THE MATHEMATICAL TRUTH

Enrico Bombieri
IAS, Princeton

THE MATHEMATICAL TRUTH

Enrico Bombieri
IAS, Princeton

For angling may be said to be so like the mathematics, that it can never be fully learnt; at least not so fully, but that there will still be more new experiments left for the trial of other men that succeed us.

Izaak Walton, ***The Compleat Angler,*** To the Reader of this Discourse.

WHAT IS MATHEMATICAL TRUTH?

WHAT IS MATHEMATICAL TRUTH?

1) An absolute.

WHAT IS MATHEMATICAL TRUTH?

1) An absolute.

2) A relative notion.

WHAT IS MATHEMATICAL TRUTH?

1) An absolute.

2) A relative notion.

3) A tautology.

WHAT IS MATHEMATICAL TRUTH?

1) An absolute.

2) A relative notion.

3) A tautology.

4) Does not exist.

WHAT IS MATHEMATICAL TRUTH?

1) An absolute.

2) A relative notion.

3) A tautology.

4) Does not exist.

5) A product of culture.

Platonic Realism: The view that numbers, geometry, hence mathematics, exist in the platonic world of ideas as absolutes.

Plentiful Platonism: It allows for the existence of an objective set of distinct mathematics.

Platonic Realism: The view that numbers, geometry, hence mathematics, exist in the platonic world of ideas as absolutes.

Plentiful Platonism: It allows for the existence of an objective set of distinct mathematics.

Formalism: The view that mathematics is only a construction of the mind (or the collective mind).

The role of the mathematician is analogous to that of an architect, rather than of an explorer. One has different types of mathematics according to which constructions and rules are allowed.

A serious difficulty: Freewheeling infinite constructions quickly lead to antinomies and paradoxes, as in early models of set theory.

Platonic Realism: The view that numbers, geometry, hence mathematics, exist in the platonic world of ideas as absolutes.

Plentiful Platonism: It allows for the existence of an objective set of distinct mathematics.

Formalism: The view that mathematics is only a construction of the mind (or the collective mind).

The role of the mathematician is analogous to that of an architect, rather than of an explorer. One has different types of mathematics according to which constructions and rules are allowed.

A serious difficulty: Freewheeling infinite constructions quickly lead to antinomies and paradoxes, as in early models of set theory.

Russell's Paradox: The impossible ***set*** R ***of all sets*** S ***with the property that*** S ***is not an element of*** S***.***

Brouwer's Intuitionism: Everything in mathematics must be 'effectively' defined. Mathematical entities do not exist until they have been constructed.

John Stuart Mill's Empiricism: Mathematics is the result of empirical research, which puts mathematics on a par with other sciences.

Lakatos's Quasi-empiricism (Post-modernism): It questions the validity of mathematics as a whole, based on the assertion that no foundation of mathematics can be proved to exist.

Social Constructivism and Social Realism: Mathematics is only a product of culture, subject to change. It does not exist until it has been thought out. Social realism presents a postmodernist view: Mathematics is shaped by the fashions of the social group doing it.

Hartry Field's Fictionalism: Mathematics is meaningless in absolute. It is at best a useful fiction.

Applied mathematics: The subject of study has its roots in the description of reality.

Applied mathematics: The subject of study has its roots in the description of reality.

However, it is very hard to describe actual phenomena by simple mathematical models. Finding good mathematical models may be more difficult than the actual mathematics needed to study them.

Applied mathematics: The subject of study has its roots in the description of reality.

However, it is very hard to describe actual phenomena by simple mathematical models. Finding good mathematical models may be more difficult than the actual mathematics needed to study them.

Hardy, in his well-known short essay *"A Mathematician's Apology"* puts it bluntly in these terms: "most of the finest products of an applied mathematician's fancy must be rejected, as soon as they have been created, by the brutal but sufficient reason that they do not fit the facts."

Applied mathematics: The subject of study has its roots in the description of reality.

However, it is very hard to describe actual phenomena by simple mathematical models. Finding good mathematical models may be more difficult than the actual mathematics needed to study them.

Hardy, in his well-known short essay *"A Mathematician's Apology"* puts it bluntly in these terms: "most of the finest products of an applied mathematician's fancy must be rejected, as soon as they have been created, by the brutal but sufficient reason that they do not fit the facts."

As an example, sophisticated mathematical models of investment finance have turned out to be grossly insufficient to take into account the distinction between real wealth and paper profits.

Most mathematicians agree with the platonic view, but work in the formalistic way. They are platonists on Sundays but formalists on week days.

Most mathematicians also believe that the mathematical objects are not just formulas, propositions, or theorems.

Most mathematicians agree with the platonic view, but work in the formalistic way. They are platonists on Sundays but formalists on week days.

Most mathematicians also believe that the mathematical objects are not just formulas, propositions, or theorems.

Hardy's view: "A mathematician, like a painter or poet, is a maker of patterns. If his patterns are more permanent than theirs, it is because they are made with ideas."

Most mathematicians agree with the platonic view, but work in the formalistic way. They are platonists on Sundays but formalists on week days.

Most mathematicians also believe that the mathematical objects are not just formulas, propositions, or theorems.

Hardy's view: "A mathematician, like a painter or poet, is a maker of patterns. If his patterns are more permanent than theirs, it is because they are made with ideas."

My own view: Mathematics is the science of relations. What matters is the relation between objects, not the objects themselves. Very different objects can share the same relation. Patterns are aspects of relations and, sometimes, can be identified with relations.

RATIONAL TRUTH

The School of Athens by Raphael

Aristotle and Plato in the center, Euclid in the lower right corner

MATHEMATICAL TRUTH

The School of Athens by Raphael
Detail of Euclid with his students

QUESTIONS ABOUT MATHEMATICS AND TRUTH

- Is classical mathematics free from contradiction?
- Does mathematics deal with truth?
- Is truth identifiable with verification (i.e. proof)?
- Can truth, or proof, be achieved by consensus?
- Is there a mathematical notion of ‘probable truth’?
- Is automatic verification (i.e by computer) acceptable in mathematics?

TRUTH IN FORMALISTIC MATHEMATICS

Hilbert proposed a program to obtain a complete axiomatization of mathematics and proof of its consistency, starting from the assumption of the consistency of a small number of intuitive basic axioms. Hilbert's program in its original form was brought to a sudden halt by Gödel second incompleteness theorem: ***Any sufficiently large model of mathematics cannot prove its consistency within itself.***

TRUTH IN FORMALISTIC MATHEMATICS

Hilbert proposed a program to obtain a complete axiomatization of mathematics and proof of its consistency, starting from the assumption of the consistency of a small number of intuitive basic axioms. Hilbert's program in its original form was brought to a sudden halt by Gödel second incompleteness theorem: ***Any sufficiently large model of mathematics cannot prove its consistency within itself.***

The formalization of mathematics continued quite successfully with the Bourbaki group with the axiomatization of large parts of algebra, analysis, and geometry. Unfortunately, Bourbaki's ideology excluded entire sectors of mathematics from its program.

TRUTH IN FORMALISTIC MATHEMATICS

Hilbert proposed a program to obtain a complete axiomatization of mathematics and proof of its consistency, starting from the assumption of the consistency of a small number of intuitive basic axioms. Hilbert's program in its original form was brought to a sudden halt by Gödel second incompleteness theorem: ***Any sufficiently large model of mathematics cannot prove its consistency within itself.***

The formalization of mathematics continued quite successfully with the Bourbaki group with the axiomatization of large parts of algebra, analysis, and geometry. Unfortunately, Bourbaki's ideology excluded entire sectors of mathematics from its program.

Truth in formalistic mathematics is not an absolute about a Platonic absolute in an absolute world of ideas. However, the formalization of truth in a suitable formalistic model of mathematics is possible, as shown by Alfred Tarski in a famous paper.

TARSKI's SOLUTION, I

At the basis of the difficulty of defining truth in a system with the classical axiom $(A \vee \neg A)$ of the excluded middle (either A is true or the negation of A is true) is the well-known *liar's paradox*, embodied in the sentence

'This sentence is false'

TARSKI's SOLUTION, I

At the basis of the difficulty of defining truth in a system with the classical axiom $(A \vee \neg A)$ of the excluded middle (either A is true or the negation of A is true) is the well-known *liar's paradox*, embodied in the sentence

'This sentence is false'

Tarski's solution of the problem of truth is exemplified by his famous phrase (translated in English from German)

'Snow is white' is true if and only if snow is white

Here the first 'Snow is white' is a sentence, the second 'snow is white' is a proposition. The distinction is a subtle one.

TARSKI's SOLUTION, II

For Tarski, the definition of truth in a language L (i.e. an alphabet and a collection of words and phrases according to a certain syntax) must be given in another language, the *metalanguage* ML. The metalanguage ML should contain a copy of L and should be able to talk about the sentences and the syntax of L. Also ML should contain a predicate symbol $True$ where $True(x)$ means x is a true sentence of L. A definition of $True$ should be a sentence of the form

For all x, $True(x)$ if and only if $\varphi(x)$

where $True$ never occurs in φ. The equivalence 'if and only if' must be provable using axioms of ML that do not contain $True$. Of course, one wants to be able to say that, in an adequate definition of truth, intuitive truths become truths. This is *convention* T.

