PROOF AND PROGRESS IN MATHEMATICS

By Ming Ng

MATHS & PAIN

Math Can Be Truly Painful, Brain Study Shows

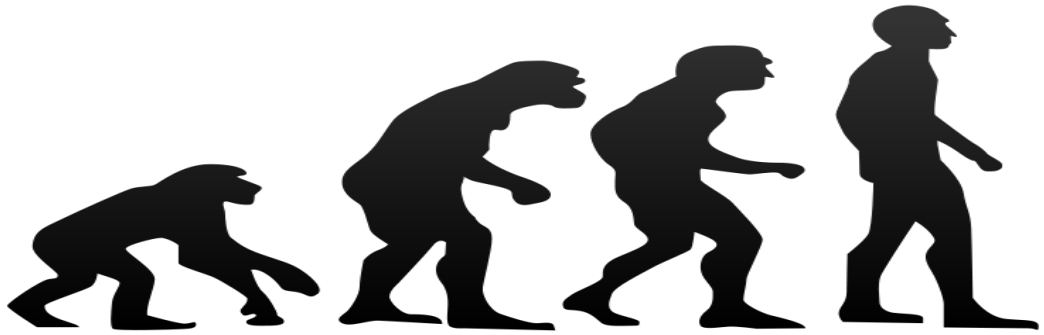
For math-phobes, anticipation of math work activates pain centers in brain.

By **Jeremy Berlin**, National Geographic News

PUBLISHED NOVEMBER 7, 2012

WHAT IS "EVOLUTION"?

- "Evolution is not just any kind of change occurring over a particular stretch of time, it is also a *continuous* kind of change, i.e. a process of change where the past conditions have some kind of meaningful influence on the present as well as the range of future potential states. "

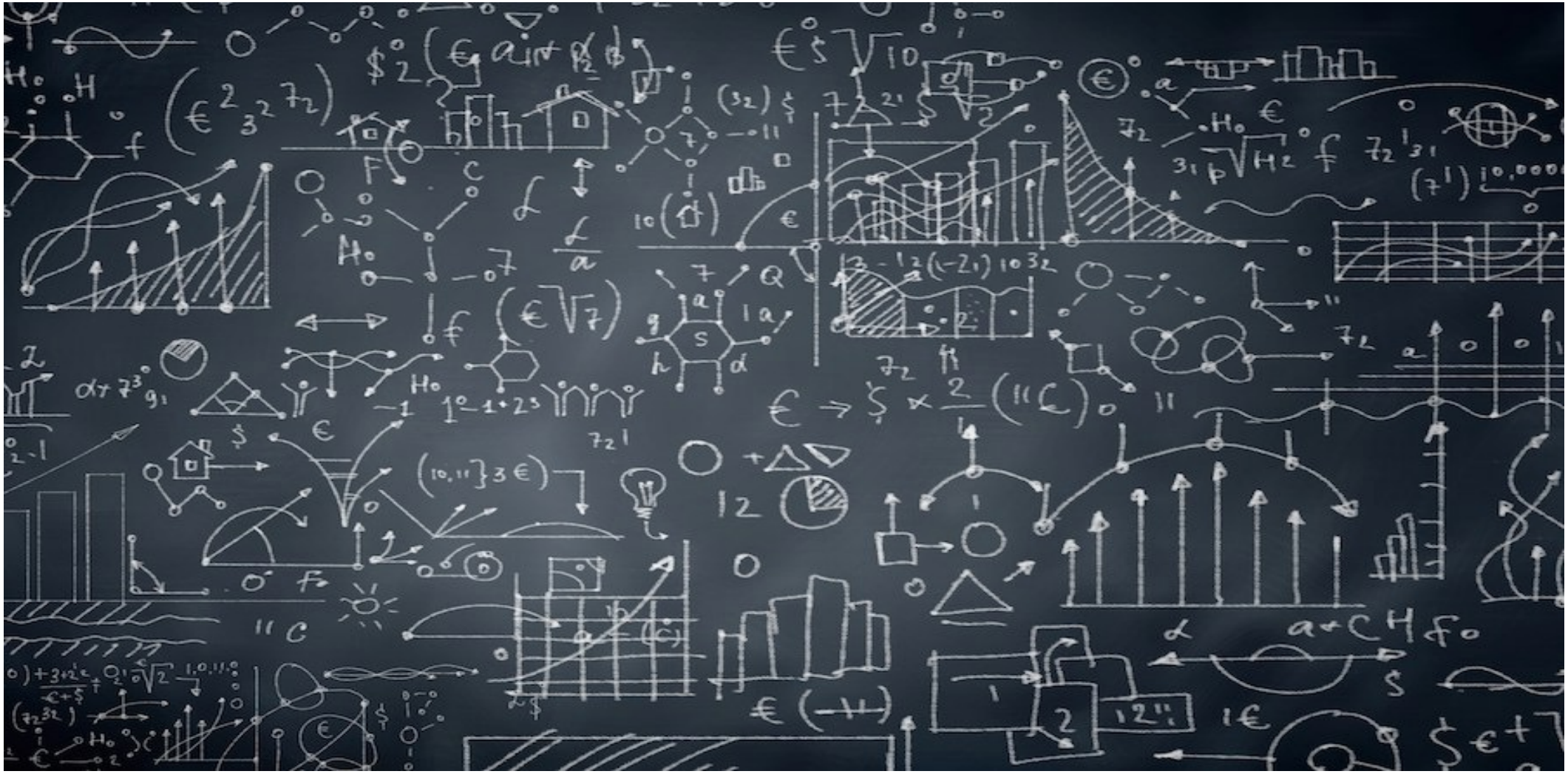


EVOLUTION OF MATHEMATICAL KNOWLEDGE

- "All sciences including the most evolved are characterised by a state of perpetual becoming" - Jean Piaget

