Why Do We Prove Theorems?

YEHUDA RAV*

Prologue

Once in conversation at a social gathering, a colleague working in medical research grumbled about the difficulties of doing research in his field, given the ever increasing complexity of laboratory techniques and the unmanageable amount of scientific literature to be assimilated. Turning toward me, he added: 'It is so much easier to be a mathematician. If you want to know whether a theorem is true or not, all that you have to do is to program your computer and you get the right answer.' Such statements, in one form or another, are frequently made, and curiously, even in many scientific circles there is the widespread belief that computers can, or at least will eventually be able to, solve every mathematical problem and dispense with mathematicians' searching for proofs. Various weaker claims are even occasionally made within the mathematical community, and together with certain technical results on probabilistic algorithms, to be discussed below, have led to misleading journalistic reporting. As to the medical researcher, he was rather surprised to learn that it had been *proven* in the early thirties that no computer program (read: algorithm) can be constructed to check, in a finite number of steps, whether any given formula of first-order logic is or is not derivable (provable) in that system. (This is the Church-Turing Theorem, yielding a negative solution to the general decision problem as proposed by Hilbert.)

The conversation at the social gathering and recent discussions of the function of proofs spurred the following musings. Let us fancifully pretend that the general decision problem did after all have a positive solution, that every axiomatisable theory was decidable, and that a universal decision algorithm was invented and implemented on oracular computers, marketed under the trade name of PYTHIAGORA (Pythia + Pythagoras). There she is, sitting on the desktop of every mathematician. Not only can PYTHIAGORA answer all our questions, but she does so at the speed of light, having no complexes about complexity of computation. Think how won-

* Department of Mathematics, University of Paris-Sud, F-91405 Orsay, France.
yehuda.rav@wanadoo.fr

derful it all would be. You want to know whether the Riemann hypothesis is true or not, just type it in (using some appropriate computer language), and in a split second, the answer is flashed back on your screen: 'true' or 'false'. And on you could go using the Riemann hypothesis, now turned into Riemann's ζ-theorem by the grace of PYTHIAGORA if she said 'true'. Fermat's Last Theorem? No more unpalatable stretching of the margin so that it can contain all the subtleties of elliptic curves, Iwasawa theory, automorphic forms, deformation theory and what not. No sooner have you typed in Fermat's problem than the long-awaited answer appears on your magic screen, without any brain-wracking help from Andrew Wiles! Perhaps we should not strain PYTHIAGORA with the continuum hypothesis, unless we let her say a little bit more than 'true' or 'false'. With due accommodations, think of the explosion in mathematical knowledge thanks to PYTHIAGORA. No more painful refereeing, no more plowing through incomprehensible, or at best, difficult proofs. After all, if all our toil and sweat in proving theorems served only to ascertain whether they were true or not, then PYTHIAGORA would deliver us of useless labours and frustrations. No more 'dirty work'; all our creative energies would be channelled into brilliant and daring conjecturing. We mathematicians would only have to produce conjectures, and let PYTHIAGORA weed out the false from the true. What a paradise! What a boon!

Did I say boon? Nay, I say, no boon but doom! A universal decision method would have dealt a death blow to mathematics, for we would cease having ideas and candidates for conjectures. The main thesis to be developed here is that the essence of mathematics resides in inventing methods, tools, strategies and concepts for *solving problems* which happen to be on the current internal research agenda or suggested by some external application.[1] But conceptual and methodological innovations are inextricably bound to the search for and the discovery of proofs, thereby establishing links between theories, systematising knowledge, and spurring further developments. Proofs, I maintain, are the heart of mathematics, the royal road to creating *analytic tools* and catalysing growth. We are, as Bergson put it, *Homo faber*, the makers of tools, be they material or conceptual. But as tool makers, mathematicians are artists and artisans, guided by a deep sense of beauty and search for harmony. Before embarking on a general discussion of these issues, let me present two typical case histories, one drawn from number theory and the other from set theory. They illustrate the intricate role of proofs in generating mathematical knowledge and understanding, going way beyond their purely logical-deductive function.

[1] The interplay between individuals' creative vision and the socio-cultural factors in the choice of research topics is particularly complex, and will not concern us here.

Two Case Histories

In a letter to Euler dated June 7, 1742, the number-theorist Christian Goldbach (1690–1764) conjectured that every even integer greater than 6 is representable as a sum of two distinct odd primes. Euler expressed his belief in the correctness of Goldbach's conjecture, but wrote that he could not prove it. E. Waring, in 1770, also arrived at the Goldbach conjecture and added that every odd integer is either a prime or is a sum of three odd primes (Dickson [1919], Vol. I, p. 421). So far, the Goldbach conjecture is still unsettled, notwithstanding the efforts of many outstanding mathematicians. Curiously, whether the Goldbach conjecture turns out to be correct or not is of no known theoretical or practical importance. Nothing non-trivial seems to follow from the conjecture, except that for every n there is a prime p such that $n \leq p \leq 2n$ (for if $2n = p_1 + p_2$ one of p_i lies between n and $2n$). But this result is weaker than Chebychev's theorem which asserts the existence of a prime p strictly between n and $2n - 2$. Indeed, it is known that the number of primes between n and $2n$ is greater than $n/[3\log(2n)]$.

