmetry, simplification, and generalization, if only to cope with the sheer amount of imposed detail. This is actually how all of sections "Combinatorial Hypermaps" (p. 1385) and "The Formal Theorem" (p. 1388) came about. Perhaps this is the most promising aspect of formal proof: it is not merely a method to make absolutely sure we have not made a mistake in a proof, but also a tool that shows us and compels us to understand why a proof works.

In this article, the next two sections contain background material, describing the original proof and the Coq formal system we used. The following two sections describe the sometimes new mathematics involved in the formalization. Then the next two sections go into some detail into the two main parts of the formal proof: reducibility and

Georges Gonthier is a senior researcher at Microsoft Research Cambridge. His email address is gonthier@microsoft.com.

Empilement optimal de sphères, *conjecture de Kepler*

Wikipedia : In January 2003, Thomas Hales (1998) announced the start of a collaborative project Flyspeck to produce a complete formal proof of the Kepler conjecture.

The aim was to remove any remaining uncertainty about the validity of the proof by creating a formal proof that can be verified by automated proof checking software such as *HOL Light* and *Isabelle*.

$$\frac{\pi}{3\sqrt{2}} = 0.740480489\ldots$$

http://experimentalmath.info

Il n'existe pas de plan projectif d'ordre 10 (1989)

Théorème de la double bulle (1995)

Ces (longues) preuves formelles ne fournissent pas d'explication...

Doron Zeilberger & SHALOSH B. EKHAD

"*The deductive method ruled mathematics for the last 2500 years, now it is the turn of the inductive method.*"

All the theorems in this textbook were automatically discovered (and of course proved) by computer. The discovery program started with 3 generic points in the plane, and iteratively constructed new points, lines, and circles using a few primitives. Whenever a new point (or line, or circle, or whatever) coincided with an old one, a "theorem" was born.

Using an analogous method for guessing, after cranking-out enough data, we can get these generating functions easily, using procedure

`GFrameDouble(a1,a2,b1,b2,x,y,N)`

in `RITSUF`. For example, if $D(m,n)$ is the number of domino tilings of $Frame(2,2,2,2,m,n)$, then

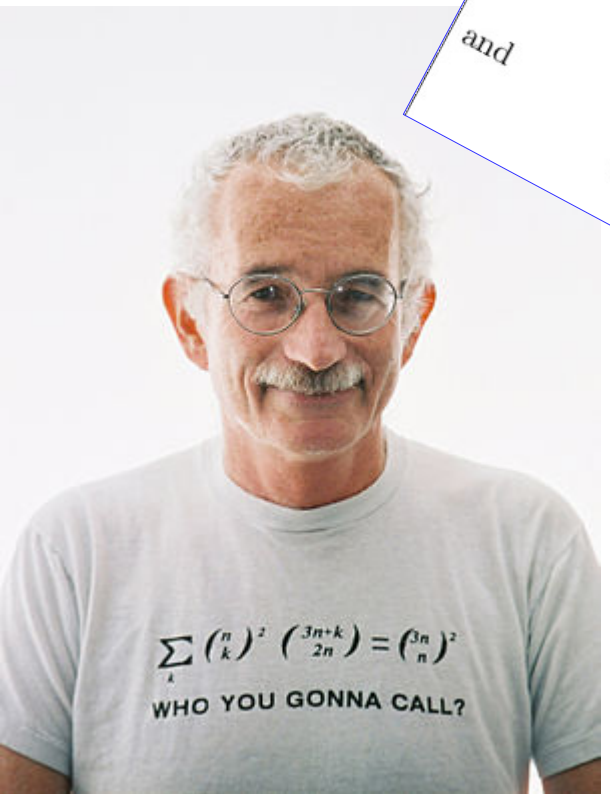
$$\sum_{m=0}^{\infty}\sum_{n=0}^{\infty} D(m,n)x^m y^n = \frac{P(x,y)}{Q(x,y)} ,$$

where

$$P(x,y) = 4x^3y^3 - 7x^3y^2 - 7x^2y^3 - 14x^3y + 10x^2y^2 - 14xy^3 + 13x^3 + 35x^2y + 35xy^2 + 13y^3 - 30x^2 + 10xy - 30y^2 - 23x - 23y + 36 ,$$