TARSKI's SOLUTION, III

If the language L is big enough to talk about its own semantics, convention T makes the liar paradox inevitable. To avoid this problem it is essential that the metalanguage ML should be much larger than L. Tarski then shows that there is a single formula φ in ML which defines $True$ in L. For a language containing the standard $\neg$ ("not"), $\wedge$ ("and"), $\vee$ ("or"), and quantifiers $\forall$ ("for all") and $\exists$ ("there exists") the following intuitive truths must hold:

- $\neg A$ **is true if and only if** A **is not true.**
- $A \wedge B$ **is true if and only if** A **is true and** B **is true.**
- $A \vee B$ **is true if and only if** A **is true or** B **is true.**
- $\forall x\, A(x)$ **is true if and only if each object** x **satisfies** $A(x)$**.**
- $\exists x\, A(x)$ **is true if and only if there is an object** x **satisfying** $A(x)$**.**

TARSKI's SOLUTION, IV

The advantage of Tarski's definition is that truth in a language L can be formally defined in a more ample language ML containing L, but truth cannot be defined inside L itself.

For the working mathematician, Tarski's notion of truth, taking for L the mathematics with the Zermelo–Fraenkel axioms and L within the metalanguage of plain English (with some caveats), is indeed a satisfactory solution that allows him to continue to explore or create new relations and new patterns of significant mathematics.

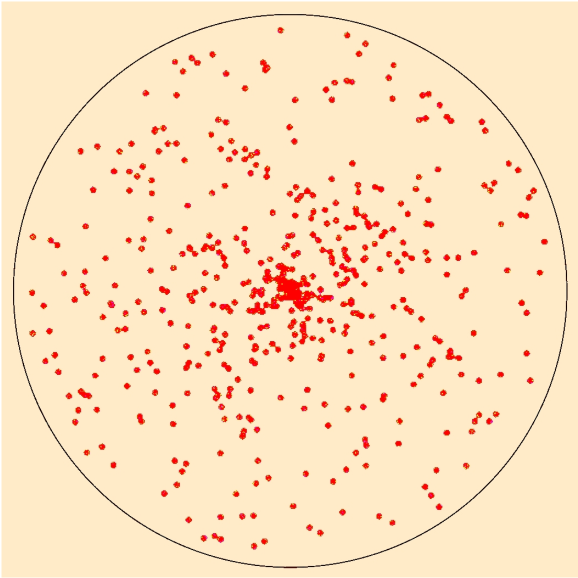
TARSKI's SOLUTION, IV

The advantage of Tarski's definition is that truth in a language L can be formally defined in a more ample language ML containing L, but truth cannot be defined inside L itself.

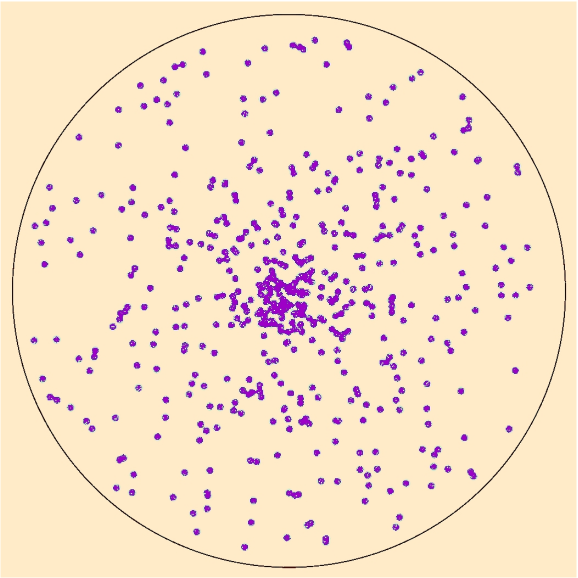
For the working mathematician, Tarski's notion of truth, taking for L the mathematics with the Zermelo–Fraenkel axioms and L within the metalanguage of plain English (with some caveats), is indeed a satisfactory solution that allows him to continue to explore or create new relations and new patterns of significant mathematics.

A question: Is then the Continuum Hypothesis true or false?