Another open problem in prime-number theory, with no overt logical relation to the Goldbach conjecture, is the twin-prime problem: do there exist infinitely many primes p such that $p + 2$ is also a prime, such as the pairs (3;5), (5;7), (11;13), *etc.* The first breakthrough on the Goldbach problem yielded also a *method* to attack thé twin-prime problem. In a short note published by Jean Merlin in the *Comptes Rendus de l'Académie des Sciences de Paris* in 1911 (communicated for publication by Henri Poincaré), Merlin outlined a sieve method which generalised the sieve of Eratosthenes (*fl.* 3$^{\text{rd}}$ century B.C.E.). The method was claimed to lead to a proof of both the twin-prime conjecture and the Goldbach conjecture. Jean Merlin was killed at the beginning of World War I, and Jacques Hadamard published in 1914 a lengthier manuscript found among the papers of Merlin. The proofs of Merlin turned out to be invalid. Did the matter end here? Why still talk about it, why call it a breakthrough? After all, Merlin was neither the first nor the last mathematician who presented an invalid proof of the Goldbach conjecture! The breakthrough consisted of inventing a new *method*, the Merlin sieve method. Though Merlin did not live long enough to rectify his claims and develop his method, the Norwegian mathematician Viggor Brun (1885–1978) recognised immediately the potentialities of Merlin's method, and in a series of papers starting in 1915, perfected the method and applied it successfully to a host of problems in number theory. (See Scriba [1980] for a biography of Brun.) The sieve method, as refined by Brun and appropriately now called 'Brun's sieve', enabled Brun to obtain *inter alia* the following results:

(a) There exist infinitely many integers n such that both n and $n + 2$ have at most nine prime factors;

(b) Every sufficiently large even integer is the sum of two numbers each having at most nine prime factors.

Brun's sieve method has been refined, extended and combined with other powerful methods in number theory. The literature on sieve methods (plural!) has grown to such an extent that a lengthy monograph by Halberstam and Richert [1974] was dedicated to surveying the state of the art. Though one still keeps an eye on the Goldbach and twin-prime problems, the development of sieve methods has become a subject in its own right, with applications to algebraic number fields, Latin squares, lattice theory, *etc.* Here, as normally happens in mathematics, one can say that the Goldbach problem acted as a catalyst, an impetus to remarkable developments due to the *search* for a proof. The sieve methods are not the only developments stemming from the Goldbach problem. In 1930 L. Schnirelmann (1905–1938) achieved another breakthrough on the Goldbach problem by combining the sieve method with his combinatorial density arguments, a method which he subsequently applied to other number-theoretical problems. As to the Goldbach conjecture, the famous Schnirelmann theorem of 1930 states that there exists a constant c such that every integer greater than 1 can be represented as a sum of at most c primes. From a value of $c \leq 800,000$ by Schnirelmann's original method, through subsequent refinements and further developments, the value has come down to $c \leq 6$. (See Wang Yuan [1984] for details.) The Goldbach problem has also catalysed further developments of the Hardy-Littlewood circle method, and notably the famous use of trigonometric sums in the theory of numbers.

Look at the treasure which attempted proofs of the Goldbach conjecture has produced, and how much less significant by comparison its ultimate 'truth value' might be! Think of what PYTHIAGORA would have deprived us by telling us whether the conjecture was true or false, or, what amounts nearly to the same thing, had Euler produced a two-line proof by a *reductio ad absurdum*. Now let us suppose that one day somebody comes up with a counter-example to the Goldbach conjecture or with a proof that there exist positive even integers not representable as a sum of two primes. Would that falsify or just tarnish all the magnificent theories, concepts and techniques which were developed in order to prove the now supposed incorrect conjecture? None of that. A disproof of the Goldbach conjecture would just catalyse a host of *new* developments, without the slightest effect on hitherto developed *methods* in an attempt to prove the conjecture. For we would immediately ask new questions, such as to the number of 'non-goldbachian' even integers: finitely many? infinitely many? If finite, best upper bound? structure? characterisation? and so on. New treasures would be accumulated alongside, rather than instead of the old ones—thus and so is the path of proofs in mathematics!

Let us turn now to the second case history, the continuum hypothesis

(CH). Whereas, as noted before, the Goldbach conjecture is not known to imply any new theorems, the continuum hypothesis is rich in consequences. Here again, the remarkable developments stemming from attempts to prove or refute CH overshadow, in the long run, the importance of the 'ultimate truth value' of the hypothesis (if, at all, it has a theory-independent truth value). In 1878, Cantor formulated his 'two-class theorem', stating that every uncountable subset of the set $\mathbb{R}$ of real numbers can be put in one-to-one correspondence with the set of all real numbers; in other words, there is no cardinal strictly between the cardinal of the set of natural numbers $\mathbf{N}$ and that of $\mathbf{R}$. Following Moore ([1990], p. 155), I shall refer to this statement as the *weak continuum hypothesis* (WCH). A second formulation, given by Cantor in 1883 (on the strength of the well-ordering theorem) states that the power of $\mathbf{R}$ (the continuum) is the same as the power of the set of all countable ordinals. This is the continuum hypothesis (CH), a statement equivalent to WCH (in ZFC). As is well known, Cantor did not succeed in proving CH using the arithmetic machinery of cardinal and ordinal numbers—a machinery he originally invented for dealing with a problem in Fourier analysis. He then turned to topological methods, opening unforeseeable vistas for future developments. Here Cantor obtained partial success in 1884 through the Cantor-Bendixon theorem from which it follows that WCH holds for all *closed* subsets of R: every uncountable closed subset of $\mathbb{R}$ has the same power as $\mathbf{R}$. Continuing the topological attack, W. H. Young proved in 1903 that WHC holds for all uncountable G_δ subsets of $\mathbb{R}$, followed by Hausforff's proof in 1916 that WCH holds for all infinite Borel sets. Further work on CH spurred many developments in topology by the Moscow school, contributing to the emergence of what is now known as descriptive set theory. Among its early highlights is Suslin's proof that WCH holds for all analytic sets. I shall not continue with an account of these and subsequent developments but just refer the reader to Moore [1989], [1990] and to Hallett [1984] for the history (plus explanation of technical terms used above), and to Woodin [1994] for the current state of the art.

