euresis journal

euresis
Association for the Promotion of the Scientific Endeavour

Volume 5
Summer 2013

journal homepage
www.euresisjournal.org

The shifting aspects of truth in mathematics

Enrico Bombieri

Institute for Advanced Studies, Einstein Drive, Princeton, New Jersey 08540, USA.
eb@math.ias.edu

Abstract

For many philosophers and logicians, mathematics is a formal language which, starting from a few axioms and rules of inference, produces new sentences. The "verifiable truth" of these sentences is basically a tautology — assuming that one can assign a meaning to the word truth in this context. However, verification can be extraordinarily comples and many working mathematicians, myself included, consider such a point of view as irrelevant, in the same way that limiting English to just a set of words put together by means of grammar and syntax does not suffice for understanding Shakespeare, Dickens, or Yeats. This is indeed an important subject of philosophy about which much has been written, with important contributions by Heidegger, Wittgenstein, and Quine. The implication for mathematics of the problem of translation are clear. Is all of mathematics expressible in a single language, or are there several distinct, not quite comparable, mathematics, each one with its own language?

> *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.*

1. Premise

The English mathematician G.H. Hardy tells us the story of one of his visits to his friend and mathematical genius Srinivasa Ramanujan, while he was lying ill on his deathbed. This is how Hardy recalls the story of how he tried to start a conversation without asking right away about the status of his health in [8], p.12. 'I had ridden in taxi-cab No. 1729, and remarked that the number seemed to me rather a dull one, and that I hoped it was not an unfavorable omen. "No", he replied, "it is a very interesting number; it is the smallest number expressible as a sum of two cubes in two different ways."'[1]

This true story is quite remarkable because it sheds light on the way a mathematician such as

[1] $1729 = 12^3 + 1^3 = 10^3 + 9^3$.

Ramanujan thinks about mathematics. For many philosophers and logicians, mathematics is a formal language which, starting from a few axioms and rules of inference, produces new sentences. The 'verifiable truth' of these sentences is basically a tautology. (Assuming that one can assign a meaning to the word truth in this context.) However, verification can be extraordinarily complex and many working mathematicians, myself included, consider such a point of view as irrelevant, in the same way that limiting English to just a set of words put together by means of grammar and syntax does not suffice for understanding Shakespeare, Dickens, or Yeats. Moreover, anyone familiar with the difficulty of translating one language into another (the literal "away from the eye, away from the mind" could become "the blind man is an idiot") will agree that languages are in general not isomorphic and present subtle, but important, differences both in structure and emphasis.

This is indeed an important subject of philosophy about which much has been written, with important contributions by Heidegger, Wittgenstein, and Quine [12] with his influential thesis of 'indeterminacy of translation'. The implications for mathematics of the problem of translation are clear. Is all of mathematics expressible in a single language, or are there several distinct, not quite comparable, mathematics, each one with its own language?

2. Different views

For the working mathematician, the *'Simple Platonic'* point of view that there is only one mathematics in the Platonic world of ideas, limiting mathematics to a language with its own grammar and syntax, is too narrow; even the modified *'Plentiful Platonism'*, which allows for the existence of an objective set of distinct mathematics (as long as they are consistent) putting all of them on a par, is too wide and again missing the point when it comes to describe what mathematics is or should be.

However, many mathematicians agree with the *Platonic* (or *realist*) view that mathematics exists independently of us, but also believe the mathematical objects are not just formulas, propositions, or theorems. Hardy's view here is quite explicit: "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*." Mathematics as a science of patterns is treated in the chapter by Oliveri in [10] and is closely related to Wittgenstein's notion of aspect. The fact that the patterns themselves can be described by formulas is irrelevant. No one (except a computer) would describe a painting as a collection of colored dots or, even worse, as a collection of atoms and molecules arranged on a canvas in a certain way. Such a narrow description is clearly inadequate. What really matters is the pattern.

Another point of view, espoused by a smaller group of theoretical mathematicians, is that mathematics is only a construction of the mind (or the collective mind) and the role of the mathematician is analogous to that of an architect, rather than of an explorer. This is the *constructivist* view of mathematics. Thus one has different types of mathematics according to which constructions and rules are allowed. Constructivism allows only dealing with actual mathematical objects; the plus side is to provide a method with a solid foundation. Thus the constructivist mathematician works like an architect and builder, with the materials available to him; the constructions coming out of nowhere, done overnight by a jinn in the novels from the Thousand and One Nights, do not exist in his solid world.

However, much everyday mathematics may need modification in a constructivist world. For example, in the definition of limit it is not sufficent to say that a sequence $a_1, a_2, \ldots$ tends to a limit a; it is also needed to say constructively *how* it tends to a. A classical proof by contradiction (if the negation of a statement S leads to contradiction, then S is true) is not part of constructivism, because it is an inference for which the premise has not been constructed. Pure existence statements also are severely restricted, creating difficulties with 'self-evident' methods used by the professional mathematician, such as the pigeon-hole principle. Notwithstanding the fact that certain deep classical results of mathematics could be reformulated and proved anew in these limited models, these theories have so far a small number of practitioners among the working mathematicians.

Somewhat half-way between constructivism and realism is the *formalistic* view of mathematics, for which mathematical statements may be thought of as consequences of the allowed rules (the inference rules) for deducing new statements from initial statements (axioms). Concepts like 'number', 'line', 'space', belong to the platonic world but not, *per se*, to formalism. A serious difficulty with the formalistic approach was that freewheeling infinite constructions quickly led to antinomies and paradoxes, as in early models of set theory. (Justly famous is Russell's Paradox, namely the impossible 'set R of all sets S with the property that S is not an element of S'.) A way out of such difficulties was obtained by restricting mathematical objects and proofs in various ways, for example by barring self-referential definitions of sets or allowing only finite constructions, but the last word on this has not been written yet.