TARSKI's SOLUTION: AN INTUITIVE EXPLANATION

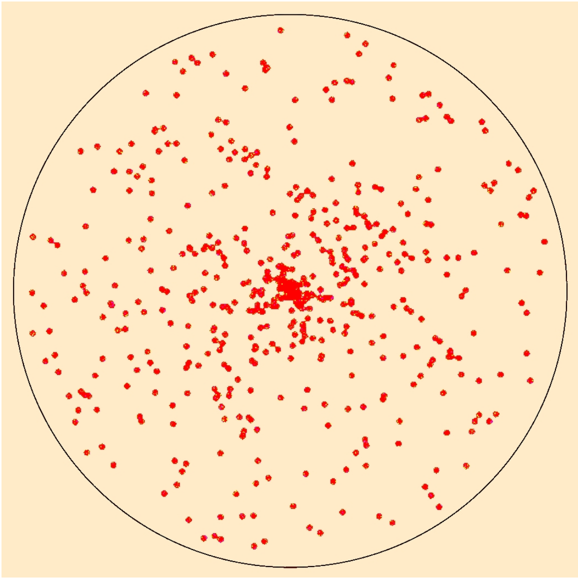


The true in ML

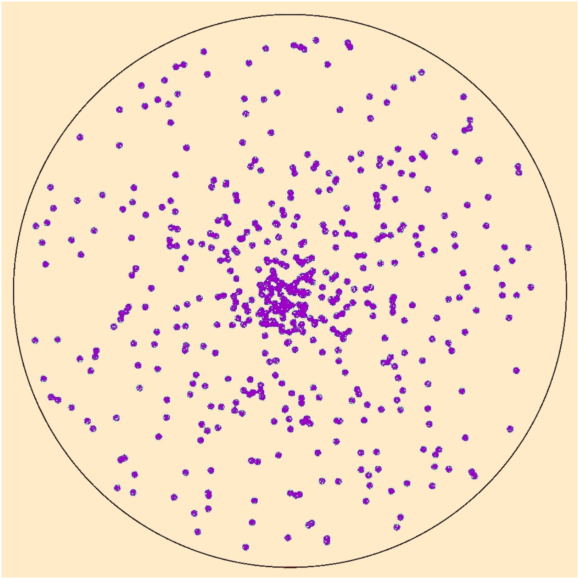


The false in ML

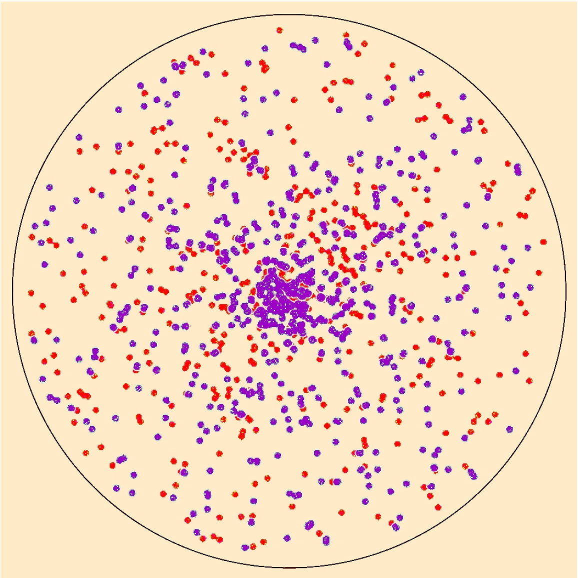
TARSKI's SOLUTION: AN INTUITIVE EXPLANATION



The true in ML

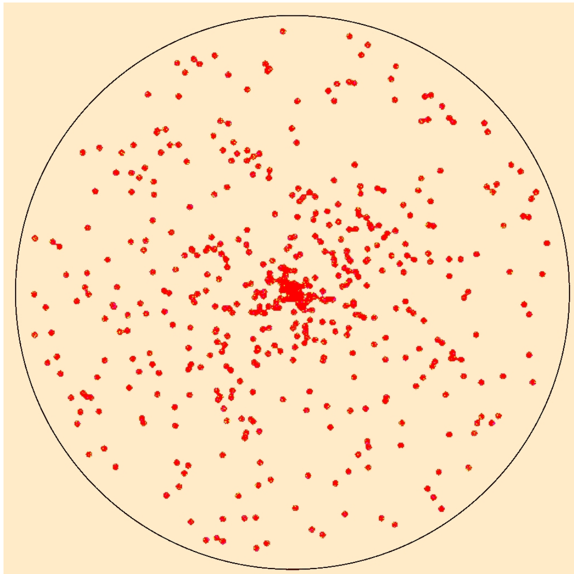


The false in ML

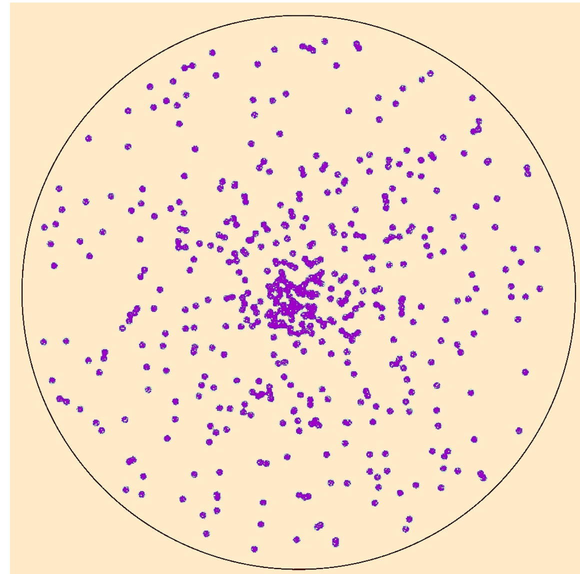


True and false overlap in ML

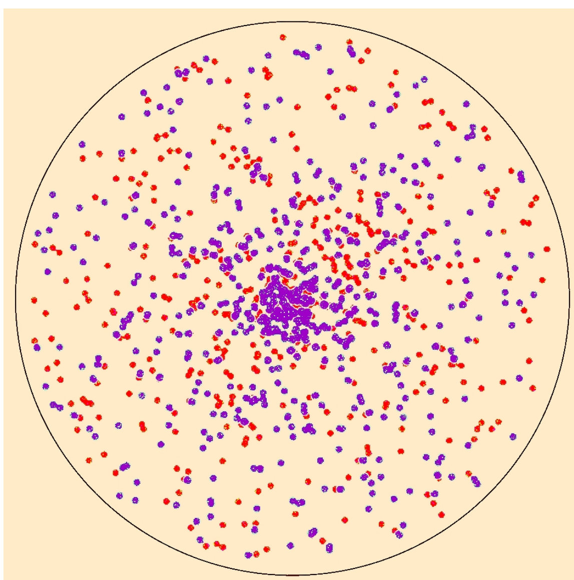
TARSKI's SOLUTION: AN INTUITIVE EXPLANATION



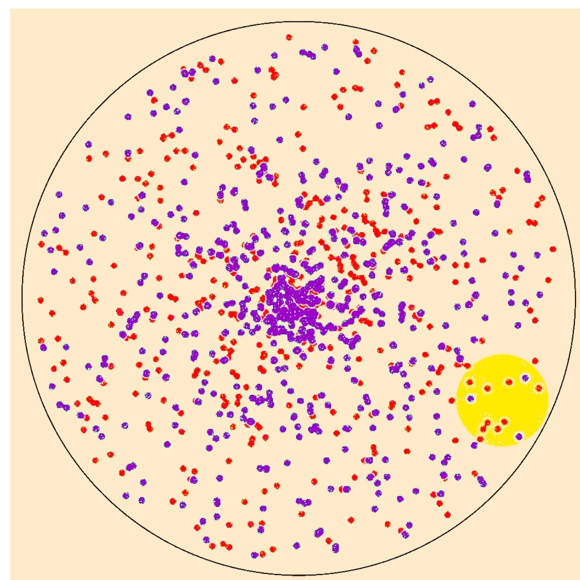
The true in ML



The false in ML



True and false overlap in ML



No overlaps in the yellow L

THE CONTINUUM

The simplest infinity $\aleph_0$ is the infinity of counting, i.e. the cardinality of the set of all natural integers.

THE CONTINUUM

The simplest infinity $\aleph_0$ is the infinity of counting, i.e. the cardinality of the set of all natural integers.

The continuum c is the cardinality of the set of all real numbers.

THE CONTINUUM

The simplest infinity $\aleph_0$ is the infinity of counting, i.e. the cardinality of the set of all natural integers.

The continuum c is the cardinality of the set of all real numbers.

Cantor showed that it is the same as the cardinality of the set of all subsets of the natural integers, denoted by $2^{\aleph_0}$:

$$c = 2^{\aleph_0}.$$

THE CONTINUUM IS UNCOUNTABLE

Suppose it is countable in an infinite list:

$$
\begin{array}{l}
0.643546675432534645600112\ldots \\
0.100053453647545546043860\ldots \\
0.000000000000100004534237\ldots \\
0.999999999961045674732017\ldots \\
0.222955600333054564501179\ldots \\
0.141592653589793238462643\ldots \\
0.777777777777777777777777\ldots \\
0.421047542507075505555001\ldots \\
0.777777771777777777777777\ldots \\
0.777777777177777777777777\ldots \\
0.010010001000010000010000\ldots \\
0.099999999999999900000000\ldots \\
\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots
\end{array}
$$

THE CONTINUUM IS UNCOUNTABLE

Suppose it is countable in an infinite list:

$$
\begin{array}{l}
0.643546675432534645600112\ldots \\
0.100053453647545546043860\ldots \\
0.000000000000100004534237\ldots \\
0.999999999961045674732017\ldots \\
0.222955600333054564501179\ldots \\
0.141592653589793238462643\ldots \\
0.777777777777777777777777\ldots \\
0.421047542507075505555001\ldots \\
0.777777771777777777777777\ldots \\
0.777777777177777777777777\ldots \\
0.010010001000010000010000\ldots \\
0.099999999999999000000000\ldots \\
\text{.......................................}
\end{array}
$$

Diagonal marker: $0.600952741109\ldots$ **(nth digit of nth number)**

THE CONTINUUM IS UNCOUNTABLE

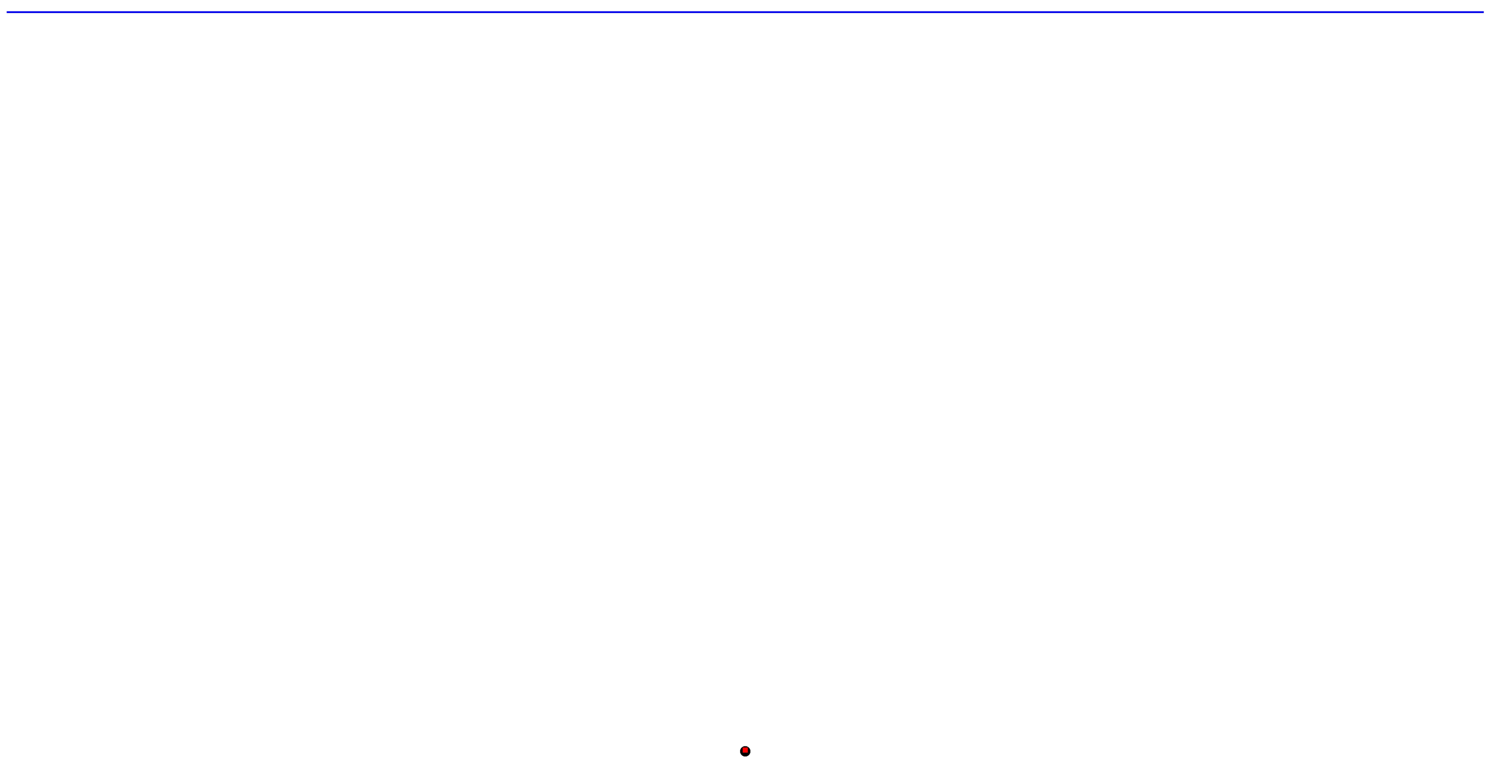
Suppose it is countable in an infinite list:

$$
\begin{array}{l}
0.643546675432534645600112\ldots \\
0.100053453647545546043860\ldots \\
0.000000000000100004534237\ldots \\
0.999999999961045674732017\ldots \\
0.222955600333054564501179\ldots \\
0.141592653589793238462643\ldots \\
0.777777777777777777777777\ldots \\
0.421047542507075505555001\ldots \\
0.777777771777777777777777\ldots \\
0.777777777177777777777777\ldots \\
0.010010001000010000010000\ldots \\
0.099999999999999900000000\ldots \\
\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots
\end{array}
$$