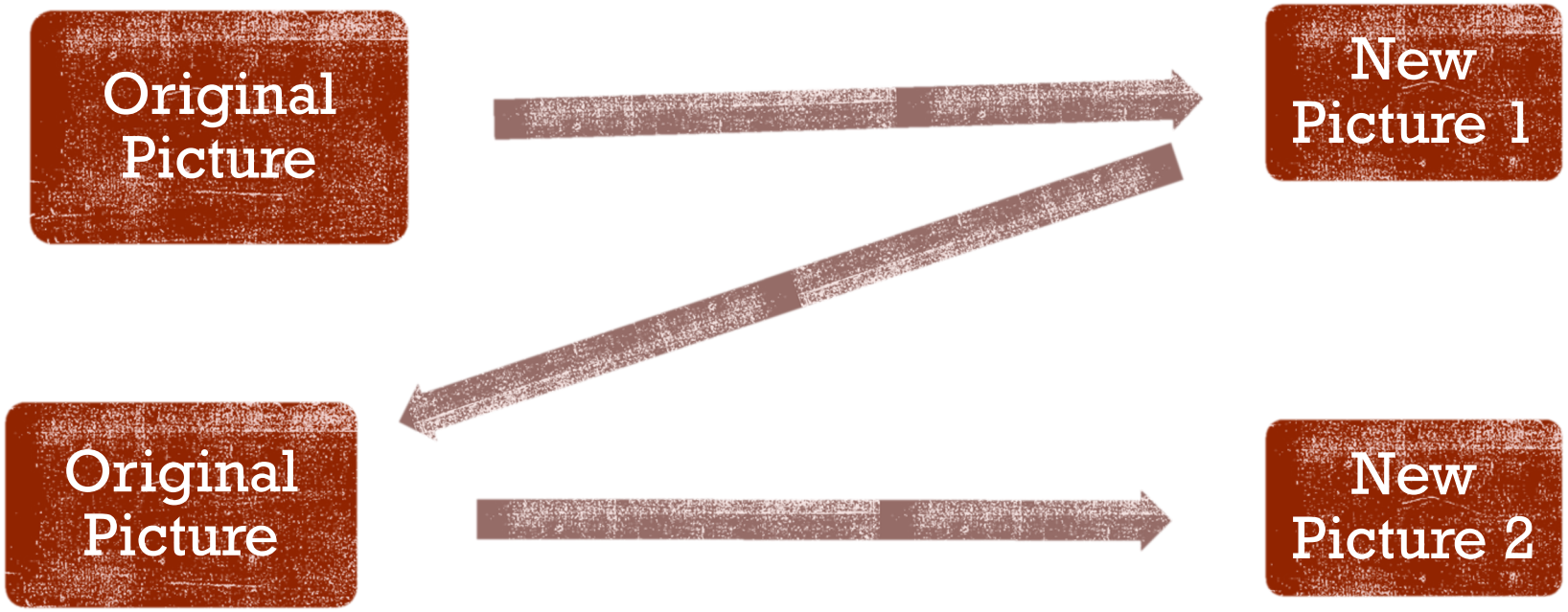
- "*A mathematical theory is not to be considered complete unless you made it so clear that you can explain it to the man in the street.*" - Henri Poincaré

KNOWLEDGE: FORM FROM FORMLESSNESS



HOW IS MATHEMATICAL KNOWLEDGE CONSTRUCTED?

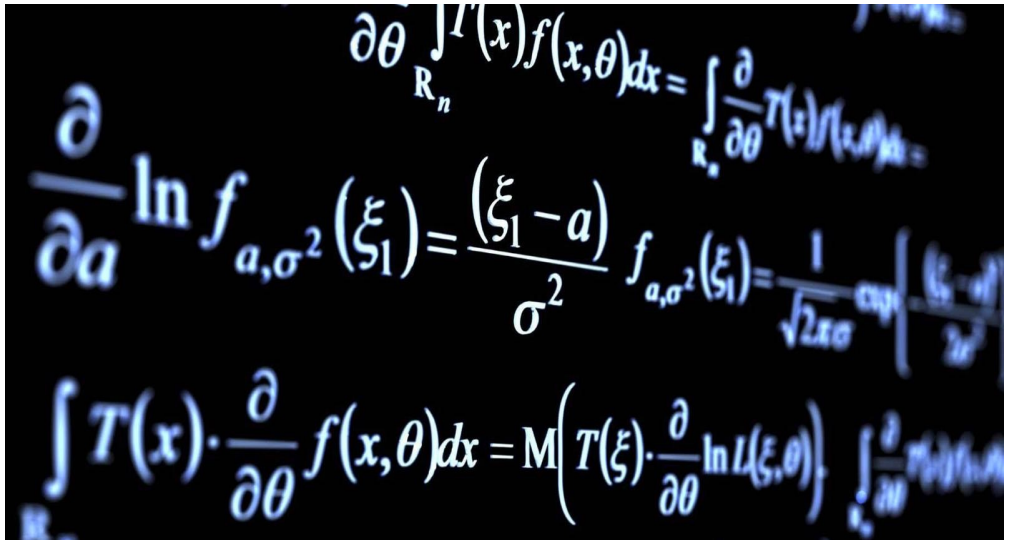
HOW IS MATHEMATICAL KNOWLEDGE CONSTRUCTED?



HOW IS MATHEMATICAL KNOWLEDGE CONSTRUCTED?

HOW IS MATHEMATICAL KNOWLEDGE CONSTRUCTED?

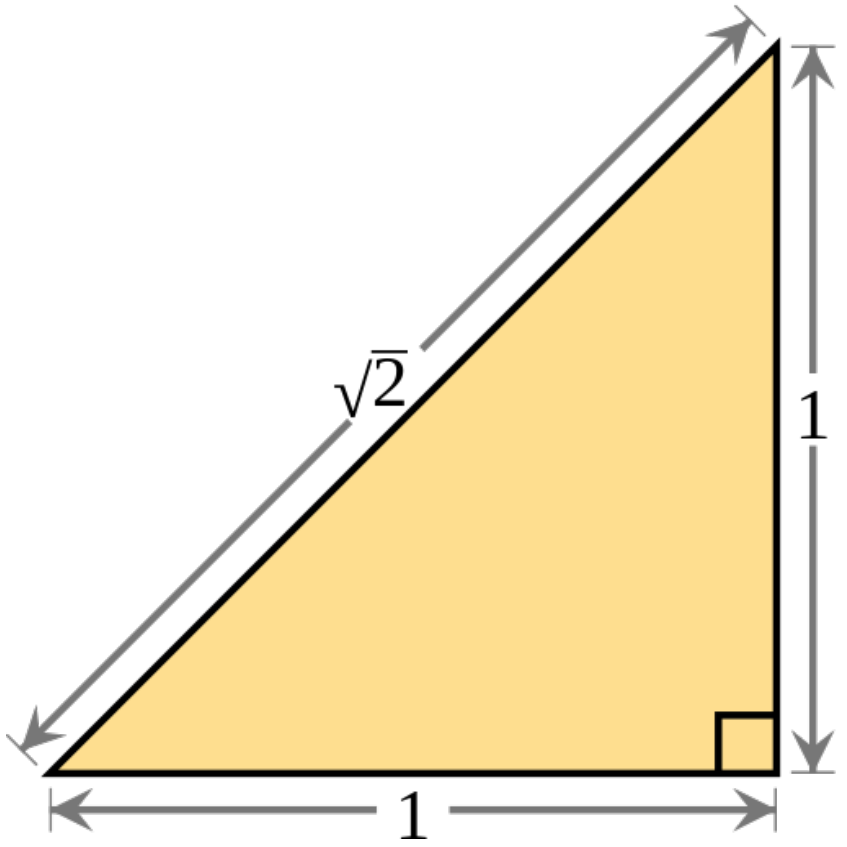
- Knowledge: Justified True Belief
  - Mathematical Justification
    - Proofs
    - Tools & Mathematical Machinery
  - Mathematical Intuition
  - Mathematical Evidence



IS $\sqrt{2}$ AN IRRATIONAL NUMBER?