A fascinating turning point occurred with Hilbert's *attempted* proof of the continuum hypothesis in his famous 1926 article 'On the Infinite'. For Hilbert, CH was a testing ground for the metamathematical methods he and his collaborators were developing.

> The final test of every new theory is its success in answering pre-existent questions that the theory was not specifically created to answer. By their fruits ye shall know them—that applies also to theories... The problem of the continuum is distinguished by its originality and inner beauty; in addition it is characterized by two features that raise it above other famous problems: *its solution requires new ways*, since the old methods fail in its case, and, besides, this solution is in itself of the greatest interest on account of the result to be determined. (Hilbert [1926]; p. 384 in van Heijenoort [1967]; italics added.)

The novelty in Hilbert's attack on the continuum hypothesis consisted in first replacing the real numbers by number-theoretic functions of the same cardinality—and then moving to the metamathematical level by replacing the functions by their *definitions* in a suitable logical system. With this move Hilbert confronts the logical problems of definability of objects by recursive schemes. Moreover, Hilbert adds a tacit axiom to the effect that *every set can be defined*, as Gödel keenly observed.[2] However, faithful to his philosophical program, Hilbert wished to reduce transfinite recursion to ordinary recursion in order to maintain the finitistic attitude of his proof theory. And thus, already on this account, the attempted proof was doomed to failure. Yet, as van Heijenoort ([1967], p. 369) points out:

> Hilbert's paper gave an impetus to the study of the hierarchy of number-theoretic functions and to that of the various schemas for the recursive definitions of functions. In particular, Hilbert's work provides an approach to the problem of associating ordinals with number-theoretic functions defined by recursion.

Exit Hilbert. Enter Gödel. After settling the completeness problem of the predicate calculus, a problem proposed in Hilbert and Ackermann ([1928], p. 68), Gödel turned his attention to carrying out Hilbert's program and proving the consistency of analysis by finitist methods. To reduce the difficulty of the problem, he first represented real numbers by arithmetic functions and these in turn by formulas, in the manner Hilbert attempted to prove CH. Running quickly afoul of the paradoxes connected with truth and definability, he arrived at his famous incompleteness theorem. (See Wang [1978], p. 183, and Wang [1981], p. 654.) Having already introduced non-finitary reasoning into metamathematics in the proof of the completeness theorem and thereby breaking with the Skolem and Hilbert injunctions, Gödel freely used ordinals in his work on CH. As Wang ([1974], p. 11) relates:

> With regard to the continuum hypothesis, Gödel attributes to a philosophical error Hilbert's failure to attain a definite result from his approach to the continuum problem. The approaches of Gödel and Hilbert are similar in that they both define, in terms of ordinal numbers, a system of functions (or sets) for which the continuum hypothesis is true. The differences are: 1. Gödel used all ordinals as given, while Hilbert attempts to construct them; 2. Hilbert considers only recursively defined functions or sets, while Gödel admits also nonconstructive definitions (by quantification).

Gödel himself discussed the link between Hilbert's attack on CH and his own consistency proof in a lecture held at Brown University in 1940 (see Gödel [1995] *Collected Works* III, p. 175).

[2] Reported by Wang [1981], p. 656. Here is the first link with Gödel's 'constructible' sets—a term Gödel chose for *definable* sets in order not to clash with other notions of definability.

The two case histories which I have just presented, namely that of the Goldbach conjecture and that of CH, are typical of the catalytic effect of proofs as vehicles of ideas. Such examples are commonplace. Quite frequently, mathematicians find themselves in the situation of Columbus: one sets out to find a route to India, misses the objective, and... discovers America! The case of Hilbert's attempt to prove CH with the indirect path leading eventually to Gödel's inner model of constructible sets teaches us that even an aborted proof, if containing innovative ideas, is not necessarily a dead end. An incorrect *derivation*, on the other hand, leads nowhere. It is important, therefore, to look closer at the difference between proofs and derivations.

Proofs *versus* Derivations

Let us fix our terminology to understand by *proof* a conceptual proof of customary mathematical discourse, having an irreducible semantic content, and distinguish it from *derivation*, which is a syntactic object of some formal system. Since 'derivation' is a technical term, it admits of a precise definition in the usual textbook fashion. Recall that a (linear) derivation in a formalised theory **T** is a finite sequence of formulas in the language of **T**, each member of which is either a logical axiom, or an axiom of **T**, or is the result of applying one of the finitely many explicitly stated rules of inference to previous formulas in the sequence. With some minor modification one similarly defines a tree derivation. A formula of **T** is said to be derivable if it is the end-formula of a linear or tree derivation. Furthermore, given a finite sequence of formulas in a formal system, there is a purely mechanical way for ascertaining whether the given sequence satisfies the conditions of being a derivation in the system. So far so good. On the other hand, when it comes to the term 'proof'—in the sense of an informal *conceptual* proof as used in this article—the situation is entirely different. Since the meaning and scope of the term 'proof' are not fixed by a technical definition, the subject of proofs is *par excellence* a topic for philosophical reflection and analysis. Indeed, as Detlefsen [1992b] writes in the preface, 'arriving at some understanding of the nature and role of proof becomes one of the primary challenges facing the philosophy of mathematics'.