At least as I can judge from talking to very distinguished colleagues, most mathematicians usually regard mathematics as the discovery of arcane constructions, with an internal coherence and beauty and lying in a far-away land of which we can grasp only a tiny piece at a time. In practice, he works as a formalist in order to validate his discoveries. There are notable exceptions here and some of the greatest geometers of the 20th century, for example Poincaré, Enriques, and the contemporary Fields medalists Thurston and Jones, considered, or consider, strict formalism as an unnecessary baggage and an obstacle to imagination and creativity, especially when dealing with geometry. For them, the right idea and vision are more important than a formal proof that necessarily takes only second place. Certainly, this view has many merits. Mathematics, in the presence of the right ideas, can advance also without proofs. However, I firmly believe that even if the consolidation of first ideas can be postponed, it cannot be avoided altogether and eventually it must be done if we want further progress to occur.

The first and main validation of big ideas consists in the opening of new large vistas coherent with existing knowledge, which indicate the answers to long-standing questions and suggest approaches to the solution of new problems arising from these new ideas.

Applied mathematics is somewhat different, in the sense that at least 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 and 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" ([9], p.135) 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." This disdaining view applies also to the way some practitioners of the so-called 'pure mathematics' regard the work of others. André Weil, one of the foremost geometers of the twentieth century, referring to the flood of papers appearing in mathematical journals on the subject of partial differential equations used to quip that it was the work of 'elliptic engineers'. Personally, I believe that this self-serving purist stance is damaging to science and that scientific work is good if it reaches its objective.

My own view is that mathematics is the science of relations. What matters here is the relation between objects, not the objects themselves. Very different objects can share the same relation. The simplest relation is the relation of equality[2] denoted by the symbol =. A deeper example is the Laplace equation, expressing a fundamental condition for the minimum energy at which equilibrium is attained. Patterns are aspects of relations and, sometimes, can be identified with relations. The study of relations clarifies the task of determining the validity of mathematical work even in the absence of proofs and may be a source of inspiration as well. At any rate, this view of relations is clearly related to the patterns of Hardy or Oliveri.

Since relations can be taken as objects of other relations, as is the case in the branch of mathematics called category theory, mathematics can be self-referential, in contrast to all other sciences. Hence there is a certain risk in abandoning the information about the objects in favor of studying only the structure of relations; it consists in being caught in a sterile game in which research is done for its own sake, losing connection with reality and motivation and validity as well. On the other hand, the real strength of mathematics derives from the

[2] Mathematicians tend to use the equality symbol in a loose fashion, often using the same symbol = to define a new symbol (e.g. π = area of a circle of radius 1) and other times as a result of an operation or value of a function, (e.g. $2 + 2 = 4$). Although there are modified symbols available in the standard mathematical vocabulary to distinguish among various notions of equality, such as := to assign a value or definition to a symbol, they are not used consistently and the actual logical meaning of the symbol = is derived from the context in which it is used.

fact that mathematics is the study of relations between objects and therefore is of almost universal applicability. Thus we need to understand which relations are worth studying and then integrate our understanding of the relations with our understanding of the objects.

With the advent of the computer, traditional theoretical mathematics, long considered useless for applications, has become available to the other sciences in unforeseen ways. Hardy's remark (and belief) that "real mathematics has no effects on war" (he uses the term 'real' opposite to the 'trivial' utilitarian view of mathematics as the "grammar of size and order" propounded by Hogben) is not valid anymore today, as witnessed by the routine use of deep parts of number theory in cryptography. Twenty years ago I would have agreed with Hardy that, fortunately, prime number theory had no role in war or real life, but certainly this is no longer the case today.

3. Truth and mathematics

Mathematics has always been a paradigm for truth. When we want to emphasize in ordinary language the certainty of knowledge, we say "It is mathematically certain". The word 'proof' is often used as a synonym for established truth.

In contrast to other sciences, mathematical knowledge, once established, remains and is never discarded. Results may be subject to revision, as exemplified by the discovery of alternative proofs of difficult theorems. Old theories may become fragments of larger all-encompassing theories.

I remember a very interesting discussion I had with Thomas Kuhn about the absence, or presence, of revolutions in mathematics. Kuhn's view was that mathematics, since it lacked the ultimate test of fitting with reality, could not possibly undergo revolutions in its development. A revolution in science occurs when existing well-established theories develop to a point in which they are in contradiction with the observation. The effect of the revolution is to create a new understanding and rapid development of a new branch of science. My own view was that revolutions in mathematics occur when new discoveries suddenly make an established theory obsolete, even if it is correct. My favorite example was Abel's introduction of elliptic functions that transformed completely the existing theory of elliptic integrals, but Kuhn readily made mincemeat of my romantic thesis. The reader may find a thorough discussion of the subject, with various different views, in the book *Revolutions in Mathematics*, edited by D. Gillies [6].

Quantum physics and relativity are prime examples of revolutions in the physical sciences, the first arising from the failure of classical physics to explain the observed law of a black body radiation, the second from the Michelson and Morley interferometric experiment that showed that the motion of the earth does not change the speed of light, in total contrast with

Galileian and Newtonian mechanics. In chemistry, the discovery of elements destroyed the idea that matter was a mix of air, water, earth, and fire. In astronomy, the Ptolemaic model of the universe collapsed when better instruments of observation were invented.

Nothing comparable could be found in mathematics. Kuhn quickly objected to my feeble attempts to present the discoveries of non-Euclidean geometries and of elliptic functions as revolutions in mathematics. Non-Euclidean geometries did not diminish the validity and interest of Euclidean geometry, he said, they only showed that the fifth postulate of Euclid was essential for the existence and uniqueness of parallels and was not a consequence of the other postulates. Abel's discovery of elliptic functions perhaps was nearer to a revolution, since it led to an explosion of research that continues unabated today, and also because it signed the demise of the classical theory of elliptic integrals, now viewed only as the inverse functions of elliptic functions. However, in Kuhn's view, there was one factor missing to qualify Abel's discovery as a revolution, namely preceding theories were shown to be inadequate or obsolete, but still there was no contradiction there.

The absence of contradiction in classical mathematics is an interesting phenomenon. Does mathematics deal with truth? But what is truth? Should we view classical logic and classical mathematics as contradiction free? Is the notion of truth absolute, or is truth identifiable with verification, i.e. proof? Can truth, or proof, be achieved by consensus? By automatic verification, i.e. by computer programs? Can a phrase such as "it is 99% true" be meaningful in mathematics? Is the *tertium non datur* (i.e. the law of the excluded middle) a necessary building block of mathematics? Is a purely existential statement (for example, the theorem[3] that the equation $ax^n + by^n = cz^n$ with a, b, c non zero integers and $n \geq 3$ has only finitely many solutions in coprime integers (x, y, z)) acceptable in mathematics as a valid statement?