Some definitions

- Integers are basically whole numbers - e.g. 2, 3, -67 etc. If number a is an integer, we may express this fact as $a \in \mathbb{Z}$.
- A rational number x is any number that can be written in the form $x = \frac{a}{b}$, where $a, b \in \mathbb{Z}$, i.e. a and b are integers
- If a number x cannot be written in this form, then x is an irrational number.
- Hence, the question as to whether $\sqrt{2}$ is a rational number or not may be rewritten as asking whether there exists integers a and b such that $\sqrt{2} = \frac{a}{b}$.



IS $\sqrt{2}$ AN IRRATIONAL NUMBER?

Proof (by contradiction)

- Suppose for contradiction that $\sqrt{2}$ is a rational number. Then, we may express it as $\sqrt{2} = \frac{a}{b}$, where a and b are integers and $b \neq 0$.
- Note that any fraction may be reduced to the simplest terms by getting rid of common factors, i.e. we can express any rational number $r = \frac{a}{b}$ as a fraction $r = \frac{a'}{b'}$ where a' and b' have the greatest common factor of 1.
- E.g. $\frac{12}{30} = \frac{6\times2}{6\times5} = \frac{2}{5}$, where the greatest common factor of 2 and 5 is 1.
- Hence, let us assume for simplicity that $\frac{a}{b}$ is simplified to lowest terms, i.e. we assume that the greatest common factor between a and b is 1.
- Note: If this is the case, then a and b cannot both be even, otherwise their greatest common factor would be 2. Hence, one or both must be odd.

IS $\sqrt{2}$ AN IRRATIONAL NUMBER?

Proof

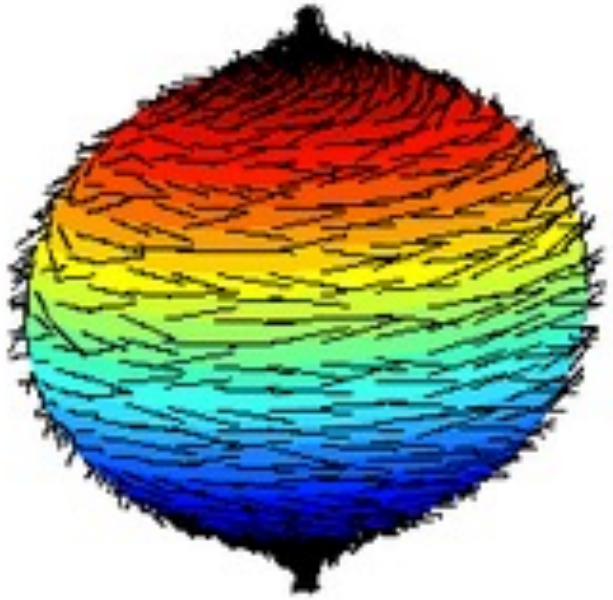
- Since $\sqrt{2} = \frac{a}{b}$, it follows from squaring both sides that $2 = \frac{a^2}{b^2}$. Hence, a^2 is an even number.
- From this, it follows that a has to be even as well, because the square of any odd number is also odd. Let us thus express a as $a = 2k$ for some number k.
- Hence, plugging this into the original equation $2 = \frac{a^2}{b^2}$, we get: $2 = \frac{(2k)^2}{b^2} = \frac{4k^2}{b^2}$
- Rearranging terms on either side of the equation, this in turn implies: $2b^2 = 4k^2 \Rightarrow b^2 = 2k^2$, which (by our above remark about the square of odd numbers being odd) implies that b is itself even, i.e. the greatest common factor between a and b is 2. This contradicts the fact that $\frac{a}{b}$ has in fact been reduced to lowest terms.

IS $\sqrt{2}$ AN IRRATIONAL NUMBER?

Proof (Summary of Strategy)

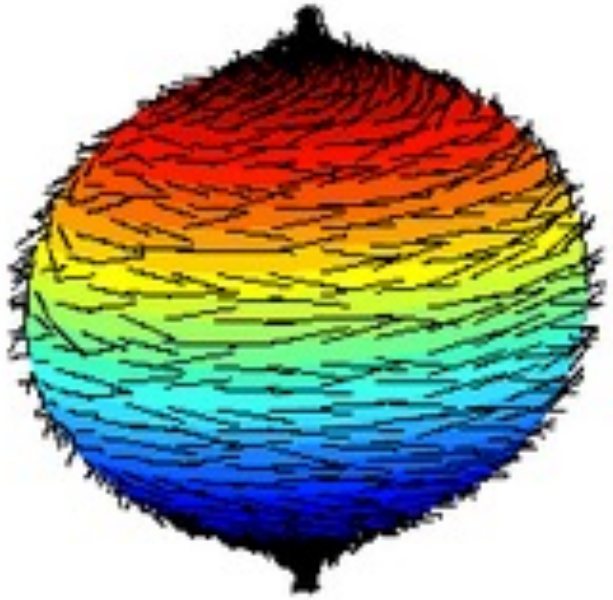
- In sum, we assumed that $\sqrt{2}$ was in fact a rational number, i.e $\sqrt{2} = \frac{a}{b}$ for some integers a, b. We then got a contradiction - in particular, we got that $\frac{a}{b}$ was both reduced to lowest terms (by assumption) and not reduced to lowest terms (by our computation above). Since something cannot be X and not-X at the same time, this means that $\sqrt{2}$ is not a rational number, i.e. it is an irrational number. QED.

HAIRY BALL THEOREM



- Theorem: There is no non-vanishing continuous tangent vector field on even-dimensional n-spheres.
- Layman's terms: "You can't comb a hairy ball flat without creating a cowlick" or "you can't comb the hair on a coconut".
- Intuitively obvious, but how to justify/prove?