The relation between proofs and derivations is in a limited sense analogous to the relation between the non-technical term of effectively computable function and the technical term of partially recursive function. *Church's Thesis* serves as a bridge between the intuitive and the technical notion of computability. In a similar vein it has been suggested to name *Hilbert's Thesis* the hypothesis that every conceptual proof can be converted into a formal derivation in a suitable formal system: proofs on one side, derivations on the other, with Hilbert's Thesis as a *bridge* between the two.[3] One immediately observes, however, that while Church's Thesis is a two-way bridge, Hilbert's Thesis is just a one-way bridge: from a formalised version of a given proof, there is no way to restore the original proof with all its semantic elements, contextual relations and technical meanings. Once we have crossed the *Hilbert Bridge* into the land of meaningless symbols, we find ourselves on the shuffleboard of symbol manipulations, and as these symbols do not encode meanings, we cannot return *via* the Hilbert Bridge and *restore* meanings on the basis of a sequence of symbols representing formal derivations. After all, it is the very purpose of formalisation to squeeze out the sap of meanings in order not to blur focusing only on the logico-structural properties of proofs. Meanings are now shifted to the metalanguage, as is well known. Metaphorically speaking, the relation between a proof and its formalised version is about the same as the relationship between a full-view photo of a human being and a radiograph of that person. Surely, if one is interested in the skeletal structure of an individual for diagnostic purposes, then the X-ray picture yields valuable information. But from a radiograph one cannot reconstruct the ordinary full-fledged view of the individual.

Let there be no misunderstanding. The study of structural properties of formalised proofs is a deep and important branch of mathematical logic, known as proof theory. (No pedantic insistence now on calling it derivation theory.) By a general consensus, mathematical logic is now considered part of mathematics and proof theory is a branch of mathematics, on par with, say, homological algebra. With the demise of Hilbert's program as originally conceived, important new lines of proof-theoretical research have emerged. (See Simpson [1988].) The study of proofs (in the sense of this essay) and the proof-theoretical study of derivations and related problems belong respectively to different methodologies. We render therefore unto proof theory the things which are proof theory's, and let philosophy of mathematics deal with the nature and function of conceptual proofs as they occur in actual mathematical practice.

Proofs as the Site and Source of Mathematical Knowledge

I. Methodology and Pure Logic in Meaning-Dependent Proofs

Proofs employ deductive reasoning; so do judicial rulings. In both cases logical inferences *cement* sequences of topic-specific claims and considerations. However, neither mathematical proofs nor legal rulings can be rendered intelligible by attending only to their deductive components.

[3] To avoid any misunderstanding, let me stress that I do not subscribe to Hilbert's Thesis. I just explore here its implications. See also the insightful articles of Vega [1993], [1995].

Proofs are the mathematician's way to *display the mathematical machinery* for solving problems and to *justify* that a proposed solution to a problem is indeed a solution. The word 'problem' is used here in a generic sense for any open question, in the manner one speaks of the famous Hilbert Problems of 1900. The problem might be an existing conjecture, like the twin-prime conjecture, or the problem of charting properties of some structures, or it may have been posed with some applications in mind. Frequently, problem and solution are the brain-child of one and the same person. We normally ask ourselves how to extend and refine an existing theory, method, technique, concept, and the like. It is the mark of creative mathematicians to propose interesting avenues for research and make a significant contribution toward the solution of the ensuing problems. But what does a solution consist of in a theoretical context? Recall the words of Hilbert concerning the continuum problem, saying that 'its solution requires new ways, since the old methods fail in its case'. Does *new ways* mean *new canons of logic*? Certainly not. The handful of rules of inference of a system of natural deduction ought to suffice. No additional rules of inference have ever been proposed for solving new problems. Moreover, one does not even think about rules of logic in writing or reading a proof, technical work in logic apart, but uses them in the manner in which Molière's Monsieur Jourdain speaks prose. A proof in mainstream mathematics is set forth as a sequence of claims, where the passage from one claim to another is based on drawing consequences on the basis of meanings or through accepted symbol manipulation, not by citing rules of predicate logic.[4] The argument-style of a paper in mathematics usually takes the following form: '...from so and so it follows that..., hence...; as is well known, one sees that...; consequently, on the basis of Fehlermeister's Principal Theorem, taking in consideration α, β, $\gamma, \ldots, \omega$, one concludes..., as claimed'. Why is it so difficult, in general, to understand a proof? Why does one need so much background information, training and know-how in order to follow the steps of a proof, when the purely logical skeleton is supposed to be nothing more than first-order predicate calculus with its few and simple rules of inference? A comparison with legal texts comes again to mind and deserves a closer look because of the many parallels with reasoning in mathematics.[5]

Logic, ever since Aristotle, has been concerned with valid inferences of

[4] In the same spirit, Arbib ([1990], p. 55), writes: 'In fact, the usual proof generated by a mathematician does not involve the careful application of a specifically formalised rule of inference, but rather involves a somewhat large jump from statement to statement based on formal technique and on intuitions about the subject matter at hand.'