Diagonal marker: $0.600952741109\ldots$ **(**n**th digit of** n**th number)**

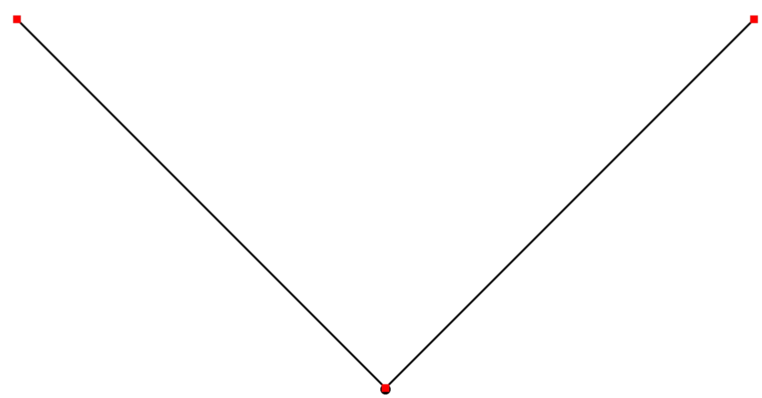
The number $0.711063852210\ldots$ **is not in the above list.**

A PICTURE OF THE CONTINUUM



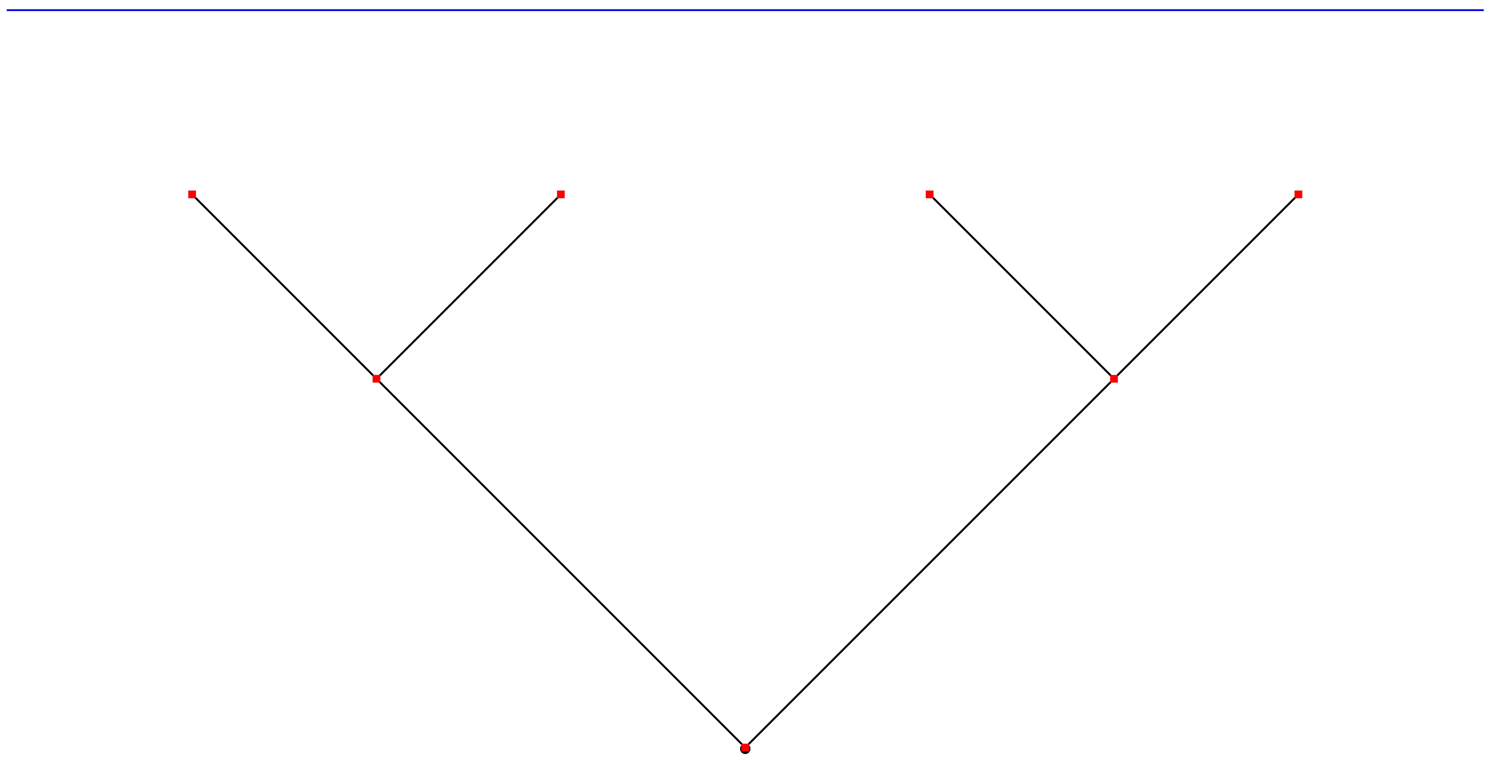
A binary tree. Level 0.

A PICTURE OF THE CONTINUUM



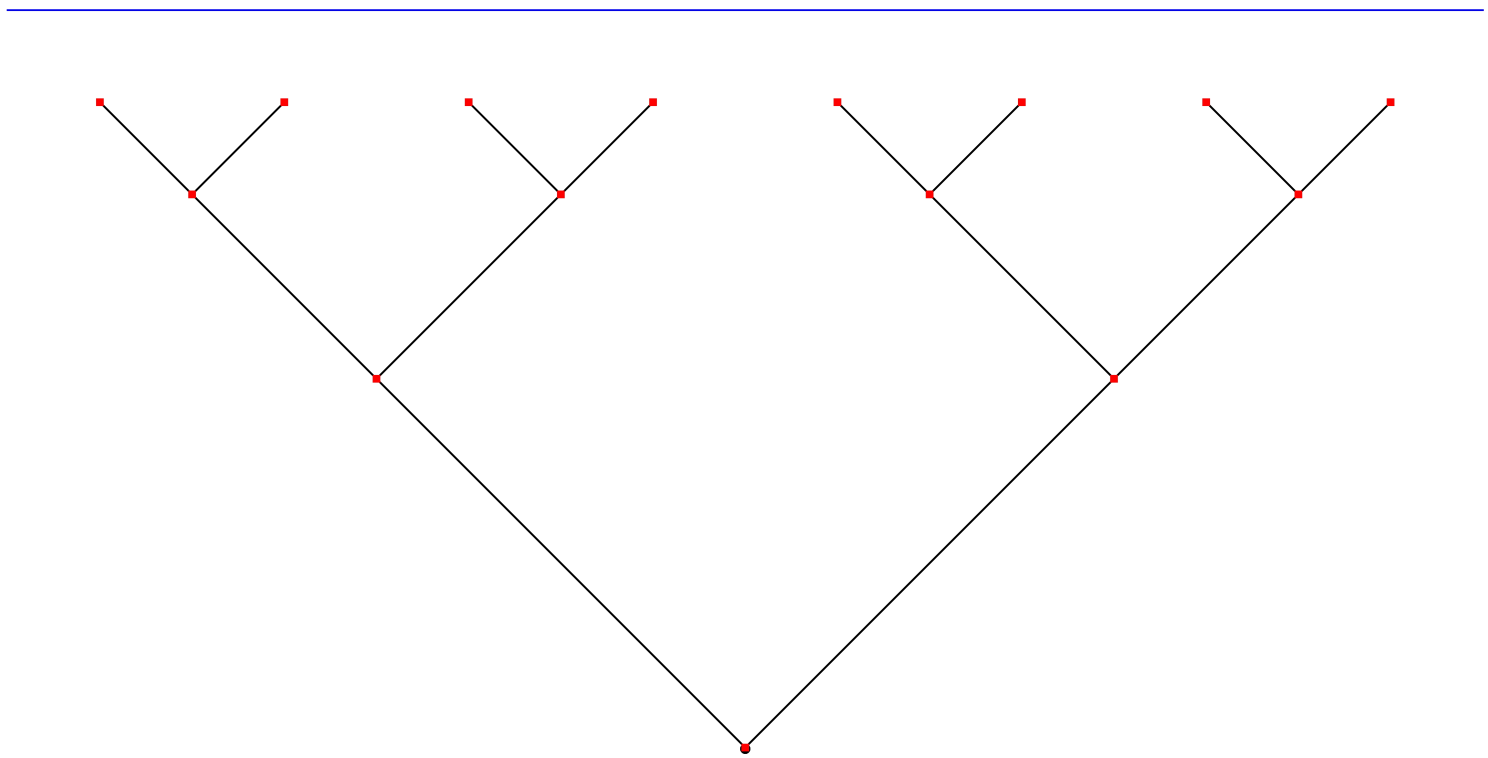
A binary tree. Level 1.