HAIRY BALL THEOREM



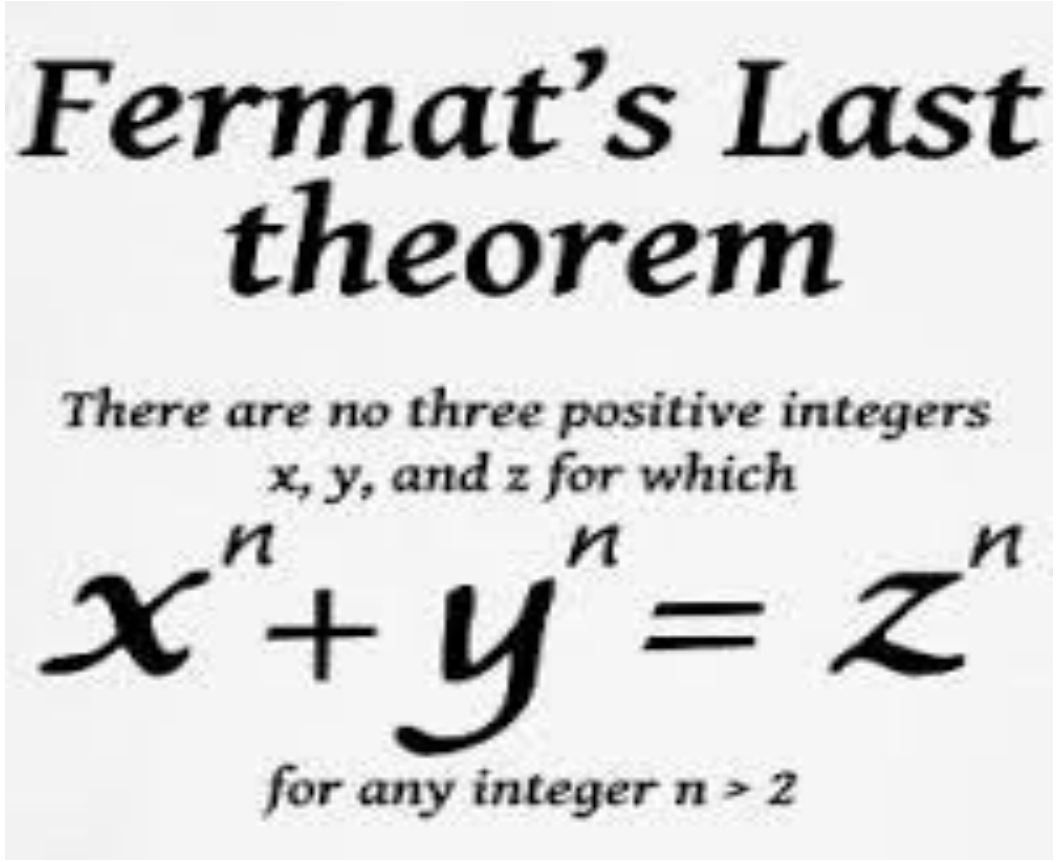
- Theorem: There is no non-vanishing continuous tangent vector field on even-dimensional n-spheres.
- Layman's terms: "You can't comb a hairy ball flat without creating a cowlick" or "you can't comb the hair on a coconut".
- Intuitively obvious, but how to justify/prove?
  - Use Algebraic Topology!

HAIRY BALL THEOREM

- What is Algebraic Topology concerned with?
  - We may view a topological setting as basically a system that contains certain rules how to build "geometric objects".
  - We may then ask: what kind of objects can be built within this system? What kind of phenomena can exist within this system?

- Suppose we want to know if some complicated object X can exist within some topological setting T.
  - If we want to prove that <u>X CAN EXIST IN T</u>, then we construct such an object.
  - If we want to prove that <u>X CANNOT EXIST IN T</u>, then we usually appeal to the "structure" of the topological setting (basically, a set of broad consequences that are the result of the abovementioned rules on how to build objects) and argue how this "structure" prevents X from existing.
- **<u>Algebraic Topology</u>** provides us with a set of analytical tools to say intelligent things about this so-called structure within a sufficiently "nice" topological setting (e.g. homological algebra).

MODULAR FORMS & LEHMER'S CONJECTURE



- Modular forms are a different kind of analytical tools, and are very useful for questions in number theory – in fact, modular forms were instrumental in Andrew Wiles' proof of Fermat's Last Theorem.

- But this prompts even more questions about these tools.
  - E.g. What kind of things are modular forms? How do they behave and relate to each other?

- Answers to many of these questions are often quite difficult – whereas the previous example illustrated the gap between intuition and justification, here intuition (or at least, the untutored intuition) is often of very little help.

MODULAR FORMS & LEHMER'S CONJECTURE

- The modular Discriminant is a famous example of a modular form (more specifically, it is a cusp form of weight 12).

- The Dedekind Eta Function is defined as:

$$\eta(z) = q^{\frac{1}{24}} \prod_{n=1}^{\infty}(1-q^n), \qquad q = e^{2\pi i z}.$$

- The modular discriminant is defined as: $\Delta(z) = \eta(z)^{24}$, which we may write out explicitly as:

$$\Delta(z) = \sum_{n>0} \tau(n) q^n = q \prod_{n>0} (1-q^n)^{24} = q - 24q^2 + 252q^3 - 1472q^4 + 4830q^5 - \cdots,$$

MODULAR FORMS & LEHMER'S CONJECTURE

$$\Delta(z) = \sum_{n>0} \tau(n) q^n = q \prod_{n>0} (1-q^n)^{24} = q - 24q^2 + 252q^3 - 1472q^4 + 4830q^5 - \cdots,$$

- Some Interesting Results

- $\tau(mn) = \tau(m)\tau(n)$ if $gcd(m, n) = 1$
- $|\tau(p) \geq 2p^{11/2}|$ for all primes p
- $\tau(n) \equiv \sigma_{11}(n) \bmod 691$
- $\tau(n) \neq 0$ for all n.

N	reference
3316799	Lehmer (1947)
214928639999	Lehmer (1949)
10^{15}	Serre (1973, p. 98), Serre (1985)
1213229187071998	Jennings (1993)
22689242781695999	Jordan and Kelly (1999)
22798241520242687999	Bosman (2007)
982149821766199295999	Zeng and Yin (2013)
816212624008487344127999	Derickx, van Hoeij, and Zeng (2013)

DTP MODEL OF MATHEMATICS

- A particular caricature of how one might view mathematics (The "Definition-Theorem-Proof (DTP) Model of Mathematics"):

- D. Mathematicians start from a few basic mathematical structures and a collection of axioms "given about these structures"
- T. There are various important questions to be answered about these structures that can be stated as formal mathematical propositions.
- P. The task of the mathematician is to seek a deductive pathway from the axioms to the propositions or to their denials

DTP MODEL OF MATHEMATICS

- "A clear difficulty with the DTP model is that it doesn't explain the source of the questions. Jaffe and Quinn discuss speculation (which they inappropriately label "theoretical mathematics") as an important additional ingredient. Speculation consists of making conjectures, raising questions, and making intelligent guesses and heuristic arguments about what is probably true.
- Jaffe and Quinn's DSTP model still fails to address some basic issues. We are not trying to meet some abstract production quota of definitions, theorems and proofs. The measure of our success is whether what we do enables people to understand and think more clearly and effectively about mathematics"
  - Bill Thurston