[5] Notice how even some of the phrasings of judicial rulings and mathematical arguments are analogous: the one refers to precedents, the other to known theorems, and so on. Also, see the article of Alchourron and Martino [1987] and other articles in the same volume dealing with legal reasoning.

argument forms, while accounts of arguments in terms of their intertextual contexts have remained outside its scope. The situation will hopefully change because of work in linguistics, artificial intelligence and cognitive science. As things stand now, we have remarkable mathematical theories of formal logic, but inadequate logical theories of informal mathematics. (Cf. Corcoran [1973] for concrete examples of gaps in logical theories.) As to the importance of logic for mathematics, I certainly do not wish to imply in the manner of Poincaré[6] that mathematical knowledge cannot be extended by means of logical inferences. I think Poincaré sought refuge in outmoded Kantian conceptions of logic because it was congenial to his own geometric and intuitive ways of thinking. On the other hand, to algebraic spirits, logical inferences are definitely productive in extending knowledge by virtue of bringing to light otherwise unsuspected connections. Consider a simple example: we do not have to postulate that a group contains a *unique* identity element. It suffices to postulate that such an element exists, and then derive its uniqueness on the basis of the other group axioms. And that constitutes knowledge, simple as it is. Standard algebraic symbol manipulations can readily be rewritten as formal derivations, hence computer programs can be developed for symbolic calculations. Obviously, the results of such calculations constitute knowledge. (Why else bother?) To return to the main point, Poincaré did however raise an important issue concerning the non-logical parts of a mathematical proof. But the viewpoint developed in this essay is rooted in a different perspective.

In reading a paper or monograph it often happens—as everyone knows too well—that one arrives at an impasse, not seeing why a certain claim B is to follow from claim A, as its author affirms. Let us symbolise the author's claim by '$A \rightarrow B$' . (The arrow functions iconically: there is an informal logical path from A to B. It does *not* denote formal implication.) Thus, in trying to understand the author's claim, one picks up paper and pencil and tries to fill in the gaps. After some reflection on the background theory, the meaning of the terms and using one's general knowledge of the topic, including eventually some symbol manipulation, one sees a path from A to A_1, from A_1 to $A_2, \ldots$, and finally from A_n to B. This analysis can be written schematically as follows:

$$A \rightarrow A_1, A_1 \rightarrow A_2, \ldots, A_n \rightarrow B.$$

Explaining the structure of the argument to a student or non-specialist, the other may still fail to see why, for instance, A_1 ought to follow from A. So again we interpolate $A \rightarrow A'$, $A' \rightarrow A_1$. But the process of interpolations for a given claim has no theoretical upper bound. In other words, how far has one to analyse a claim of the form 'from property A, B follows'

[6] For a penetrating analysis of Poincaré's position, see Detlefsen [1992a], [1993].

before assenting to it *depends on the agent.*[7] There is no theoretical reason to warrant the belief that one ought to arrive at an atomic claim $C \rightarrow D$ which does not allow or necessitate any further justifying steps between C and D.[8] This is one of the reasons for considering proofs as *infinitary objects.* Both Brouwer and Zermelo, each for different reasons, stressed the infinitary character of proofs. Kreisel ([1970] footnote 22, p. 511) cites the appropriate references and notes (with respect to the insight that proofs are of infinite character) that 'properly interpreted, Gödel's theorems can be used to *support* this insight, just as they are used to refute Hilbert's *assumption* that finite formal derivations reflect faithfully the structure of mathematical reasoning' (Kreisel's emphasis).

II. '*Was sind und was sollen die Axiome?*' or Where Are the Axioms?

So far I have talked about proofs without mentioning theorems. But aren't theorems the essence of a mathematical research paper while proofs serve only the subsidiary function of deducing theorems from axioms? Indeed, the *standard view* in philosophical writings seems to be that mathematical knowledge resides in a body of theorems (propositions, sentences), whereas the function of proofs is to derive theorems from first principles, true axioms, and thus confer truth on the theorems. Or, in a less Aristotelian fashion, proofs serve *only* to validate theorems on the basis of accepted axioms. No doubt that the 'standard view' is neat and philosophically satisfying. Its major drawback is that it does not fit mathematical practice, nor is it capable of explaining the source of mathematical knowledge and the dynamics of its growth (see Kitcher [1981] and [1984]). Thurston ([1994b], p. 162) even dubs the 'standard view' a 'caricature [of] the popular model'. Let us look at some typical examples which bring out the ill-foundedness of the 'standard view', putting conceivable set theoretical reductions aside for a moment.

[7] The process of 'arrow interpolations' can be modelled as a *dialogue* (cf. Mackenzie [1980] and [1981]; Ernest [1995]). The length of a dialogue depends, of course, on the interlocutors.