A PICTURE OF THE CONTINUUM



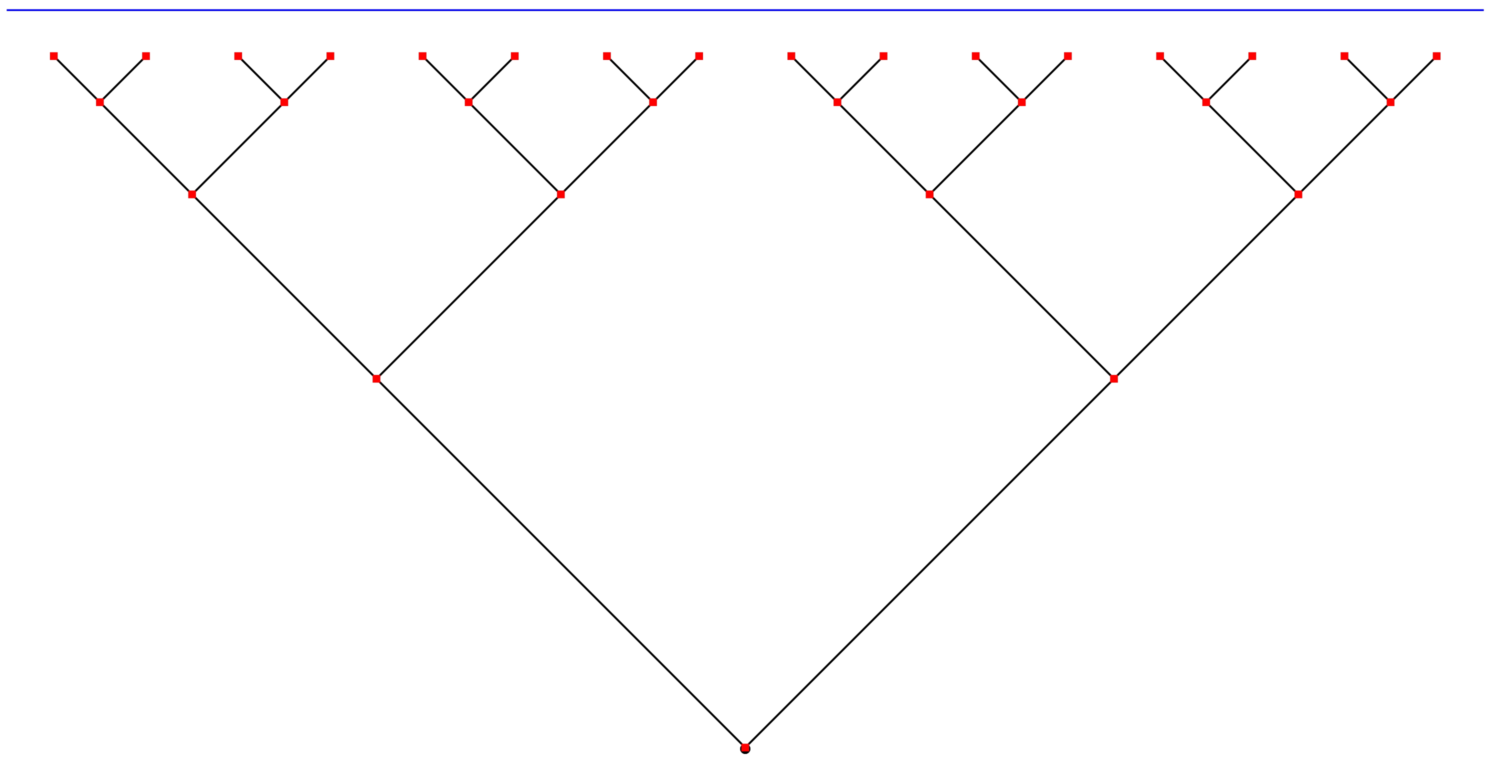
A binary tree. Level 2.

A PICTURE OF THE CONTINUUM



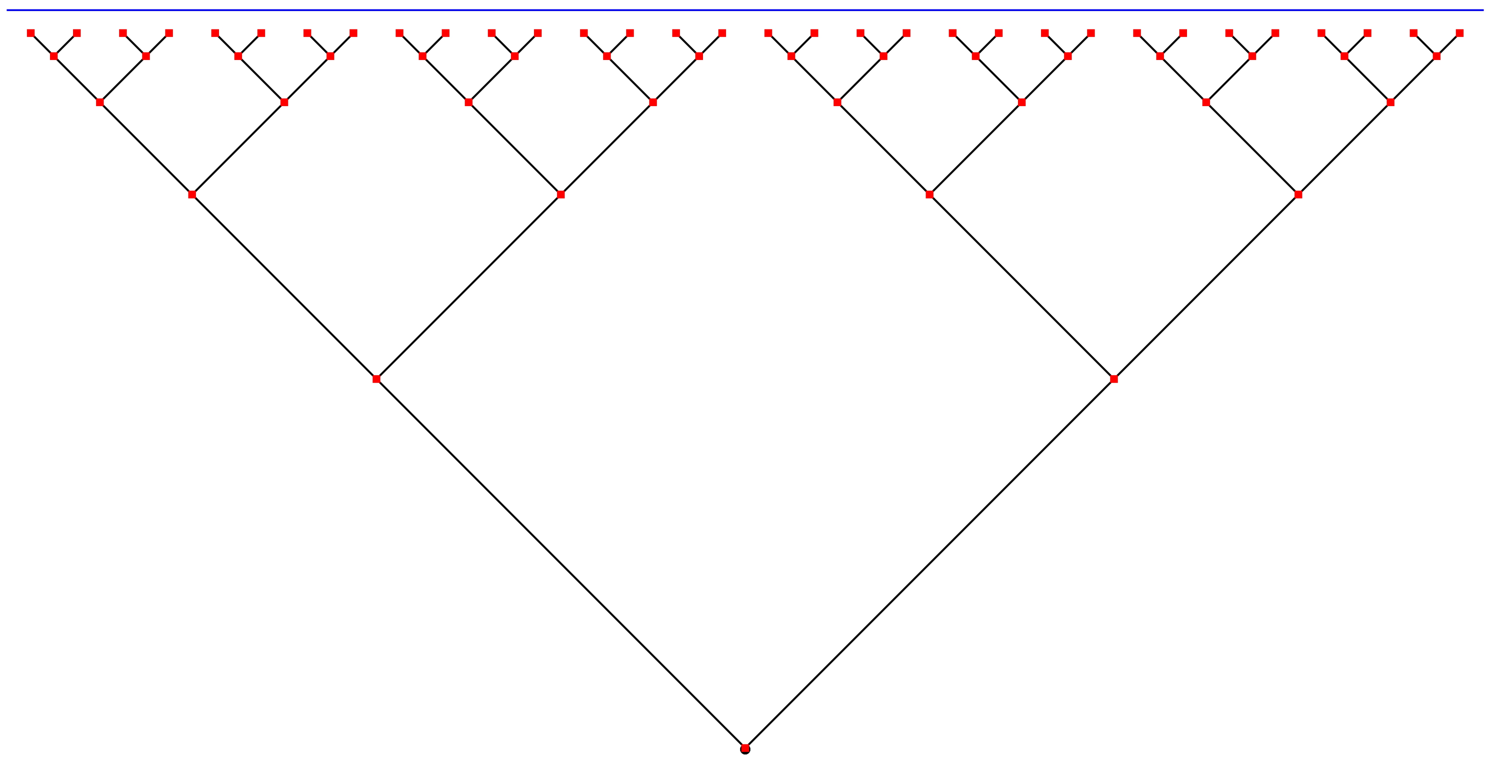
A binary tree. Level 3.

A PICTURE OF THE CONTINUUM



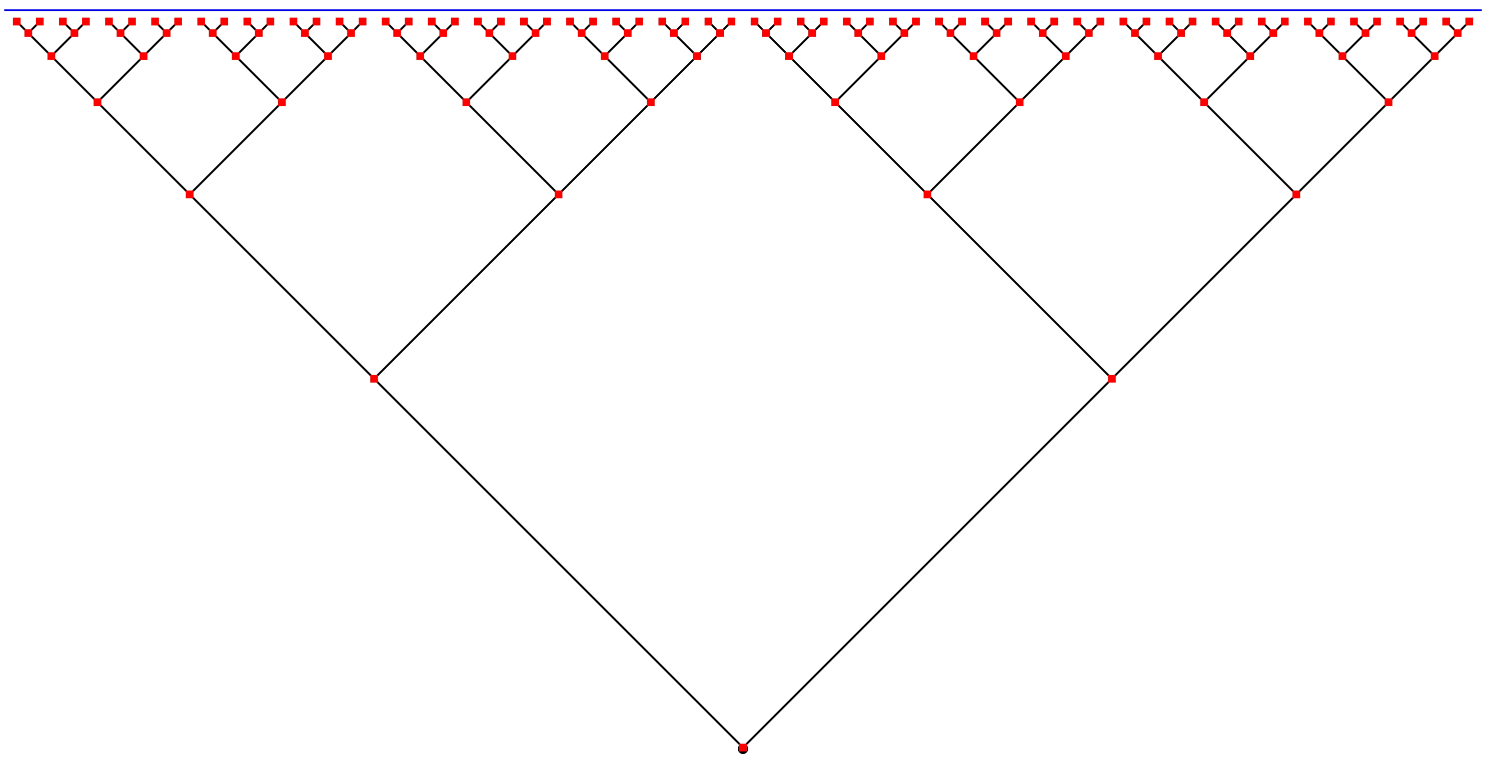
A binary tree. Level 4.