- "Any fool can know. The point is to understand." - Einstein

DTP MODEL OF MATHEMATICS

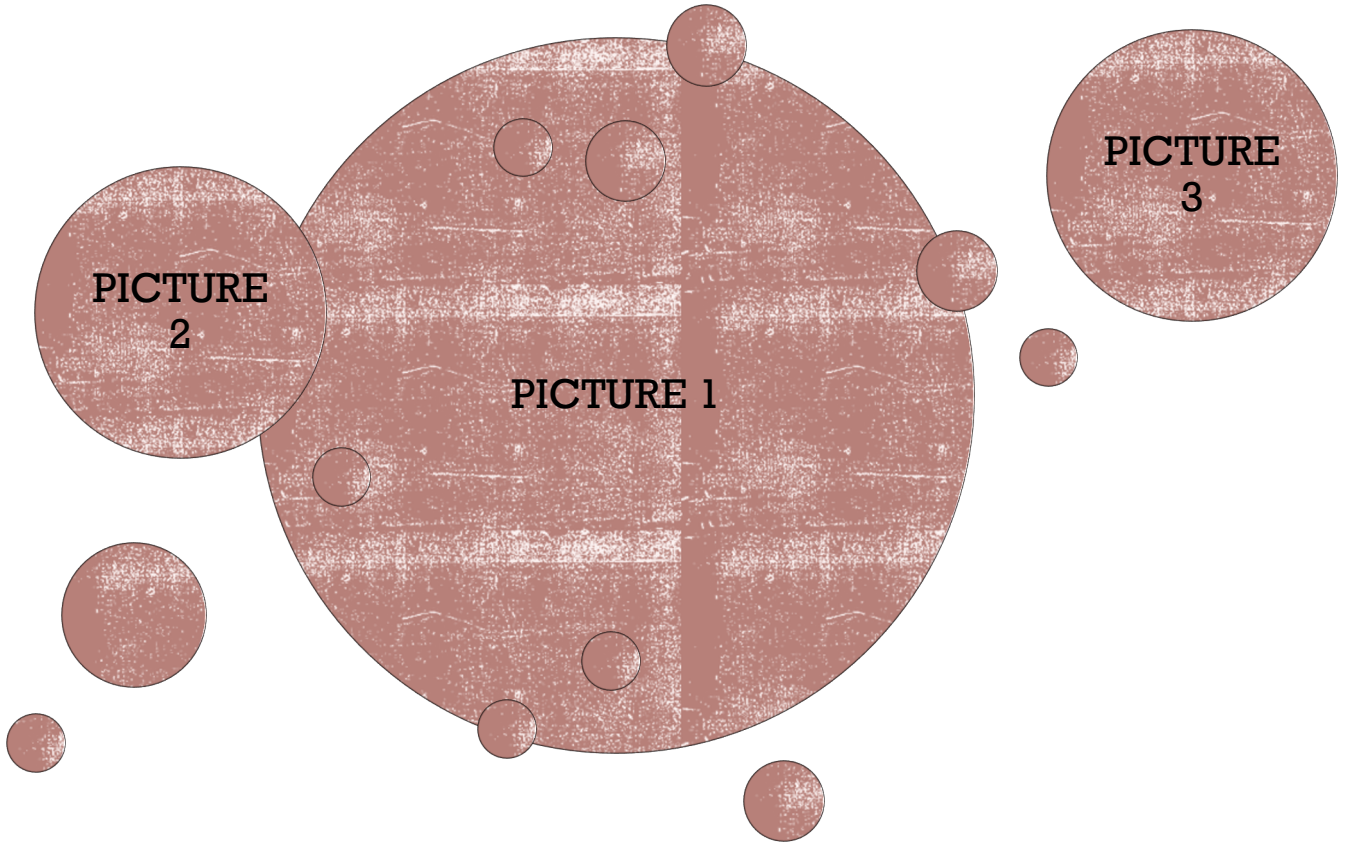
People have very different ways of understanding particular pieces of mathematics. To illustrate this, it is best to take an example that practicing mathematicians understand in multiple ways, but that we see our students struggling with. The derivative of a function fits well. The derivative can be thought of as:

(1) Infinitesimal: the ratio of the infinitesimal change in the value of a function to the infinitesimal change in a function.
(2) Symbolic: the derivative of x^n is nx^{n-1}, the derivative of $\sin(x)$ is $\cos(x)$, the derivative of $f \circ g$ is $f' \circ g * g'$, *etc.*
(3) Logical: $f'(x) = d$ if and only if for every ϵ there is a δ such that when $0 < |\Delta x| < \delta$,

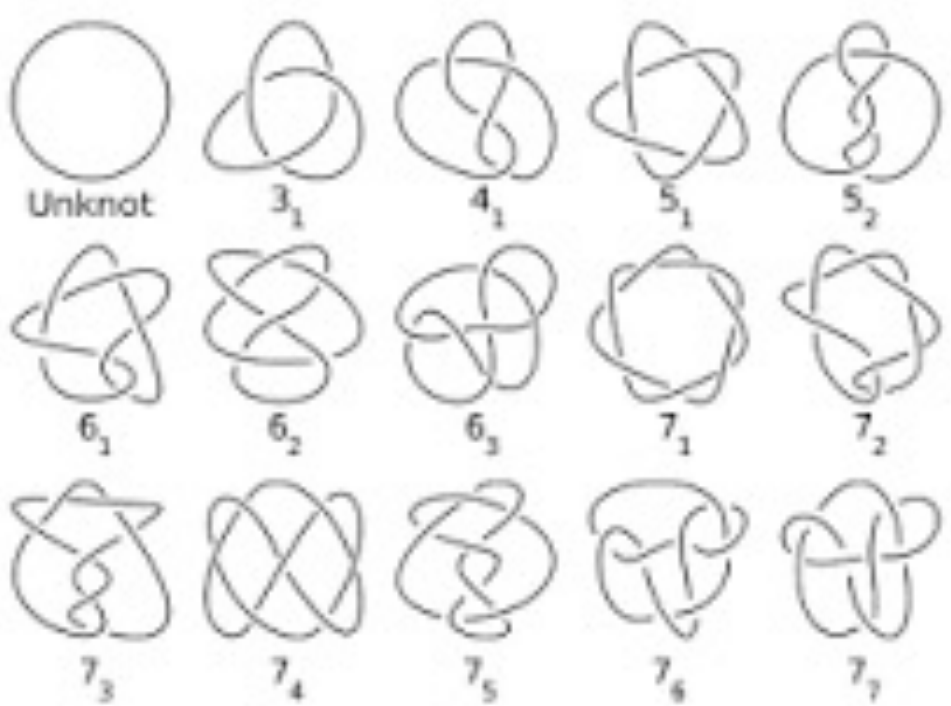
$$\left| \frac{f(x + \Delta x) - f(x)}{\Delta x} - d \right| < \delta.$$

(4) Geometric: the derivative is the slope of a line tangent to the graph of the function, if the graph has a tangent.
(5) Rate: the instantaneous speed of $f(t)$, when t is time.
(6) Approximation: The derivative of a function is the best linear approximation to the function near a point.
(7) Microscopic: The derivative of a function is the limit of what you get by looking at it under a microscope of higher and higher power.