4. Different mathematics

I have already hinted at different ways to look at mathematics.

- *Platonic realism* – the numbers are primitive concepts that exist on their own. Assuming certain axioms about numbers, other logical statements follow, as well as other concepts. Everything about numbers follows from arithmetic. In the same way, all geometry follows from primitive concepts such as lines and circles.
- *Brouwer's intuitionism* – here the language of mathematics is restricted. Mathematical entities do not exist until they have been constructed. The axiom of the excluded middle is not part of the system, therefore forbidding the classical 'proof by contradiction'. Existence proofs must be constructive. A non-constructive pigeon-hole principle is not allowed either. Notwithstanding its apparent narrowness, many basic theorems of

[3] A special case of a famous theorem of Gerd Faltings. As of today, there is no proven algorithm to determine all solutions of this general equation.

mathematics can be proved in this system.

- *Formalism* – here the language of mathematics is quite ample and can be modeled by set theory. Infinite constructions are allowed, with much more freedom than before. As shown by Alfred Tarski, the concept of truth can be formalized in such a system.

There are other views about mathematics. Although many mathematicians consider them as irrelevant, if not nonsensical, philosophical exercises, these views have found a good audience with social scientists and are bound to change the way mathematics is taught in schools. If only for this reason, they deserve our attention.

However, my personal opinion is that many of these all-encompassing theories suffer of what I call the 'Shoehorn Principle', namely trying to force a big, complex subject into the too narrow petty theory of the proposer. This reduces the validity of the new ideas which may be present in it.

- *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 full Platonic ontology (the existence of abstract entities without characterization in space or time), by limiting it to the part of the Platonic universe which is required by scientific theories, and justifying 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.
- *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.
- *Social constructivism and social realism* – In social constructivism, mathematics is a product of culture, subject to correction and change. As such, it is only a product of the human mind and it does not exist until it has been thought out; mathematics has no universal connotation. Social realism goes even further, presenting a postmodernist view of it. As with empiricism, mathematics goes through constant re-evaluation, but dictated by the fashions of the social group doing mathematics, hence subject to the influence of racism and ethnocentrism, or by the needs of the society financing it.

Again, while one cannot deny the presence of fashion and social factors in the development of today's mathematics, the very fact that major milestones such as elliptic functions and the theory of groups were introduced by Abel and Galois, at the time young unknown mathematicians working in isolation and poverty, indicates that social realism alone cannot explain by itself why mathematics is the way it is today. A reading of the letters of Abel and Galois ([5], pp.25–32) is the best explanation why they were mathematicians and what they were seeking with their work, namely knowledge of truth and not fame nor wealth.

5. Truth in classical mathematics

Hilbert proposed a program to obtain a complete and consistent axiomatization of mathematics, starting from the reasonable assumption of the consistency of a small number of intuitive basic axioms, as in *finitary arithmetic*. Hilbert's program in its original form was brought to a sudden halt by Gödel's second incompleteness theorem, that states that any sufficiently strong model of mathematics (in the sense that it can prove a certain amount of arithmetic, as in the theory PA (Peano arithmetic)) cannot prove its consistency within itself.

Notwithstanding this drawback, the formalization of mathematics continued quite successfully with the Bourbaki group with the axiomatization of large parts of algebra, analysis, and geometry. Unfortunately, the rather dogmatic approach taken by Bourbaki had a negative influence at the end, by excluding explicitly entire sectors of mathematics from consideration in their program. The disastrous introduction in the schools of the 'new mathematics' based on elementary set theory was an offshoot of the Bourbaki influence. Its negative effects are felt even today.

Truth in classical mathematics is not an absolute about a Platonic absolute in an absolute world of ideas. The formalization of truth for specific formal theories of mathematics is possible, as shown by Alfred Tarski in a famous paper.

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 the *name* of a sentence, the second 'snow is white' is a sentence in the language for which we are giving a definition of truth. The distinction is a subtle one. For Tarski, the definition of truth in 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

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

where $True$ does not occur in φ. Of course, one wants to be able to say that, in an adequate definition of truth, intuitive truths become truths. This is *convention* T, namely the requirement that for any formula A of the language L, the language ML proves '$True$('A') if and only if A', where 'A' is the name of the sentence A in ML.

For suitable formalized theories expressed in a language L, the definition of truth will take place in a richer metalanguage ML. Under suitable conditions too technical to describe here, Tarski 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 definition of truth is a semantic definition and therefore is language dependent, a fact criticized by Field and others philosophers advocating an universal concept of truth. A response to this criticism is that, after all, there is no valid *apriori* reason to assume truth as an absolute concept, in the same way that beauty cannot be considered an absolute concept.

The advantage of Tarski's definition is to point out that, by embedding L in the stronger language ML, a predicate $True$ can be formally defined in ML that can be used to define 'truth' in L, with all the properties intuitively expected from a notion of 'truth'. In Tarski's model, classical logic with the assumption that every sentence is either true or false (bivalency) makes it impossible to define truth in L within L itself. This is Tarski's famous theorem of indefinibility of truth.

The indefinability of truth has proved to be hard to swallow and even more so when one wants to have a notion of absolute truth at all costs. Other interesting theories exist that deal with the liar's paradox and its variants, still admitting them as meaningful sentences of the language. Kripke's theory (1975) succeeds in showing that a truth predicate $True$ can be still defined in L if one abandons the bivalence condition that the truth function has only the two values 'True' and 'False' and accepting that some sentences may have a third truth value 'neither True nor False'.

For the working mathematician, Tarski's notion of truth, taking for L the mathematics with the Zermelo-Fraenkel axioms, with 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.

In this context, one should note the extraordinary discovery by Kurt Gödel and Paul Cohen[4] of the independence of Cantor's continuum hypothesis CH from ZFC, yielding two distinct mathematics, one in which CH is a valid axiom, and another mathematics in which $\neg CH$ is also a valid axiom. With Tarski's definition of truth there is no contradiction here with the axiom $(A \vee \neg A)$. Truth in the language ZFC can be defined in a metalanguage M_1ZFC where $True(CH)$ holds, but also can be defined in another metalanguage M_2ZFC where $True(\neg CH)$ holds.