A PICTURE OF THE CONTINUUM



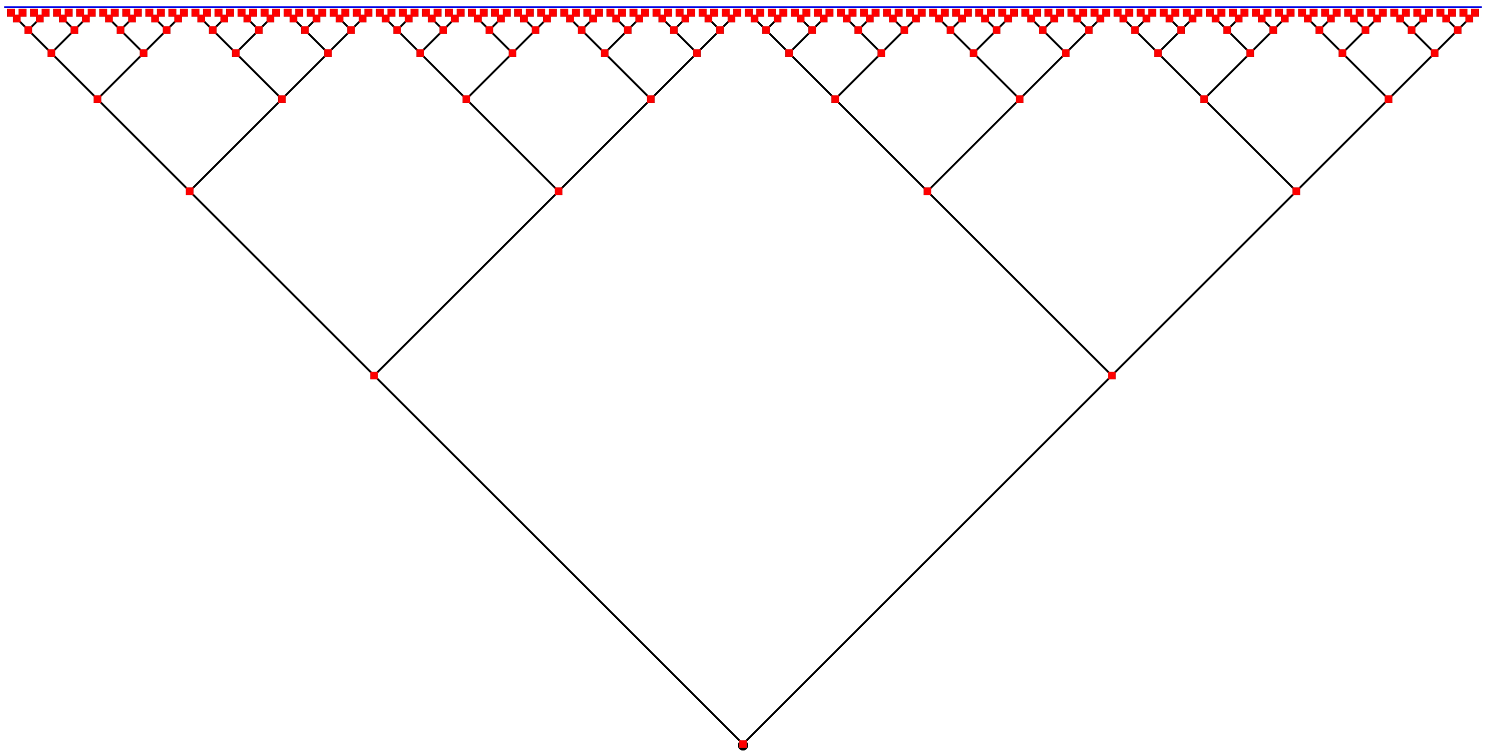
A binary tree. Level 5.

A PICTURE OF THE CONTINUUM



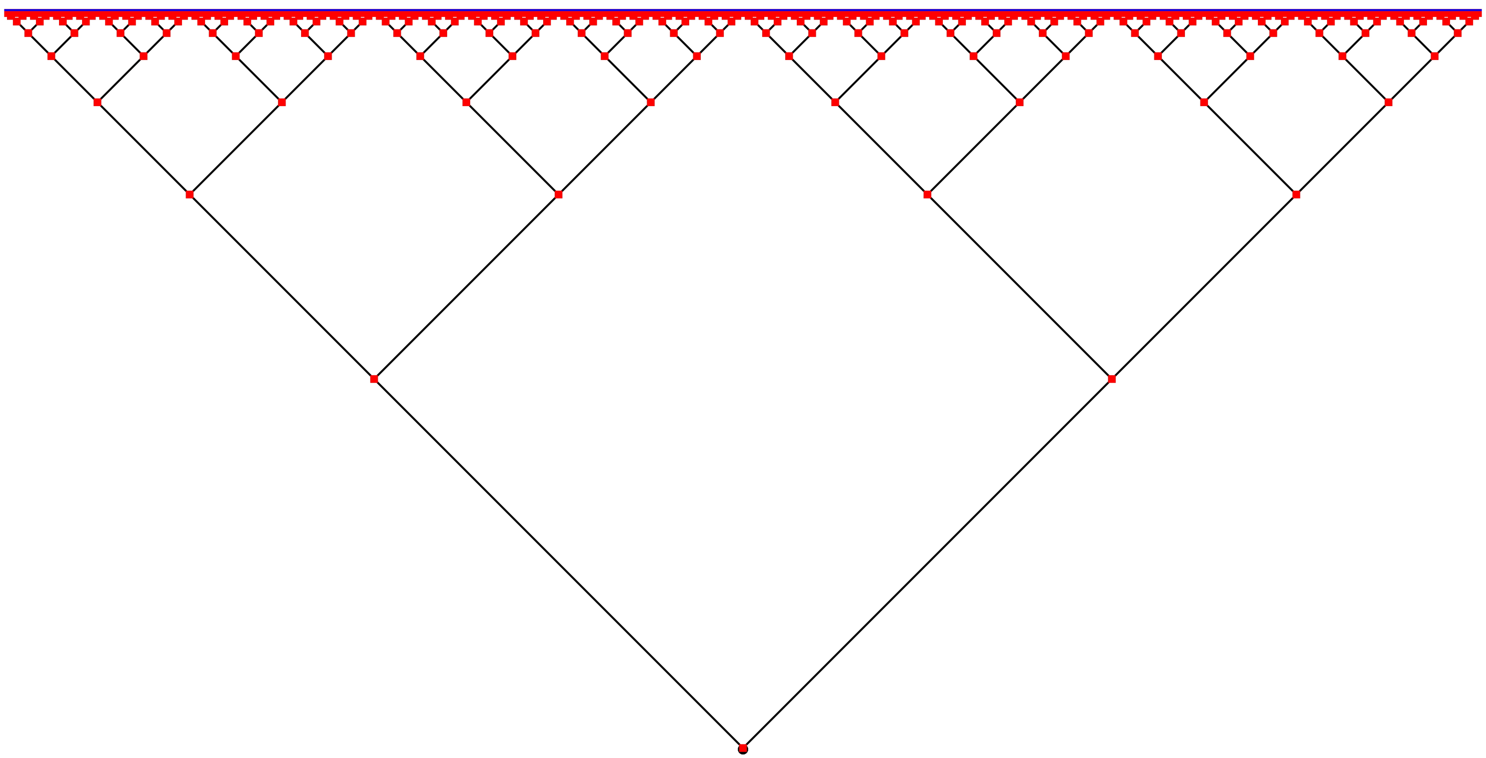
A binary tree. Level 6.