RELATIONS BETWEEN DIFFERENT MATHEMATICAL AREAS/THEORIES

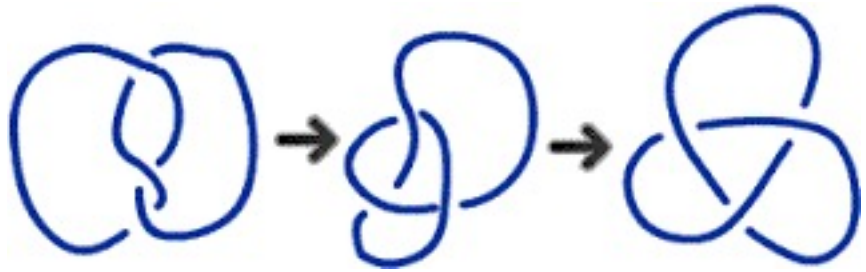


KNOTS & DYNAMICS (INTRO TO KNOTS)



- In **mathematics**, a **knot** is an embedding of a circle in 3-dimensional Euclidean space, R^3 (also known as E^3), considered up to continuous deformations (isotopies)

KNOTS & DYNAMICS (INTRO TO KNOTS)



- In **mathematics**, a **knot** is an embedding of a circle in 3-dimensional Euclidean space, R^3 (also known as E^3), considered up to continuous deformations (isotopies)

- When are two knots equivalent?

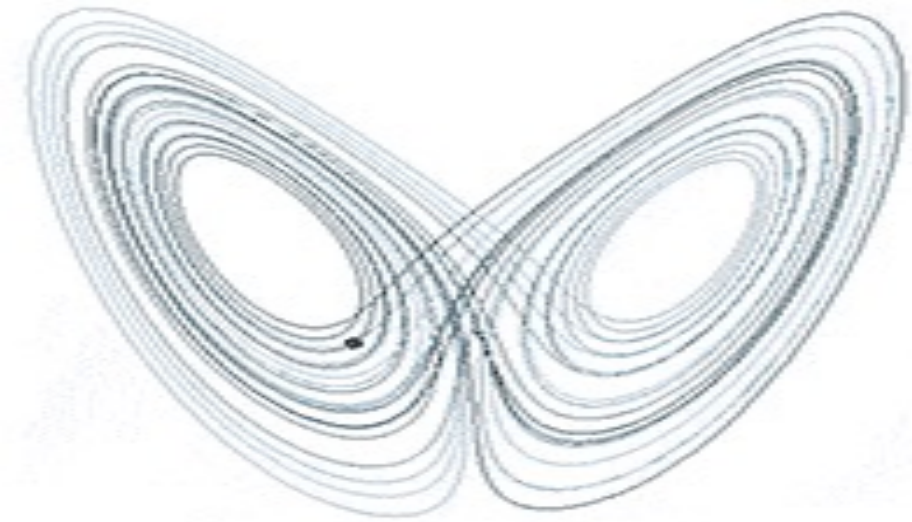
KNOTS & DYNAMICS (LORENZ SYSTEM)

- E. N. Lorenz, Deterministic, non-periodic flows, J. Atmospheric Sciences, 1963. Is weather fundamentally deterministic? Many many variables. Sometimes seems unpredictable. Why? Does deterministic $\Longrightarrow$ ultimately periodic? If so, then weather can't be deterministic.

- Lorenz started off with the Navier-Stokes Equation, which described dynamics of a viscous, incompressible fluid, and simplified it to get the Lorenz system of Ordinary Differential Equations

KNOTS & DYNAMICS (LORENZ SYSTEM)

- Lorenz Attractor



- ODE:

$$\frac{\mathrm{d}x}{\mathrm{d}t} = \sigma(y - x),$$
$$\frac{\mathrm{d}y}{\mathrm{d}t} = x(\rho - z) - y,$$
$$\frac{\mathrm{d}z}{\mathrm{d}t} = xy - \beta z.$$

KNOTS & DYNAMICS (LORENZ KNOTS)

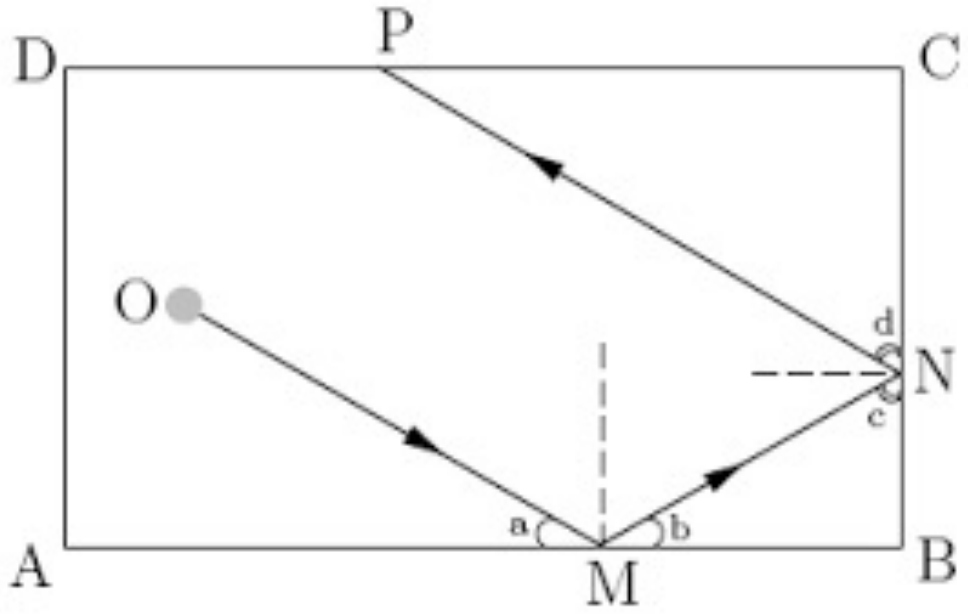
- Analysing periodic orbits of this system of ODEs as knots
  - What kind of mathematical tools do we need in order to do this? (Template Theory – developed by Birman and Williams)
  - What kind of knots occur within this system? What properties do they have?

- The tools of analysing a dynamical system's periodic orbits as knots need not be restricted to Lorenz ODEs and may be applied elsewhere

- Strange connection:
  - A mathematician named Etienne Ghys constructed a dynamical flow using modular forms ("modular flow"), and analysed the resulting periodic orbits as knots ("modular knots").
  - Turns out, the Lorenz Knots & Modular Knots are an identical class of knots!