[8] Nor do we have any guarantee that a lengthy mathematical argument can be arranged in a neat linear chain as the above schematisation might suggest. Mathematics does not escape the circularity predicament of dictionary definitions, valiant efforts in both cases notwithstanding. Thus Steinbring ([1991], p. 505) writes:

> Bernoulli's theorem required the abandonment of a supposedly deductive point of view in the development of knowledge and theory: what probability is can only be explained by means of randomness, and what randomness is can only be modelled by means of probability. This is where one accedes to those problems in the theoretical foundations of mathematics which, in a modern perspective, have become known as the *circularity of mathematical concept definitions*... This *circularity* or *self-reference* implies that knowledge must be interpreted, at all stages of its development, as a complex structure which cannot be extended in a linear or deductive way, but rather requires a continuous, qualitative change in all the concepts of a theory. (Italics in original.)

(1) *Matrix theory.* The term matrix first appeared in an article by Sylvester in 1850; but the topic grew from prior concern with determinants. Today, matrix theory is a vast subject of importance both in pure mathematics and for its applications to such diverse fields as quantum mechanics, game theory, economics—to name just a few. No axioms have ever been proposed for even a fragment of matrix theory. It is a typical unaxiomatised theory. What is then the logical status of its extensive results?

(2) *Graph theory and combinatorics.* Both have long histories, with roots in recreational mathematics, chemistry (Cayley) and physics (Kirchhoff). In the first standard text on graph theory by König [1936], its author mentions just one axiom, and significantly, puts the word axiom in quotation marks. Indeed, the axiom in question is just a more elaborate and abstract version of Euclid's postulate permitting points to be joined by a line. Once more we have an unaxiomatised theory, rigorous nonetheless, on the frontier of current research, with multiple applications, including to mathematical logic! The close relative of graph theory, algebraic topology, is likewise not axiomatically treated, definitions apart.

(3) *Probability theory.* Probability theory originated as early as the fifteenth century (Pacioli, Galileo, *etc.*) in analyses of games of chance and rapidly developed into a significant mathematical theory. Yet an axiomatic foundation was first proposed in the famous monograph of Kolmogorov in 1933. And yet, Kolmogorov's five axioms serve little for a *logical* foundation of probability theory in the sense that all its theorems could be deduced from these axioms. Rather, the significance of Kolmogorov's monograph consists in making probability theory a branch of measure theory, with its specific emphases and applications. As to measure theory, apart from various definitions of measure, it has never been axiomatised.[9]

(4) *Number theory.* Once more, a non-axiomatised theory! Notice that I am talking about number theory as the term is understood by the general mathematical community—not to be confounded with first-order or fragments of second-order axiomatised Peano arithmetic, which is a branch of mathematical logic.[10] As a matter of fact, the Queen of Mathematics—as Gauss called number theory—is rather promiscuous, opening her arms to algebraic, analytic, topological, geometrical, proof-theoretical, numerical, model-theoretical, combinatorial, and come as they may types of proofs and methodologies. Categorically, the Queen

[9] See the previous footnote.

[10] The book by Smorynski [1991] is typical of work in Peano arithmetic, while, for instance, the book of Yuan Wang [1984] about the Goldbach conjecture typifies work in number theory.

disdains being degraded to the rank of a recursively axiomatisable theory. *Noblesse oblige!*

(5) *Group theory.* Evariste Galois (1811–1832) introduced the term *le groupe*, but group theory had a long prior history, with origins in geometry, number theory and the theory of equations.[11] Starting with groups of transformations and permutations, the abstract concept of group became standard only in the 1880s, defined as a collection of elements with a binary operation $\circ$ and a distinguished identity element e satisfying the following axioms:

(i) $$(\forall x)(\forall y)(\forall z)[x \circ (y \circ z) = (x \circ y) \circ z];$$

(ii) $$(\forall x)[e \circ x = x];$$

(iii) $$(\forall x)(\exists y)[y \circ x = e].$$

Thus, group theory can be formalised as a first-order theory and, as such, has been extensively studied by logicians.[12] But behold: the metamathematical methods used in studying the first-order theory of groups are themselves not axiomatised! Furthermore, the standard theorems of group theory that one finds in books and papers on group theory are not even expressible in first-order predicate calculus.[13] One just has to think about such fundamental concepts as normal subgroup, torsion group, finite group, composition series, or such famous theorems such as the Sylow theorems about p-groups, the Jordan-Hölder theorem[14] and the like, to realise that the implicit underlying logic of mainstream group theory is second-order logic.[15] But as there is no complete and

[11] See Kline [1972], pp. 764–770 and pp. 1137–1146 for an overview of the history of group theory. A detailed account can be found in Wussing [1984 (1969)].

[12] One of the earliest applications of logic to group theory goes back to 1948 with Tarski's theorem to the effect that first-order group theory is undecidable, whereas the theory of abelian groups is decidable, as was shown by Tarski's doctoral student, Wanda Smielew. Hodges [1985] discusses many applications of model theory to group theory, including the use of infinitary logic, and word problems.

[13] Observe the following: turning the crank of the deductive machinery of first-order predicate logic upon the first-order axioms of group theory will produce a potentially infinite number of formulas which count as theorems of first-order group theory. But hardly any of these formally derived theorems would be found as a theorem in the immense literature on group theory. Why? (Rhetorical question) This ought to stir the slumber of those who still think of mathematicians as deduction machines rather than creators of beautiful theories and inventors of methods and concepts to solve humanly meaningful problems.

[14] For terminology, see Rotman [1973].