For the mathematician, choosing between the two solutions is not a matter of verifying truth, but rather of seeing whether the patterns in the first type of mathematics are preferable to the patterns in the second type of mathematics. Certainly, 'preferable' is a subjective word, but one here is guided by clear aesthetic considerations: Simplicity of arguments, linearity of patterns, and a mathematically undefinable Aristotelian 'fitting with reality'. It is here that intuition plays an important role in choosing between alternative systems, for example considerations of 'mathematical fruitfulness' in which a system leading to the solution of outstanding problems may become preferable to others. Such choices may change with time when the accumulation of knowledge clarifies obscure parts but, unlike art, the overall result of 2500 years of mathematics has been the creation of a single science. This bodes well for the future.

6. Truth in other models

Mathematicians dismiss Field's fictionalism as irrelevant and useless at best. For them, Field's success in axiomatizing Newtonian mechanics without referencing functions and numbers, and proceeding to show that mathematical physics is an extension of his non-mathematical system, is a meaningless tour-de-force. First of all, Newtonian mechanics is to physics as elementary calculus is to mathematics, or like an *abc* book in the world of literature, i.e. a mathematical triviality. Secondly, and more specific to the point, the reduction of physics to Field's non-mathematical world uses large fragments of second-order logic, bringing back

[4] Gödel proved in 1940 that CH is consistent with ZFC. Cohen proved in 1963 that $\neg CH$ is consistent with ZFC.

deep mathematics as a tool to sweep everything under the rug in order to conclude that mathematics does not exist. Although the debate whether the second-order logic implicit in Field's is really essential or not for his thesis continues, the assumption of a continuum of space-time points as an actual object seems to remain a real problem.

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 evinced from a fragment of the Conan Doyle story "A Study in Scarlet", beginning of Chapter 2 (this is the first occurrence of Sherlock Holmes's address in the corpus of Sherlock Holmes stories).[5]

The empiricist view of mathematics has certain merits. It is undeniable that the natural sciences have indicated to mathematicians, at crucial times, new fundamental directions to explore. On the other hand, reducing all of mathematics to such an empirical view does not describe the present mathematical world.

When Einstein set up his model of general relativity he found all the mathematical tools he needed ready for use, with Riemann's theory of differential geometry in arbitrary dimensions and the absolute tensor calculus of Christoffel, Ricci-Curbastro, and Levi-Civita. In the other direction, the new string theory of physics awakened the interest of mathematicians by making extraordinary predictions about the geometry of manifolds. Mathematicians had been studying curves for centuries, and the underlying spaces parametrizing curves of similar types (the so-called moduli spaces) for a long time too. Physicists showed that curves and moduli spaces could be put together in a single object with a far richer geometry than the single components and then started making predictions. Today, the insights provided by string theory have spawned entirely new directions of study and have been the key to solve outstanding open problems.

String theory has been used as support for empiricism. General relativity can equally be used in the opposite way, since the mathematics here precedes the physics by many decades and, without it, general relativity would consist only of empty words, notwithstanding Field's beliefs. 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. Black holes and the expanding universe (if indeed they are true phenomena) can be understood only in the framework of general relativity. Quanta and quarks can be

[5] Wikipedia's articles are edited on a regular basis and this error has been duly corrected.

understood only in quantum theory and unified field theories, like quantum chromodynamics. Attempts to reduce mathematics to an overly simple picture suffer precisely from the same defects present in journalistic physics.

7. Social constructivism and society

Social constructivism cannot be dismissed so simply. Mathematics, like philosophy, is studied by people and the philosophical question is whether mathematics – with all its possible variations, as in Plentiful Platonism – exists on its own, or is a product of experiment and experience, or just a product of a given society and social class. After all, art history teaches us that art developed in different societies in different ways, for different purposes.

Certainly, the historical development of mathematics is best understood taking also into account the material culture associated with it, such as universities, academies, publications, as well as the general financial support of sciences. On the other hand, this is only part of the picture and my view towards social constructivism is that it has a role in explaining the development of mathematics during the centuries, but falls well short of explaining why mathematics is today the way it is. The mathematician Fibonacci wrote his *Liber Abaci* at the beginning of the thirteenth century with the aim of teaching how to count and how to use counting for the purpose of bookkeeping, but also wrote his *Liber Quadratorum* dealing only with abstract arithmetical problems with squares. Gauss is one of the founders of geodesy, but also wrote his *Disquisitiones Arithmeticae* laying the foundations of the modern theory of quadratic forms over the integers and contributed fundamental results to abstract number theory and geometry. The notion of truth in the mathematics of Fibonacci and Gauss is the same, with proof used as the only way to verify whether a proposition is true or false; this has little to do with empiricism and even less with social constructivism.

Social constructivism ideology may turn out to have negative consequences for the future development of mathematical literacy in society. It appears that its deconstructivist approach to mathematics has been swallowed hook, line, and sinker, by certain social scientists in charge of revising the teaching of mathematics in the schools. After the dismal failure of the introduction of 'new math' in schools, caused by its excessive emphasis on abstraction, the NCTM (National Council of Teachers of Mathematics) went on a new path, swinging the pendulum all the way in the opposite direction. Traditional K12 math was deemed too difficult for children; the solution to the problem 'Johnny can't count' consisted to great extent in eliminating counting from the program. It can all be done on a pocket calculator or, if the child is smart enough, by computer, isn't that so?

The reform is characterized by ideology, in this case by constructivism, much in the same way the 'new math' was characterized by the narrow Bourbaki ideology. Here is a sample of guiding ideas, taken from the web:

- Children must be allowed to follow their own interest in discovering mathematical knowledge.
- Knowledge should be acquired as a byproduct of social interaction in a real world setting.
- General, content-independent "process" skills are the primary goals.
- Learning must be enjoyable, happy, with knowledge emerging from games and group activities.