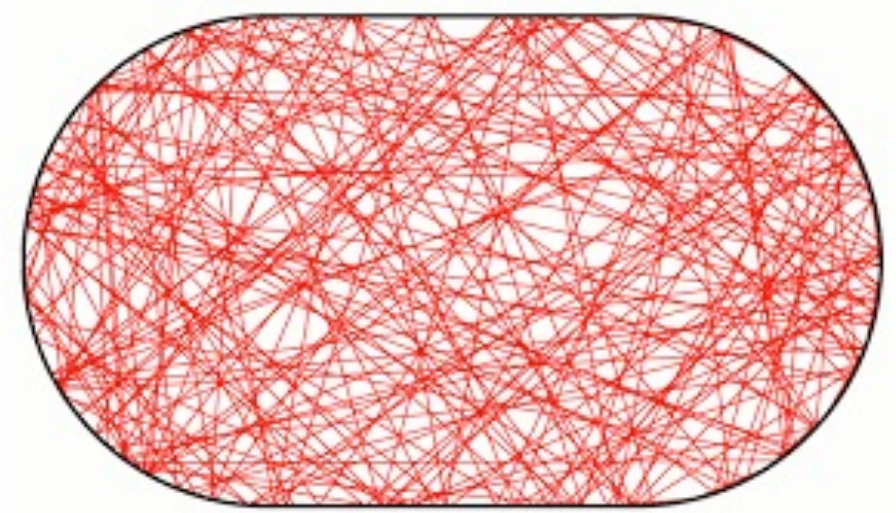
KNOTS & DYNAMICS (BILLIARD DYNAMICS)

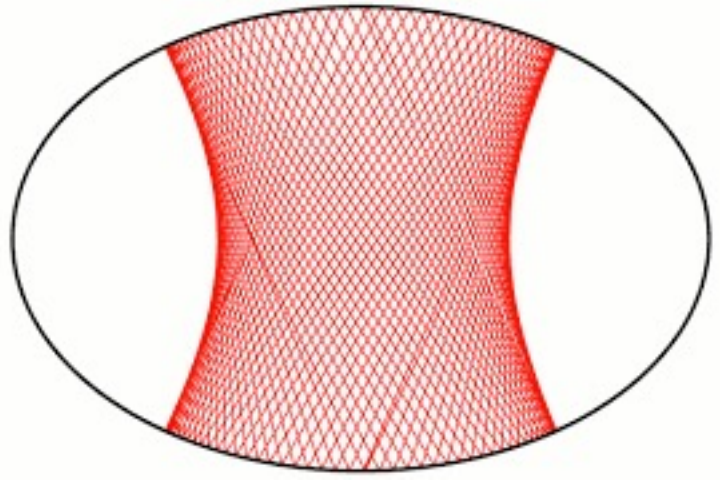
- Billiards is a simple dynamical system, where a ball bounces around a particular space and reflects off the wall in the obvious manner.



KNOTS & DYNAMICS (BILLIARD DYNAMICS)

- Billiards is a simple dynamical system, where a ball bounces around a particular space and reflects off the wall in the obvious manner.
- Questions about the trajectories of billiards tend to be primarily measure-theoretic in flavour.
- But what if we were to approach this from a topological point of view?





UNIFYING THEORY OF MATHEMATICS?

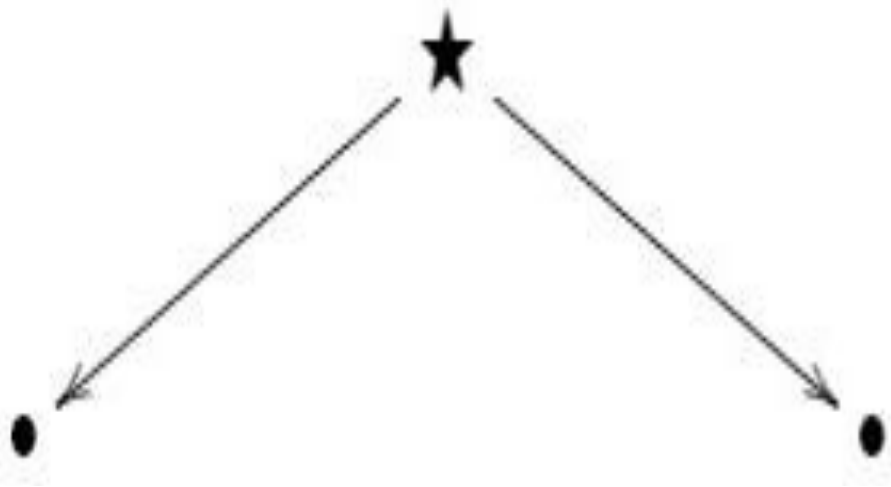
GENERALISING MATHEMATICAL METHODS

- Category Theory (Eillenerg, Mac Lane)
  - "**Category theory** formalizes mathematical structure and its concepts in terms of a collection of objects and of arrows (also called morphisms)."
- Scissors Congruence (Hilbert, Dupont & Sah, Zakharevich)
  - Hilbert's 3rd Question: "Given any two polyhedra of equal volume, is it always possible to cut the first into finitely many polyhedral pieces which can be reassembled to yield the second? "

MODEL THEORY & TOPOS THEORY

- Model Theory:
  - The study of mathematical structures from the perspective of mathematical logic.

- "Static Generalisation"
  - Allows us to regard different concepts as particular cases of a more general one but does not offer by itself a way for transferring information between them



MODEL THEORY & TOPOS THEORY

- Topos Theory

- Dynamical Unification
  - Two distinct objects are related to each other through a third one, which can be associated or **constructed** from each of them separately and which admits two different representations, each of which corresponding to a different method of constructing it.
  - Such an object acts as a '**bridge**' between the two given object in the sense that information can be transferred between the two objects by **translating** properties (resp. constructions) of the bridge object into properties of (resp. constructions on) the two objects, by exploiting the two different representations of the bridge object:

TOPOSES AS MATHEMATICAL "BRIDGES" (CARAMELLO)

- "As the (human) **DNA** embodies the essential features of an individual, so the **classifying topos** embodies the essential features of a mathematical theory.

TOPOSES AS MATHEMATICAL "BRIDGES" (CARAMELLO)

- "As the (human) **DNA** embodies the essential features of an individual, so the **classifying topos** embodies the essential features of a mathematical theory.
- As the DNA can be extracted in many different ways (for example, from different parts of an individual), so the classifying topos can represented and calculated in alternative ways (emphasizing distinct readings of the core of a theory).