[15] The arguments of this and the previous examples bring just a few more sacks to the mill of Shapiro [1991] who has cogently argued that the underlying logic of mathematical practice is second-order logic.

effective deductive system for a second-order logic, we are left with the question of how to account for the validity—or truth, if this is your preferred locution—of the group-theoretical methods and results, be they of metamathematical or mainstream nature. Are we going to affirm that the axioms of group theory are bearers of validity (or truth) and thus confer validity (or truth) via a non-effective logic to the theorems of group theory? Certainly not, for the group axioms are just *definitiones quid nominis*. Recall that we have momentarily put aside any consideration about reductions to set theory.[16] But even if one considers developing the theory of groups within ZFC set theory, one can legitimately ask what was the status of, say, the Sylow theorems when they were proven in 1872, prior even to Cantor's first publication on set theory. And if we discover one day an inconsistency in ZFC, do the Sylow theorems lose thereby their validity? And once the inconsistency is remedied after some labour and set theory is appropriately modified, will then the Sylow theorems regain validity lost? The answer is clear: the 'standard view', that the function of proofs is to deduce theorems from 'true' axioms, is untenable.

Examples of non-axiomatised theories in actual mathematical practice are the rule—geometry is the exception. Thus, Fair ([1984], p.366) writes:

> Mathematicians have "informal notions" or "intuitions" about what particular mathematical objects are like with regard to their essential or defining characteristics. They often have proceeded with the business of theorem-proving in the total absence of any explicitly stated axioms. This fact is at least a prima facie embarrassment to the thesis, "Mathematics is the science of formal systems". [Reference to Curry.] Euclid's work in number theory could hardly be described as deducing consequences from the Peano axioms first articulated in the nineteenth century.

In talking about the axiomatic method in mathematics, one has to distinguish between several variants and versions:

(i) The clearest is no doubt the notion of a first-order axiomatised theory in the sense of model theory. The logical axioms and rules of inference fix the deductive machinery, and the non-logical axioms fix the intended subject matter of given theory **T** under investigation. The axioms of a formalised theory serve as a *basis* for deriving theorems. The term 'basis' is chosen here by analogy with a basis of a vector space. Just as any vector is a linear combination of basis vectors, a theorem of **T** is a 'logical combination' of axioms. As the axioms in a formalised theory are strings

[16] Cf. Mac Lane [1992], p. 122 :

> Set theory, like the rest of mathematics, is protean, shifting and working in different ways for different uses. *It is subordinate to mathematics and not its foundations.* The unity of mathematics is real and depends on wonderful new connections which arise all around us. (italics mine)

of symbols, syntactic objects, the issue of their truth is vacuous, and so is the issue of the truth of formulas derived from the axioms. The technical Tarskian concept of 'true in a model' (as standing for 'satisfiable') is the sole context in which one can legitimately speak of truth in mathematics without committing a 'category mistake'. All other talk about truth of mathematical statements is *metaphorical*, and as such, is unproblematic.[17]

(ii) Besides axioms in a formalised theory, one also speaks of axioms which define (informally) an abstract structure, such as the axioms of a group, ring, field, vector space, topological space, *etc.* Here again the question of validity or truth of the axioms is not meaningful; the axioms function just as definitions, *definitiones quid nominis.* In other words, from the current structuralist conception of mathematics, such axioms fix the boundaries of an informal theory but do not impart it with a logical foundation in the Aristotelian sense of 'first principles'.

(iii) Between these two cases, axioms of geometries occupy an intermediate place.[18] Clearly, axioms of this category do fulfil a deductive role; indeed, the 'standard view', fashioned with the Euclidean axioms and postulates in mind, is referred to as the 'Euclidean programme' in the pungent criticism by Lakatos [1962]. Yet with the advent of non-Euclidean geometries, any conceivable justification for categorising geometric axioms as true has lost its ground. Thus, Kline ([1953], p. 9) writes:

> Mathematics is a body of knowledge. But it contains no truths... Not only is there no truth in the subject, but theorems in some branches contradict theorems in others. For example, some theorems established in geometries created during the last century contradict those proved by Euclid in his development of geometry. Though devoid of truth, mathematics has given man miraculous power over nature.

III. The Epistemic Function of Proofs

We have arrived at the core of the epistemological puzzle: what confers validity on theorems, or more generally, on mathematical methods and results? As repeatedly stressed, the Aristotelian concept of a deductive science is embrangled with insuperable difficulties, incapable of accounting

[17] I take it as a metaphorical use of 'true' when Thomas ([1990], p. 80) writes:

> A public [mathematical] statement is regarded as true when the mathematical community can be convinced that it has been properly deduced from what is already explicit in the public mathematics. Note that the truth of a public statement does not depend upon any correspondence of it with a state of affairs in a mathematical 'realm'. Semi-Platonism is irrelevant; even if all the many things that mathematicians have from time to time invented were located (even metaphorically) anywhere, it would make no difference to mathematical practice.

See also Thomas [1991] for the priority of meaning in mathematics.

[18] For a current discussion of the axiomatic method in geometry, see the articles in Henkin *et al.* [1959].

for the validity of theorems in mathematics.[19] Are we then left with the conclusion that the totality of mathematical theorems and methodologies is ill-founded unless we wave the set-theoretical *foundation* flag and express the pious hope that—at least in principle—every mathematical theory can be *formalised* in ZFC or in some similar theory? I dare say this is a pious hope, for no metamathematical *proof* has ever been advanced to justify the formalisation credo.[20] And as I have already asked before, even granting for argument's sake the possibility of such a formalisation, did mathematics created *prior* to the invention of set theory lack validity or will it be so if, per chance, ZFC turns out to be inconsistent? No doubt, mathematical knowledge is solidly soldered, but it is futile to seek foundations for mathematics *in its entirety* in another mathematical theory, be it set theory or category theory.