Unfortunately, mathematical literacy cannot be achieved by lowering the baseline and citing the increased percentage of children above the baseline as proof of the success of the new pedagogical ideas. I leave it to the reader to imagine the consequences of this type of teaching at an age when minds are formed. The message is that mathematical truth is irrelevant in real life and the only thing which matters is to give a half-hearted try to understand mathematics... If you don't like it, play games and watch your favorite singer on television. The net result may very well be a renewed flourishing of private schools for the affluent segment of society. For a serious technical critical analysis of some of these proposals, I refer to the interesting chapter by E.G. Effros in [4].

The reliance on machines rather than sound reasoning (leaving calculations to the computer) makes me shudder. We have not learned the lessons we should have learned from the failure of the first mirror of the Hubble Telescope and from the crash of the Mars probe.

The first was caused by changing, half-way in the polishing process, the system for verifying the curvature of the mirror, replacing an established auxiliary optical tool by a better one. Unfortunately, the lenses in the new optical instrument had not been mounted in the correct way and the new instrument showed readings different from the old ones. So the firm in charge of the job, instead of asking why such a dramatic change had occurred, performed more corrections to the mirror. Since it proved to be impossible to obtain interferometric images which showed no mirror defects, only the cropped central part of these images was sent to NASA for final approval and the faulty mirror went up in the sky with a lot of fanfare. Eventually, reality had to set in. It took a special set of correcting lenses to bring back the Hubble telescope to its full potential. The technology to calculate the shape of the special lenses depends on very sophisticated mathematics special to the task and was not available in the United States, where everything must agree with existing computer software. Fortunately, the optical engineering division of the ETH in Zürich had the mathematical expertise and the tools to do the job.[6]

The second failure was due to the unwarranted assumption by technical engineers in the United States that the thrust figures for the probe landing rocket provided by scientists were given in the system with units in pounds and inches (still used by the industry for monopolistic

[6] This is what I learned from a Professor at ETH during a visit there.

reasons), rather than in the kilograms and meters used universally by physicists. So the probe could not break its descent and crashed into smithereens on arrival. This failure was caused by the faith in numbers per se, without anyone being able to see that a simple 'ball-park figure' checking would have shown the error. This is a typical example of what can happen because of the 'language barrier' between two different parties, when truth has a different meaning for them.

8. Variations on proofs

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, see [11]. The difficulty, in the case just mentioned, is that any proof of the Paris-Harrington theorem requires an ϵ_0-transfinite induction, unreachable by the principle of induction allowed in PA. However, any finite specialization of the Paris-Harrington theorem reduces to a finite calculation and is (theoretically) provable in PRA by case enumeration.

Already, it is not obvious which rules we should allow on an intuitive basis for a proof. In classical logic, the standard proof of A by contradiction is: If $\neg A$ leads to contradiction then A; this is a staple of the mathematician. However, in this form it is not allowed in intuitionistic mathematics, where the only accepted form of proof by contradiction is: If A leads to a contradiction, then $\neg A$.

Complicated but interesting examples of proof by contradiction come from number theory and I will give here a concrete example. Let $\pi(x)$ be the function of $x > 0$ which counts the number of primes up to x and let $\mathrm{li}(x) = \int_0^x \mathrm{d}t/\log t$ be the function called integral logarithm of x. The prime number theorem asserts that $\pi(x)$ and $\mathrm{li}(x)$ 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 a certain equation $\zeta(s) = 0$ where $\zeta(s)$, nowadays called the Riemann zeta function, admits a deceptively simple description[7]. Riemann formulated a conjecture about the zeros of $\zeta(s)$ which turned out to be the key to the understanding of the finer distribution of prime numbers.

The Riemann hypothesis implies, and is equivalent to, the statement that

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

for $x \geq 2657$ (L. Schoenfeld, [15]). The Riemann hypothesis is still unsolved and, for various

[7] It is the sum of the s-powers of the reciprocal of the natural numbers if the resulting series is absolutely convergent and is otherwise defined by analytic continuation.

reasons which go beyond its implications on the distribution of prime numbers, has risen today to the status of the most important unsolved problem in all of pure mathematics.

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 for $x < 3 \times 10^6$ one always had $\pi(x) < \mathrm{li}(x)$. Riemann himself commented on this remarkable fact in his celebrated memoir on the distribution of prime numbers.[8] Further calculations with the help of computers showed that this phenomenon persists for all $x < 10^{23}$.

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, which was done in 1933, is on the assumption of the Riemann hypothesis and produces the existence of such an x in a certain specific very large interval. The proof of this result is sufficiently flexible to reach the same conclusion unless there is a 'large failure' of the Riemann hypothesis. The second part of the argument, obtained 22 years later, depends in an essential way on the assumption of the hypothetical 'large failure' of the Riemann hypothesis. By a different reasoning, it again produces an explicit extremely large interval containing a point x for which $\pi(x) > \mathrm{li}(x)$.

The larger of the two intervals is the final one provided by Skewes. This type of logic, in which one assumes the true sentence $(A \vee \neg A)$ (the law of the excluded middle) to deduce B, is not unusual in number theory. Note that the conclusion, where an explicit interval is computed, is deterministic in every possible sense; the fact that the interval is way too big for us to be able to produce (and possibly even write down) such an x is irrelevant for abstract mathematics. Recently, Skewes's argument has been greatly improved and refined in many ways by several authors. On the Riemann Hypothesis, the range of the interval has been narrowed down, after extensive computer calculations, to $[1.39792136 \times 10^{316}, 1.39847567 \times 10^{316}]$, see [2, 16].

Some mathematicians and philosophers may question the 'truth' of such a result on two grounds. The first, is the use of the law of the excluded middle; this would be the case for an intuitionist. The second, is the use of computer calculations, since we can never know for sure what a computer does.

[8] Mathematical folklore says that Riemann conjectured that $\pi(x) < \mathrm{li}(x)$ was always the case. A reading of Riemann's memoir shows that Riemann expressed in this context only the suggestion that

> *It would be interesting, in a further development, to study the influence of each periodic term contained in the given expression for the totality of prime numbers.*

As Littlewood later showed, he was right.