TOPOSES AS MATHEMATICAL "BRIDGES" (CARAMELLO)

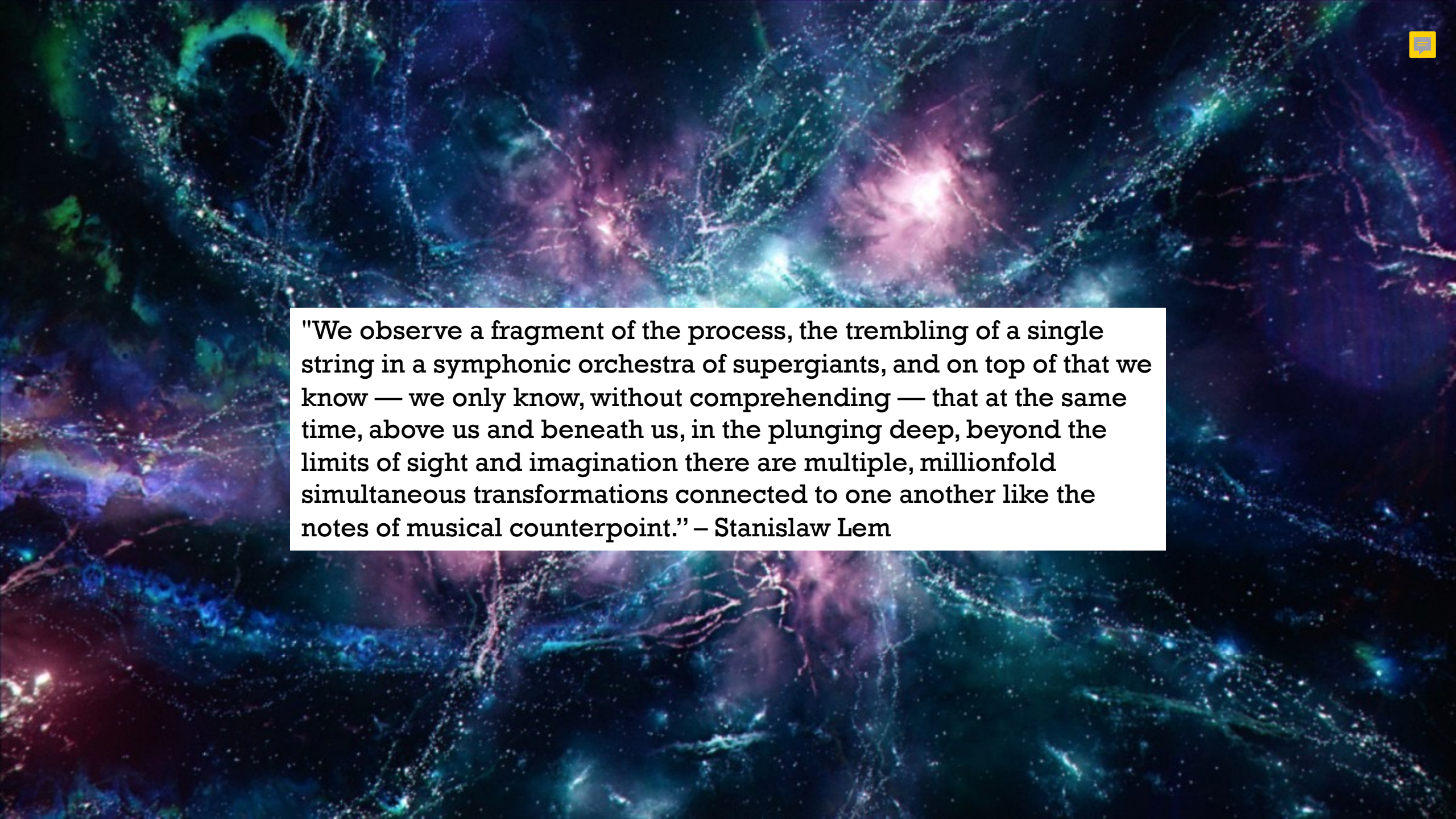
- "As the (human) **DNA** embodies the essential features of an individual, so the **classifying topos** embodies the essential features of a mathematical theory.
- As the DNA can be extracted in many different ways (for example, from different parts of an individual), so the classifying topos can represented and calculated in alternative ways (emphasizing distinct readings of the core of a theory).
- As the DNA is invariant with respect to the particular physical appearance of the individual at a given time (for example, with respect to age), so the classifying topos is invariant with respect to particular presentations of the theory (for example, with respect to a particular axiomatization of it over its signature).

TOPOSES AS MATHEMATICAL "BRIDGES" (CARAMELLO)

- "As the (human) **DNA** embodies the essential features of an individual, so the **classifying topos** embodies the essential features of a mathematical theory.
- As the DNA can be extracted in many different ways (for example, from different parts of an individual), so the classifying topos can represented and calculated in alternative ways (emphasizing distinct readings of the core of a theory).
- As the DNA is invariant with respect to the particular physical appearance of the individual at a given time (for example, with respect to age), so the classifying topos is invariant with respect to particular presentations of the theory (for example, with respect to a particular axiomatization of it over its signature).
- As the DNA of an individual can be studied by using appropriate techniques, which are not those of traditional Medicine, so classifying toposes can be studied by using peculiar methods (i.e. those of Topos Theory) which, although being entirely mathematical, differ from those of classical Mathematics.
- As in Genetics one studies how modifications of the DNA influence the characteristics of an individual, similarly in Topos Theory one can study the effect that topos-theoretic operations on toposes have on the theories classified by them.

TOPOSES AS MATHEMATICAL "BRIDGES" (CARAMELLO)

- "As the (human) **DNA** embodies the essential features of an individual, so the **classifying topos** embodies the essential features of a mathematical theory.
- As the DNA can be extracted in many different ways (for example, from different parts of an individual), so the classifying topos can represented and calculated in alternative ways (emphasizing distinct readings of the core of a theory).
- As the DNA is invariant with respect to the particular physical appearance of the individual at a given time (for example, with respect to age), so the classifying topos is invariant with respect to particular presentations of the theory (for example, with respect to a particular axiomatization of it over its signature).
- As the DNA of an individual can be studied by using appropriate techniques, which are not those of traditional Medicine, so classifying toposes can be studied by using peculiar methods (i.e. those of Topos Theory) which, although being entirely mathematical, differ from those of classical Mathematics.
- As in Genetics one studies how modifications of the DNA influence the characteristics of an individual, similarly in Topos Theory one can study the effect that topos-theoretic operations on toposes have on the theories classified by them.
- As the role of the DNA is that of a unifying concept enabling us to compare individuals with each other, point out differences and discover similarities, so the notion of classifying topos is a unifying one, enabling us to compare distinct mathematical theories with each other and transfer knowledge between them." - Caramello


"We observe a fragment of the process, the trembling of a single string in a symphonic orchestra of supergiants, and on top of that we know — we only know, without comprehending — that at the same time, above us and beneath us, in the plunging deep, beyond the limits of sight and imagination there are multiple, millionfold simultaneous transformations connected to one another like the notes of musical counterpoint." – Stanislaw Lem