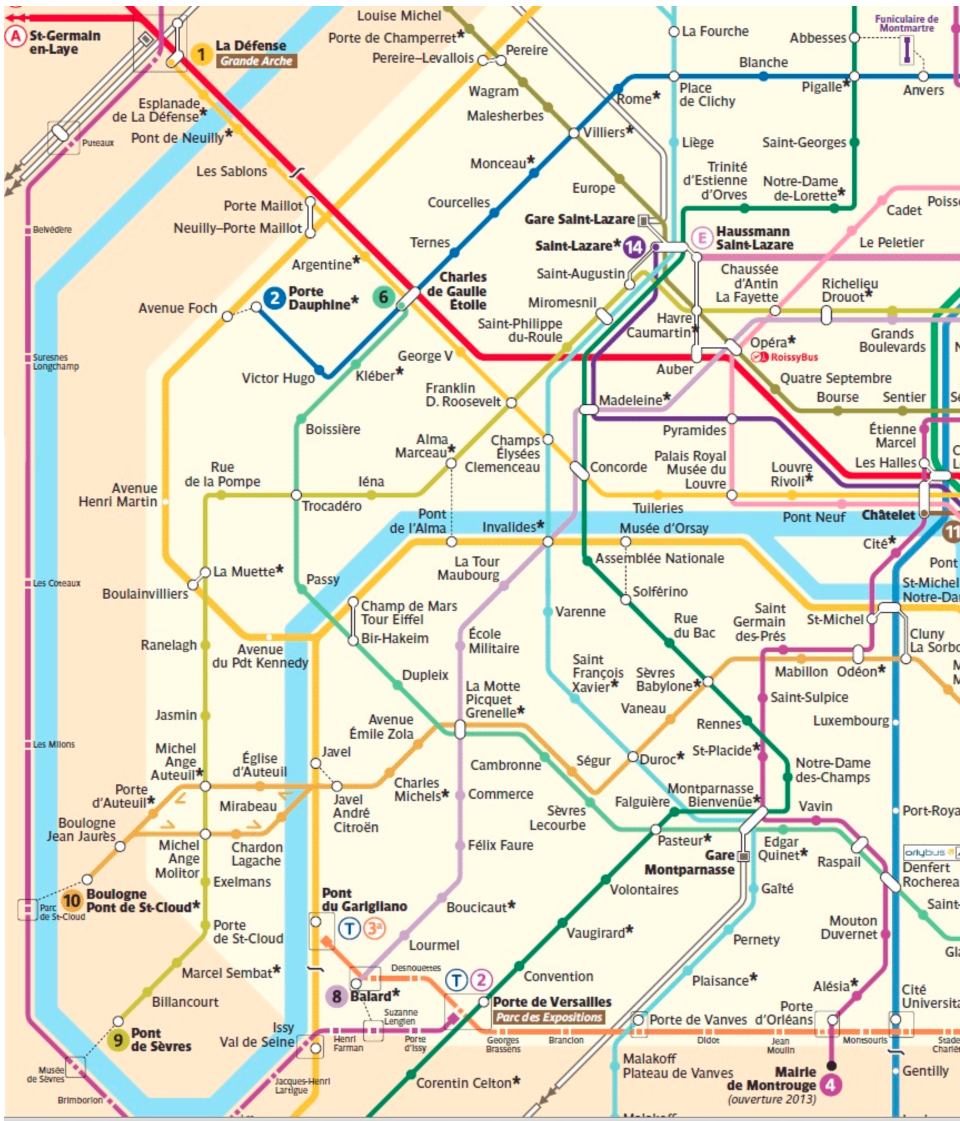
and

$$Q(x,y) = (x-1)(x+1)(x^2-3x+1)(y-1)(y+1)(y^2-3y+1) .$$



Vérification de programmes

Métro à Paris :
Ligne 14,
Saint-Lazare — Olympiades



Peut-on *tout* prouver ?

- Théorème(s) d'incomplétude (K. Gödel 1931)

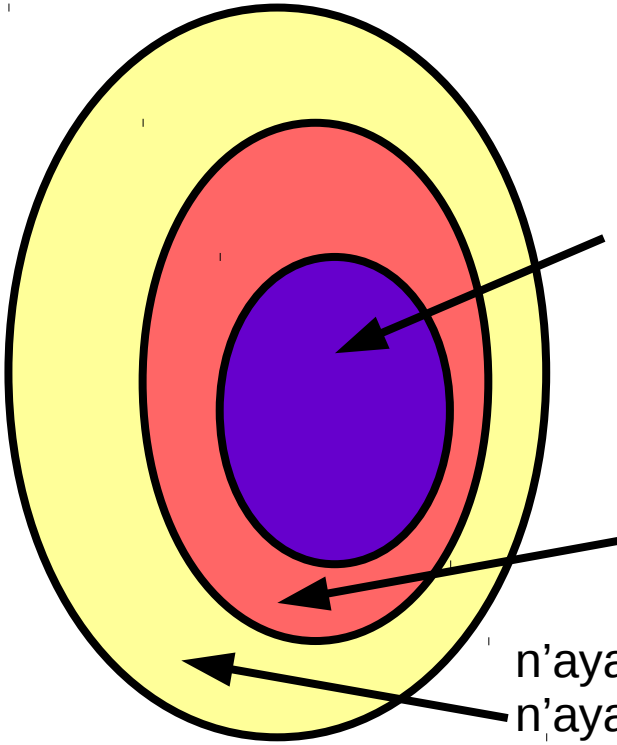
  "Une théorie contenant l'arithmétique est nécessairement incomplète :
  il existe des énoncés qui n'y sont ni démontrables, ni réfutables."

  L'hypothèse du continu est "indépendante" de la théorie des ensembles (ZFC)

- Théories (in)décidables

  existe-t-il un algorithme qui réponde toujours oui/non à la question
  de savoir si un énoncé donné est démontrable dans cette théorie ?
  Autrement dit, savoir si un énoncé est un théorème...

  Thm. de Church (1936) : la théorie du premier ordre du calcul des prédicats
  est indécidable.



Propositions ayant des preuves axiomatiques courtes

n’ayant pas de preuves axiomatiques courtes,
mais des preuves courtes par calcul

n’ayant pas de preuves axiomatiques courtes et
n’ayant pas de preuves courtes par calcul

Si tous les énoncés démontrables de longueur *n* avaient une preuve axiomatique (resp. par calcul) de taille bornée, e.g., au plus 2^n, alors par énumération, on pourrait toujours décider si un énoncé est ou non démontrable.

Ceci contredirait le thm. de Church.