Other mathematicians have also expressed reservations about computer proofs or extremely involved and complicated proofs. The first 'proof' of the four colors conjecture was obtained by very heavy use of formal calculations by computer. In this case, many reservations were put forward because of what appeared to be inefficient or insufficient programming, so it was not clear that the computer actually had analyzed all the 1476 possible cases. All this was eventually put to rest by a much simplified new proof, still based on similar ideas, where both the theoretical part and the computer part could be scrutinized carefully, see [14]. The computer analysis now requires only 20 minutes of running time and has been independently repeated on other machines, with independent programs.

The classification of finite simple groups presents problems of different type. It is an extremely long and complex endeavor and it is fair to say that not a single person has been able to verify everything in the proof. The number of authors who have contributed to the solution is large (over 40) and some of the papers are very long, complex, and computational. It is here that slips, inaccuracies, omitted or wrong analysis of subcases may occur.

I did contribute one paper with the completion of the solution of a rather difficult uniqueness problem, namely showing that the known list of finite groups of Ree type in characteristic 3 was indeed a complete list. Group theorists had reduced the problem to a question of algebra which, while in principle soluble by standard methods, remained inaccessible because those methods quickly led to formulas with more than 10^{50} terms, hence impossible to write down in any form. Fortunately, I found an additional trick which showed that any formula one could obtain in this way also implied the existence of another formula with only two terms and controlled degree and size, thus bypassing the impossible problem of following the algebra. So I wrote a paper which was examined rather carefully by several experts and eventually the paper was published. The last part was a computer analysis of a few isolated cases.

Interestingly enough, two independent runs (before the publication of the paper) of the computer analysis showed that the standard software used for the first run contained a serious error. (The supposed 'infinite precision' arithmetic and algebra did not extend to the degree of polynomials and if the degree exceeded the largest unsigned integer in the computer language it simply gave a wrong polynomial.) This was quickly corrected and the two runs gave the same conclusion, as expected.

Perhaps even more interestingly, my own analysis at the beginning of the paper contained a slip which was discovered only after its publication. I had claimed that a certain polynomial G in several variables was irreducible. In fact, it was reducible. I had forgotten that the specialization $z_1 \to 1/z_0$ I had indicated in a footnote for verifying my assertion, could also have removed a possible factor z_0; this was precisely what had happened. This was inconsequential for the paper, because the rather simple correction to my mistake consisted in removing the offensive factor z_0 from my definition of G, without any further change in the paper. In other cases, authors were not so lucky and substantial revisions, if not even retractions, had to be done.

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. Hence the collective classification of finite simple groups is comparable to a program running piecemeal in parallel on several machines in order to speed up its completion.

What about proof by consensus? Human consensus is risky, but computer consensus may be acceptable. There are computer programs which need a random additional input, besides the initial data. Changing the random input changes the way the program runs: Sometimes it will come to the conclusion very quickly, other times it will run for ever. (To avoid this, or excessive run time, one gives an escape time.)

One such algorithm is Hendrik Lenstra's elliptic curve factorization method. It routinely factors numbers of 60 digits on a desktop, in a very short time. Here the random input is an elliptic curve and the associated group law. The program itself uses the group law in an essential way, because changing the elliptic curve changes the way the program runs. Depending on the choice of the elliptic curve, the program may or may not yield a true factorization. Hence the need of a preliminary independent fast prime–composite test for a number.

Such a program is provided by the Solovay–Strassen probabilistic primality test and its variant the so-called Miller–Rabin test, of standard use in the RSA cryptography scheme[9]. Here one wants to generate very quickly prime numbers with hundreds of digits. The difficulty is not due to lack of prime numbers, rather it is the testing for primality. Performing the test on a number N requires an additional integer input a, called a 'base', chosen randomly between 1 and $N-1$. If the output of the test is 'composite' it yields a proof of compositeness (without factoring), but it may fail to detect compositeness, with a small probability of failure (the smaller, the better: it turns out that it is not more than 25%). So, performing the test on a number N choosing the base a at random k times, the probability of failing to detect compositeness decreases drastically.[10] This can be used to detect numbers with extremely

[9] The new deterministic primality test of Agrawal, Kayal, Saxena [1] is of polynomial complexity, but not yet as practical as the Miller–Rabin test. The fast probabilistic but deterministic primality test using elliptic curves of Goldwasser and Kilian [7] is used in practice to certify primality.

[10] The question of what 'random' means, even in this limited context, turns out to be a very deep one, so far solved only from a practical standpoint.

high probability of being primes. For example, taking $k = 20$ we have a primality test on numbers with at most 1000 digits which is correct better than 99.9999997% of the times. For practical use, quality control is there!

In my opinion, another mind boggling contribution of computer science to the nature of proof, and thus indirectly to the notion of truth, is probabilistic proof checking.

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. Lies have long-lasting negative effects on society and individuals.

So one may ask what is the long term effect of a false proposition or axiom in mathematics. This is a question which very recently has attracted the attention of computer scientists and they have come up with a result which, in my opinion, is truly extraordinary. This is the *probabilistic checkable proof*, or PCP. A technical discussion of PCP is beyond the scope of this article, so I will limit myself to a cursory description of it.

Classical proof checking is done by mathematicians in various ways. The most convincing method (for the working mathematician) consists of several steps:

- Looking first at the basic idea of the proof, in other words breaking the proof into a small number of smaller coherent pieces.
- Assuming that each piece is a true theorem, checking the validity of the proof of the main result.
- Analyzing the validity of each piece by the same method.

A proof amenable to this type of break-up has many advantages. Conceptual errors emerge early. Complex statements are broken into simpler statements of easier verification. Local errors can be detected and fixed. The propagation of non-local errors can be followed clearly, making it easier to correct faulty arguments, if possible at all.

Checking a computational proof cannot be brought so easily to the above format and in the worst case it needs the dreaded procedure of 'line-by-line checking'. Its complexity is at least proportional to the length, or *size*, of the proof. In complexity theory, this type of proof checking is in the class NP.

The experienced mathematician often is able to take shortcuts in line-by-line checking since, at a glance, he can often guess where it is most likely to make mistakes. For example, in a hand-written manuscript, transcribing a complex formula from the end of one page to the top of the next page is a well-known cause of trivial errors: a minus sign becomes a plus sign, a variable is omitted somewhere in a complex formula, and so on. However, while these shortcuts may show quickly that a supposed proof is incorrect, by no means do they work all the time. Line-by-line checking has no redeeming features: It does not look for guiding ideas and if an error is found the paper is only good for the wastebasket. It is also time consuming.