A PICTURE OF THE CONTINUUM



A binary tree. Level 7.

A PICTURE OF THE CONTINUUM



A binary tree. Level 8.

WHAT IS THE CONTINUUM HYPOTHESIS?

With the Axiom of Choice, cardinalities of sets can be ordered. It gives a meaning to the phrase "The set A has more elements than the set B".

Hence there is a first cardinal number $\aleph_1$ greater than $\aleph_0$.

WHAT IS THE CONTINUUM HYPOTHESIS?

With the Axiom of Choice, cardinalities of sets can be ordered. It gives a meaning to the phrase "The set A has more elements than the set B".

Hence there is a first cardinal number $\aleph_1$ greater than $\aleph_0$.

All attempts by Cantor to construct a 'small' uncountable set produced only the cardinal $2^{\aleph_0}$.

WHAT IS THE CONTINUUM HYPOTHESIS?

With the Axiom of Choice, cardinalities of sets can be ordered. It gives a meaning to the phrase "The set A has more elements than the set B".

Hence there is a first cardinal number $\aleph_1$ greater than $\aleph_0$.

All attempts by Cantor to construct a 'small' uncountable set produced only the cardinal $2^{\aleph_0}$.

The Continuum Hypothesis is the statement

$$\aleph_1 = c.$$

A common mistake, popularized by the famous physicist George Gamov in his expository book *"One, two, three, infinity"*, is to think that the equation $c = 2^{\aleph_0}$ is the continuum hypothesis.

THE CONTINUUM HYPOTHESIS

Kurt Gödel proved in 1940 that CH is consistent with ZFC. Paul Cohen proved in 1963 that $\neg CH$ is consistent with ZFC.

With Tarski's definition of truth there is no contradiction here with the axiom $(A \vee \neg A)$; the notion of truth depends on the metalanguage ML used to define the function $True$. By Gödel result on the continuum hypothesis, truth in the language ZFC can be defined in a metalanguage $\mathsf{M_1ZFC}$ where $True(CH)$ holds, but also by Cohen's result it can be defined in another metalanguage $\mathsf{M_2ZFC}$ where $True(\neg CH)$ holds.

THE CONTINUUM HYPOTHESIS

Kurt Gödel proved in 1940 that CH is consistent with ZFC. Paul Cohen proved in 1963 that $\neg CH$ is consistent with ZFC.

With Tarski's definition of truth there is no contradiction here with the axiom $(A \vee \neg A)$; the notion of truth depends on the metalanguage ML used to define the function $True$. By Gödel result on the continuum hypothesis, truth in the language ZFC can be defined in a metalanguage $\mathsf{M}_1\mathsf{ZFC}$ where $True(CH)$ holds, but also by Cohen's result it can be defined in another metalanguage $\mathsf{M}_2\mathsf{ZFC}$ where $True(\neg CH)$ holds.

Is one model better than the other? Here 'better' is a subjective word, but the working mathematician is guided by clear aesthetic considerations: Intuition, simplicity of arguments, linearity of patterns, and a mathematically undefinable aristotelian 'fitting with reality'. Such choices may change with time.

IS TRUTH THE SAME AS PROOF?

Certainly not.

The great logicians Gödel and Tarski took great pains to distinguish between truth and proof. Indeed, even at an elementary level there are undecidable statements in PA arithmetic that become provable theorems in ZFC mathematics, a famous case being the Paris–Harrington extension of the classical Ramsey theorem of combinatorics. The difficulty is that any proof of the Paris–Harrington theorem requires an ϵ_0-transfinite induction, unreachable by the countable induction allowed in PA. However, each specialization of the Paris-Harrington theorem reduces to a finite calculation and is (theoretically) provable in PRA by case enumeration.

IS TRUTH THE SAME AS PROOF?

Certainly not.

The great logicians Gödel and Tarski took great pains to distinguish between truth and proof. Indeed, even at an elementary level there are undecidable statements in PA arithmetic that become provable theorems in ZFC mathematics, a famous case being the Paris–Harrington extension of the classical Ramsey theorem of combinatorics. The difficulty is that any proof of the Paris–Harrington theorem requires an ϵ_0-transfinite induction, unreachable by the countable induction allowed in PA. However, each specialization of the Paris-Harrington theorem reduces to a finite calculation and is (theoretically) provable in PRA by case enumeration.

Why? The number of cases to considers grows so fast that it cannot be expressed by a formula that can be written in finite terms. So there is no finitistic proof as Aristotle required for all of mathematics.

TRUTH IN OTHER MODELS

- Field’s fictionalism.
- Empiricism.
- Social constructivism.

Hartry Field's fictionalism

Mathematics is dispensable and its statements cannot talk about reality; it is at best a useful fiction. A mathematical statement such as $1 + 1 = 2$ is meaningless in absolute and true only in the fictional world of mathematics.

Hartry Field's fictionalism

Mathematics is dispensable and its statements cannot talk about reality; it is at best a useful fiction. A mathematical statement such as $1 + 1 = 2$ is meaningless in absolute and true only in the fictional world of mathematics.

In a Wikipedia article on philosophy of mathematics, it was stated that, for Field, "a statement like $2+2 = 4$ is just as false as 'Sherlock Holmes lived at 22b Baker Street' – but both are true according to the relevant fiction."

Hartry Field's fictionalism

Mathematics is dispensable and its statements cannot talk about reality; it is at best a useful fiction. A mathematical statement such as $1 + 1 = 2$ is meaningless in absolute and true only in the fictional world of mathematics.

In a Wikipedia article on philosophy of mathematics, it was stated that, for Field, "a statement like $2+2 = 4$ is just as false as 'Sherlock Holmes lived at 22b Baker Street' – but both are true according to the relevant fiction."

A mathematician would answer that the sentence $2 + 2 = 4$ is true in the very simple language PRA of primitive recursive arithmetic and for the layman as well, while the second statement is false as it stands, as Hardy would have said, for the brutal but sufficient reason that Sherlock Holmes lived at 221B Baker Street, as seen from a fragment of the Conan Doyle story "A Study in Scarlet", beginning of Chapter 2.

John Stuart Mill's empiricism

Empiricism denies that mathematics exists independently of us. It is instead the result of empirical research, which puts mathematics on a par with other sciences, at least on this point. Mathematical truth here is only contingent to observation. Quine and Putnam proposed a form of *mathematical empiricism* that dispensed with the Platonic ontology of mathematics and justified the reality of mathematics by its ability to describe the real world.

Imre Lakatos's quasi-empiricism

Quasi-empiricism, also described as post-modernism in mathematics, questions the validity of mathematics as a whole, based on the assertion that no foundation of mathematics can be proved to exist. Thus a mathematical proof can transmit falsity from the conclusion to the premises in the same way that it can transmit truth from the premises to the conclusion.

String theory in physics has been used as support for empiricism, since it yielded new insights on space of three and four dimensions and it has been essential in the solution of long-standing problems in mathematics.

String theory in physics has been used as support for empiricism, since it yielded new insights on space of three and four dimensions and it has been essential in the solution of long-standing problems in mathematics.

General relativity can equally be used in the opposite way, since the mathematics here precedes the physics by half a century and, without it, general relativity would consist only of empty words.

String theory in physics has been used as support for empiricism, since it yielded new insights on space of three and four dimensions and it has been essential in the solution of long-standing problems in mathematics.

General relativity can equally be used in the opposite way, since the mathematics here precedes the physics by half a century and, without it, general relativity would consist only of empty words.

We may talk of black holes, of the expanding universe, of quanta and quarks, as is done in popular journalism, but physics at this level is like saying that a body falls towards the earth in the same way as a child always goes towards his mother, a view closer to Aristotle's than to reality. Attempts to reduce mathematics to an overly simple picture suffer precisely from the same defects present in journalistic physics.

Brouwer's intuitionism

In intuitionism, mathematical objects cannot be considered unless if obtained by explicit construction. The statement

$$True(A \vee \neg A)$$

is valid only if we first decide separately about the validity of $True(A)$ **and** $True(\neg A)$**.**

Brouwer's intuitionism

In intuitionism, mathematical objects cannot be considered unless if obtained by explicit construction. The statement

$$True(A \vee \neg A)$$

is valid only if we first decide separately about the validity of $True(A)$ and $True(\neg A)$.

Thus in intuitionism the most famous words by Hamlet are indeed only a question and a good deal of aristotelian and scholastic philosophy turns out to be meaningless.

Brouwer's intuitionism

In intuitionism, mathematical objects cannot be considered unless if obtained by explicit construction. The statement

$$True(A \vee \neg A)$$

is valid only if we first decide separately about the validity of $True(A)$ **and** $True(\neg A)$**.**

Thus in intuitionism the most famous words by Hamlet are indeed only a question and a good deal of aristotelian and scholastic philosophy turns out to be meaningless.

An example in intuitionism: The 'evident' statement "If I put three objects in two boxes then one box will contain at least two objects" is meaningless, unless I decide in advance how to put the objects in the boxes. Proof by contradiction (i.e. the classic *tertium non datur*) is not an admissible universal logical truth.