The discovery of PCP is due to the work of several mathematicians and computer scientists. 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

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

The $O(\log n)$ refers to the minimum number of random bits needed by PCP to do the random sampling, the $O(1)$ refers to the number of bits one actually reads from the proof; in fact one can take the $O(1)$ to be 3, which is optimal, to get a probability of a correct checking near to 50%, after only one sampling.

This is a deep theorem whose proof draws from logic, complexity theory, probability, and error correcting codes. A new, simpler proof of the PCP theorem has been very recently obtained by Irit Dinur and we refer to Radhakrishnan and Sudan [13] for a thorough exposition and proof of the theorem, together with an updated bibliography.

Intuitively, the PCP can be described as follows. The proof to be checked is rewritten in a slightly larger redundant form, which is done quickly (i.e. in polynomial time), for example by a certain software program. The crux of the matter is that this is done in such a way that any false statement in P propagates almost everywhere inside the rewritten proof Q. Error correcting codes are the prototypes of the method: By trasmitting a message a certain number of times with an appropriate scrambling (as determined by an error correcting code), a certain number of faulty bits can be restored correctly. As with error correcting codes, the upshot is that a random line-by-line checking of a small sample of the rewritten proof has a fixed positive probability of detecting an error.

Bernard Chazelle [3] gives a down-to-earth non-technical description as follows. A proof P of size n admits a new proof Q, where Q has two remarkable properties. The proof Q is derived from P by means of simple steps; the size of Q will be only $O(n(\log n)^c)$ (I. Dinur). The proof Q is written as a conjunction of three bits clauses on a set of logical variables $\mathcal{X}$; the actual proof is Q together with a value of $\mathcal{X}$ for which the logical value of Q is $True$.

Now pick such a clause in Q at random; this means choosing the location i of the clause, which is done in $O(\log n)$ steps, by assigning at random the $O(\log n)$ digits of i. Next, read the values of the $O(1)$ logical bits (in our case, only 3 bits) of the variables in S and evaluate S. If P is true, the test will give the answer $True$. If P is false, the test will detect $False$ with at least 49.999999% probability and this will be a proof that P is false. By repeating this random checking say 20 times, we see that if we obtain $True$ each time then it means that P is true with probability at least 99.9999%.

Does all this prove that P is true? No, but it also tells us something more. It shows (again with very high probability) that any error in P, if present at all, must be 'local', thus indicating a robustness of the supposed proof. If P is false but PCP says that P should be true, then the proof P should still be 'fixable' to a clad-iron proof.

As an example of how the PCP works, consider a supposed proof Q consisting of the conjunction of two logical clauses

$$Q = S_1 \wedge S_2 = ((\neg x_1 \wedge x_2) \wedge x_3) \wedge (x_1 \wedge (x_2 \vee x_3))$$

with the assignment $\mathcal{X} = (x_1, x_2, x_3) = (True, True, False)$ and let us pick up one clause S. Now let us toss a coin and pick up the first clause if we get heads and the second one if we get tails. If we pick up the first clause S_1, the value of the clause turns out to be $S_1 = ((\neg True \wedge True) \wedge False) = False$, so the supposed proof Q will indeed be shown to be fallacious, while if we pick the second one S_2 we have the value $S_2 = (True \wedge (True \vee False)) = True$ and we have a "false positive" testing. The probability of such a random "false positive testing" is only 50%, so if we repeat the test independently 20 times the probability of obtaining a sequence of 20 "false positive" tests is less than one in a million.

From the point of view of complexity theory, the PCP theorem is a statement that the probabilistic verification of a purported proof of a theorem is always 'very easy', even if finding a proof may be exceedingly 'hard'. In fact, the question whether finding a proof is always 'easy' is equivalent to the celebrated question of computer science whether P = NP or not.

To put this in perspective with the classical way of proof checking, a proof Q consists of a conjunction of n clauses, each one involving three variables: so, altogether not more than $3n$ variables, together with an assignment $True$, $False$, of each variable, yielding the value $True$ for Q. Since the total number of possible assignments can be exponentially large in n, finding a proof by trying out all assignments is hopelessly complex. On the other hand, checking a given assignment requires not more than $O(n)$ operations, so it has only polynomial complexity in n, so 'proof checking' is 'easy' in this sense. However, PCP is probabilistically extraordinarily efficient, requiring at each stage only $O(\log n)$ bits for selecting a location for testing, followed by testing the value of the selected clause. With $O(1)$ tests, each one requiring only $O(\log n)$ random bits (to select a random location in Q for testing), one can obtain an 'almost certain' verification of the validity of the proof. Thus we may call this type of 'practical verification' to be 'very easy', because $O(1)$ is much smaller than $O(n)$. (By what we have said, both algorithms require $O(\log n)$ space, which is quite small.)

Perhaps some day we will see pre-proofs P that will be automatically encoded in a new form Q and then checked by PCP. If Q fails the test, P will be automatically incorrect. If instead Q passes the test, then P will be considered worth of serious consideration and only then mathematicians will make the serious effort of embarking in the task of checking whether P is a formal proof or not. Alternatively, the random checking of Q will be done not 20, but instead 20000 times. Then P must be accepted as a 'human proof' in the human mathematical world!

9. Conclusion

In my view, history of mathematics shows that all these different views of mathematics may illuminate parts of it, but are grossly insufficient to give by themselves a clear picture of what mathematics really is.

Mathematicians, at times, compare their work to the work of an artist. Notwithstanding the rigidity of mathematical rules of inference, they believe that mathematics is a very creative science. They talk all the time of beauty, elegance, strength, and depth of a new concept or of a proof. Now beauty, elegance, strength, depth, are undeniably strongly influenced by culture and are far from being 'absolute'. So what gives to mathematics its monolithic structure?

Here is a personal experience which I find quite instructive. In 1973 I became interested in the problem of classification of compact complex surfaces. After the pioneering work of Kodaira around 1960, there remained some open questions and in particular the existence and classification of complex surfaces without complex curves. This was a particularly tricky problem because the methods used in classification began by looking at the complex curves sitting inside the surface, so new methods were needed. I had started thinking on the problem of the classification of surfaces without curves when I was informed by Michael Atiyah, in a casual conversation at a meeting in Paris, that Kodaira had just constructed such surfaces although he did not remember how it was done. In a couple of weeks I found not only a construction, but also proved that the new examples so found were the only ones possible, under certain natural hypotheses. The starting point of my work was Kodaira's third paper on the subject, which I had studied earlier very well, but it needed adding several entirely new ideas. Since I was aware that Kodaira had obtained something similar, I wrote to Kodaira informing him of my conversation with Atiyah, including a copy of my rather long manuscript. About two weeks later I received Kodaira's answer. It informed me that his student Inoue had been working on the problem for some time and had also obtained a little earlier the same result, and included Inoue's long manuscript. I was at first surprised to see that the two manuscripts were almost identical, including the new notation introduced in them, but the true reason for this was that there was only one logical way to attack the problem. Only at the most delicate point of the proof the two manuscripts were essentially different. Since Inoue had clear priority about the result and since my own paper more or less followed the same proof, I felt that there was no point in publishing my own version of the solution and I informed Kodaira of this. Very kindly, Inoue added a note in his final published paper acknowledging my independent solution.

I find it striking that two mathematicians, working independently on the same problem, ended up with writing almost identical papers, with almost exactly the same logical sequences of formulas. Some may view this as a proof of the strength of cultural influence, in this case Kodaira's work. To me, this is one more example that some parts of mathematics are very rigidly set up and that there is some ineluctability in the way mathematics evolves. The unity of language in today's mathematics is certainly a cultural phenomenon, but its very existence is, in my opinion, a reflection of the inner unity of mathematics. Mathematics has determined its own language, and not viceversa.

Mathematical concepts are not arbitrary. Here is a simple example. We could do Euclidean geometry without the concepts of triangle and polygons and talk instead about finite sets of points assembled in a circular ordering (this allows polygons with self-intersecting sides). What is gained with the primitive notion of triangle is that polygons with non-intersecting sides (an interesting class by itself, for example they have an intuitive notion of area) are all decomposable in triangles. In order to study general polygons, we may study first the simplest subclass, namely triangles, and then study how polygons are assembled from triangles. Since this method proved to be successful, the concept of triangle remains even today as a useful primitive concept of geometry.

My conclusion is that mathematics follows a kind of Darwinian evolution, where complicated concepts are eventually abandoned in favor of simpler ones and new concepts are introduced with the purpose of unifying and simplifying existing ones. The "Ockham razor" philosophy is relevant to mathematics. Some mathematical theories and models survive in harmony with each other, while others die for lack of interest, or because of their unnecessary extreme complication, or simply because they are absorbed within better and ampler theories. At times, we may even see different "mathematical species" appear in the mathematical world.

All this is consistent with the view that mathematics is a theory of relations and patterns. Truth in mathematics is not absolute and is directly related to language or, better, to a larger metalanguage where the meaning of truth is close to common sense. Therefore, 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 endeavor.

Acknowledgment. The author thanks Paolo Mancosu for a critical reading of this paper and suggestions on how to remove several inaccuracies. The inaccuracies that remain are the sole responsibility of the author.

Bibliography

1 Agrawal, M., N. Kayal& N. Saxena (2004). "PRIMES is in P", *Ann. of Math. (2)*, **160**, 781–793.

2 Bays, C. & R.H. Hudson (2000). "A new bound for the smallest x with $\pi(x) > \mathrm{li}(x)$", *Math. of Comp.*, **69**, 1285–1296.

3 Chazelle, B. (2006). "Mathematics: Proof at a roll of the dice", *Nature* **444**, 1018–1019.

4 Effros, E.G. (1998). "Mathematics as language", in *Truth in Mathematics*, H.G. Dales and G. Oliveri eds. (Oxford Science Publications, Clarendon Press), 131–145.

5 Galois, E. (1897). Œuvres Mathématiques (Gauthiers–Villars, Paris).

6 Gillies, D. ed. (1995). Revolutions in Mathematics (Oxford University Press, Oxford).

7 Goldwasser, S. & J. Kilian (1999). "Primality testing using elliptic curves", *J. ACM*, **46**, 450–472.

8 Hardy, G.H. (1940). Ramanujan – Twelve Lectures on Subjects Suggested by His Life and Work (Cambridge Univ. Press, Cambridge).

9 Hardy, G.H. (1967). A Mathematician's Apology — with a Foreword by C.P. Snow (Cambridge).

10 Oliveri, G. (1998). "True to the pattern", in *Truth in Mathematics*, H.G. Dales and G. Oliveri eds. (Oxford Science Publications, Clarendon Press) 235–269.

11 Paris J., J. and L. Harrington (1977). "A mathematical incompleteness in Peano arithmetic", in *Proof theory and constructive mathematics*, Handbook of mathematical logic, Part D, pp. 819–1142. Studies in Logic and the Foundations of Math., Vol. 90 (North-Holland, Amsterdam).

12 Quine, W.V.O. (1960). Word and Object. (Cambridge: MIT Press).

13 Radhakhrishnan, J. & M. Sudan (2007). "On Dinur's proof of the PCP theorem", *Bull. Amer. Math. Soc.*, **44**, 19–61.

14 Robertson, N., D. Sanders, P. Seymour, R. Thomas (1997). "The four-colour theorem", *J. Combin. Theory Ser. B*, **70**, 2–44.

15 Schoenfeld, L. (1976). "Sharper bounds for the Chebyshev functions $\theta(x)$ and $\psi(x)$. II", *Math. Comp.*, **30**, 337–360.

Internet sources:

16 Chao, K.F. & R. Plymen (2007). "A new bound for the smallest x with $\pi(x) > \mathrm{li}(x)$", preprint, 14pp. In http://arkiv.org/abs/math.NT/0509312v5

17 `http://en.wikipedia.org/wiki/Philosophy_of_mathematics`, Wikipedia

18 `http://en.wikipedia.org/wiki/Alfred_Tarski`, Wikipedia

19 `http://www.textetc.com/theory/truth-in-mathematics.html`, by John Holcombe

20 `http://plato.stanford.edu/entries/tarski-truth/`, Stanford Encyclopedia of Philosophy