PROOF BY CONTRADICTION: AN EXAMPLE, I

Let $\pi(x)$ be the function of $x > 0$ which counts the number of primes up to x and let

$$\mathsf{Li}(x) = \int_0^x \frac{\mathsf{d}t}{\mathsf{log}\,t}$$

be the function called integral logarithm of x. The prime number theorem asserts that $\pi(x)$ and $\mathsf{Li}(x)$ are asymptotically the same, in the sense that their ratio tends to 1 as x tends to ∞.
In 1859 Riemann found a formula for $\pi(x)$ in terms of the solutions (the zeros) of the equation $\zeta(s) = 0$ where

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$$

is the Riemann zeta function. Riemann formulated a conjecture about the zeros of $\zeta(s)$ which turned out to be the key for understanding the finer distribution of prime numbers.

PROOF BY CONTRADICTION: AN EXAMPLE, II

The Riemann hypothesis is equivalent to the statement that

$$|\pi(x) - \mathrm{Li}(x)| \leq \frac{1}{8\pi}\sqrt{x}\,\log x$$

for $x > 2657$**. (The Riemann hypothesis is still unsolved.)**

It is an instructive enterprise to examine the deviation of $\pi(x)$ **from** $\mathrm{Li}(x)$**. The physicist Goldschmidt, a friend of Riemann, provided Riemann with a numerical table showing that**

$$\pi(x) < \mathrm{Li}(x) \quad \textbf{for all} \quad x < 3 \times 10^6.$$

Riemann himself commented on this remarkable fact in his celebrated memoir on the distribution of prime numbers. Further calculations with the help of computers showed that this phenomenon persists at least for all $x < 10^{23}$**.**

PROOF BY CONTRADICTION: AN EXAMPLE, III

Is this numerical evidence sufficient for believing that the result must hold in general? The answer is a resounding "No". In 1955, the South African mathematician Stanley Skewes proved that there is an

$$x < 10^{10^{10^{1000}}}$$

for which $\pi(x) > \mathrm{Li}(x)$. How was such a result proved?

PROOF BY CONTRADICTION: AN EXAMPLE, III

Is this numerical evidence sufficient for believing that the result must hold in general? The answer is a resounding "No". In 1955, the South African mathematician Stanley Skewes proved that there is an

$$x < 10^{10^{10^{1000}}}$$

for which $\pi(x) > \mathrm{Li}(x)$. How was such a result proved?

Skewes's argument is in two parts. The first, done in 1933, shows that it holds on the assumption of the Riemann hypothesis.The second part of the argument, obtained 22 years later, assumes the failure of the Riemann hypothesis. Then one can still obtain the same conclusion.
Such an argument relies on $True(A \vee \neg A)$ and is not admitted as a proof in intuitionistic mathematics. Still, Skewes's number is explicit!

PROOF BY CONTRADICTION: AN EXAMPLE, III

Is this numerical evidence sufficient for believing that the result must hold in general? The answer is a resounding "No". In 1955, the South African mathematician Stanley Skewes proved that there is an

$$x < 10^{10^{10^{1000}}}$$

for which $\pi(x) > \mathsf{Li}(x)$. How was such a result proved?

Skewes's argument is in two parts. The first, done in 1933, shows that it holds on the assumption of the Riemann hypothesis.The second part of the argument, obtained 22 years later, assumes the failure of the Riemann hypothesis. Then one can still obtain the same conclusion.
Such an argument relies on $True(A \vee \neg A)$ and is not admitted as a proof in intuitionistic mathematics. Still, Skewes's number is explicit!

Today Skewes's interval has been narrowed down (on RH) to

$$[1.39792136 \times 10^{316}, 1.39847567 \times 10^{316}].$$

COMPUTER PROOFS: THE FOUR COLOR THEOREM

Some mathematicians and philosophers question the 'truth' of computer proofs on the ground that they are uncheckable by the human mind. The first 'proof' of the four color theorem by Appel and Haken was soundly criticized because the computer ran for thousands of hours and also one could not verify that the computer really checked all 1476 possible cases. A new, much simplified, computer proof by Robertson, Sanders, Seymour, and Thomas, has been accepted as valid after several independent computer verifications (the computer time required is about 20 minutes).

COMPUTER PROOFS: THE FOUR COLOR THEOREM

Some mathematicians and philosophers question the 'truth' of computer proofs on the ground that they are uncheckable by the human mind. The first 'proof' of the four color theorem by Appel and Haken was soundly criticized because the computer ran for thousands of hours and also one could not verify that the computer really checked all 1476 possible cases. A new, much simplified, computer proof by Robertson, Sanders, Seymour, and Thomas, has been accepted as valid after several independent computer verifications (the computer time required is about 20 minutes).

TOO LONG PROOFS: CLASSIFICATION OF FINITE SIMPLE GROUPS

The classification of finite simple groups presents other problems.

It is extremely long and complex (originally 10,000 pages, now reduced to less than 2,000) and it is fair to say that nobody has been able to verify by himself the whole proof. Slips, inaccuracies, omitted or wrong analysis of subcases may have occurred and not been observed.

CLASSICAL PROOFS VERSUS COMPUTER PROOFS

I strongly believe that careful use of the computer tool is beneficial to the working mathematician and I have no objections in principle to the use of computers.

In fact, we may view our mathematical brains as biological computers with their own operating system, slightly different from person to person.

A mathematical proof is like a program to be run on this biological computer, with the output ‘true’, ‘false’, or the ‘I don’t understand’ that corresponds to a non-halting state of a Turing machine. The collective classification of finite simple groups is comparable to a program running in parallel on several machines in order to speed up its completion.

THE EFFECT OF FALSE STATEMENTS

In my first encounter with algebra I read how fallacious arguments (usually based on division by 0) could 'prove' that $0 + 1 = 0$. The remarkable thing is that this single statement, if assumed true, can be used to prove quickly that all numbers are equal to 0.

In a sense, the property of a proposition being false spreads out, like a malignant growth, to invade the entire domain to which it has access. Thus truth needs to be preserved carefully, uncontaminated by the vicinity of untruth. In real life, lies work in the same way and, more often than not, they are unmasked because of their consequences. The negative effects of lies on society and individuals are very clear. Lies have long-lasting negative effects on the persons affected by them.

So one may ask what is the long term effect of a false proposition or axiom in mathematics.

PROBABILISTIC PROOF CHECKING, I

This is a question that very recently has attracted the attention of computer scientists and they have come up with a truly extraordinary result. This is the *probabilistic checkable proof*, or PCP.

Proof checking is done by mathematicians in various ways. The most convincing method consists of several steps:

- **Looking first at the basic idea of the proof. In other words, start by breaking the proof into several smaller coherent pieces.**
- **Assuming that each piece is a true theorem, check the validity of the proof of the main result.**
- **Analyze the validity of each piece by the same method.**

Advantages: Conceptual errors emerge early, complex statements are broken into simpler statements of easier verification, local errors can be detected and sometimes fixed. The propagation of non-local errors can be followed clearly.

PROBABILISTIC PROOF CHECKING, II

Computational proofs cannot be brought so easily to the above format and in the worst case one needs the dreaded 'line-by-line checking'. Its complexity is proportional to the length, or *size*, of the proof. In complexity theory, it is in the class NP**.**

In naive terms, PCP **says that any mathematical proof can be reformulated in such a way that a small random sampling of a few lines suffices for checking the truth or falsity of the proof, with probability as near to 1 as we wish. The** PCP **theorem is formally stated as**

$$\mathsf{NP} = \mathsf{PCP}(O(\log n), O(1))$$

(the $O(\log n)$ **refers to the size of samplings, the** $O(1)$ **to the bounded number of random samplings).**

Intuitively, the proof to be checked is rewritten in a slightly larger redundant form, in such a way that any false statement in it propagates almost everywhere inside the rewritten proof.

CONCLUSION

All these different views of mathematics are insufficient to give by themselves a clear picture of what mathematics really is. Mathematicians compare their work to the work of an artist. They talk of beauty, elegance, strength, and depth, of a concept or proof. So what gives to mathematics its monolithic structure?

CONCLUSION

All these different views of mathematics are insufficient to give by themselves a clear picture of what mathematics really is. Mathematicians compare their work to the work of an artist. They talk of beauty, elegance, strength, and depth, of a concept or proof. So what gives to mathematics its monolithic structure?

My conclusion is that mathematics follows a kind of Darwinian evolution: Some mathematical theories and models survive in harmony with each other, while others die for lack of interest, or because of their extreme complication, or because they are absorbed within better theories. The "Ockham razor" philosophy applies here.

CONCLUSION

All these different views of mathematics are insufficient to give by themselves a clear picture of what mathematics really is. Mathematicians compare their work to the work of an artist. They talk of beauty, elegance, strength, and depth, of a concept or proof. So what gives to mathematics its monolithic structure?

My conclusion is that mathematics follows a kind of Darwinian evolution: Some mathematical theories and models survive in harmony with each other, while others die for lack of interest, or because of their extreme complication, or because they are absorbed within better theories. The "Ockham razor" philosophy applies here.

Truth in mathematics is not absolute and belongs to a language where its meaning is close to common sense. Mathematical truth is not irrelevant, nor tautological; it is the glue that holds the fabric of mathematics together. It is up to us to work to maintain the integrity of mathematics, its intellectual attraction, as well as its connections with other sciences and all other aspects of human endeavour.

THE END