There is a way out of the foundational difficulty, and it consists of realising that *proofs rather than the statement-form of theorems are the bearers of mathematical knowledge.* Theorems are in a sense just tags, labels for proofs, summaries of information, headlines of news, editorial devices.[21] The whole arsenal of mathematical methodologies, concepts, strategies and techniques for solving problems, the establishment of interconnections between theories, the systematisation of results—the entire mathematical know-how is embedded in proofs. When mathematicians pick up a paper for study, they turn their attention to the proofs, since proofs are the centre of gravity of a research paper. Theorems indicate the subject matter, resume major points, and as every research mathematician knows, they are usually formulated *after* a proof-strategy was developed, after innovative ideas were elaborated in the process of 'tossing ideas around'. Proofs are for the mathematician what experimental procedures are for the experimental scientist: in studying them one learns of new ideas, new concepts, new strategies—devices which can be assimilated for one's own research and be further developed. Needless to stress that in studying proofs—or experimental procedures—we are also engaged in a cumulative collective verification process. Think of proofs as a network of roads in a public transportation system, and regard statements of theorems as bus stops;

[19] See Beth [1968], chap. 2, for an exposition and criticism of the Aristotelian conception. Cf. also the epoch-making attack by Lakatos [1962] on deductivism in mathematics.

[20] To avoid any misunderstanding: certainly, it is one of the many values of set theory that most of our current mathematical theories can be *expressed* in first-order set-theoretical *language*. This, however, does not imply that all our current *conceptual proofs* of informal mathematics can be *formalised* as *derivations*, as claimed by the Hilbert Thesis. Recall just the problem of 'arrow interpolation'; see also footnote 8.

[21] It is noteworthy that words like theorem, proposition, or the like appear nowhere in Descartes's *La Géométrie*; his book consists of a continual unfolding of methods. Euler rarely uses the term *propositio*; his usual phrasings are *problema—solutio—exemplum*, with an occasional *corollarium—scholium*. Such examples are quite typical of pre-nineteenth century texts.

the site of the stops is just a matter of convenience.

Let me illustrate the epistemic function of proofs by three examples. As a first example, consider Euclid's Proposition 20 (Book IX)[22] which states: 'Prime numbers are more than any assigned multitude of prime numbers'. In modern notation, the statement claims that given prime numbers $p_1, p_2, \ldots, p_n$, it is possible to find a prime number q distinct from the primes $p_1, p_2, \ldots, p_n$. The idea of Euclid's proof is to consider the number

$$N = p_1 p_2 \ldots p_n + 1$$

and argues that either N is a prime, in which case it could not be equal to any of the p_i $(1 \leq i \leq n)$; or else, since it was shown that every composite number has a prime factor (Prop. 31 of Book VIII), N is divisible by a prime q. The proof concludes with the observation that again q could not be any of the p_i (else it would divide 1). Hence there is always a prime distinct from any given number of primes. *q.e.d.* Clearly, the key idea of *forming the number N* does not follow *logically* from any previous proposition or conceivable arithmetic axiom.[23] It is a purely creative, topic-specific move; this move, simple as it is, constitutes a contribution to mathematical knowledge which goes beyond the statement of the proposition. Indeed, by the same *method* as in forming the number N one proves that there are infinitely many primes of the form $4n + 3$.[24] Furthermore, Euclid's idea of forming $p_1 p_2 \ldots p_n + 1$ was used by Gödel in order to show that the function $P(n)$ taking the n^{th} prime number as its value is [primitive] recursive. (See Gödel in van Heijenoort [1967], p. 604, formula 5).

There are various other ways of proving Euclid's Proposition 20, each proof setting forth concepts and methods which are not part of the formulation of the proposition. By way of illustration, consider the following formula of analytic number theory:[25]

$$\sum_{p \leq x} \frac{1}{p} = \log \log x + C + O\left(\frac{1}{\log x}\right).$$

It follows from this formula that there are infinitely many prime numbers, for the term on the right-hand side is unbounded, whereas if the number of primes were finite, the left-hand-side summation would be bounded.

[22] Heath [1956], vol. 2, p. 412.

[23] Notice, apropos first-order logic, that the numeral corresponding to the number $p_1 p_2 \ldots p_n + 1$ cannot be expressed by a single formula in first-order Peano arithmetic (because of the parameter 'n' in the term).

[24] Put $N = 4[(4n_1 + 3)(4n_2 + 3) \ldots (4n_k + 3)] + 3$. If N is composite, not *all* prime factors of N could be of the form $4m + 1$, else their product would also be of that form.

[25] Cf. Rademacher [1964], p. 120.

But the formula yields more information about the infinitary character of the number of primes than does Euclid's proof: for the formula implies that the series on the left-hand side *diverges*, and this in turn has various number-theoretical implications. Proofs, we conclude, contain significant topic-specific information going beyond the statement incorporated into the formulation of a theorem. Or to speak metaphorically, *theorems are the headlines, proofs are the inside story.*

My second example comes from the theory of finite groups and concerns one of the oldest theorems in the field, namely, the theorem of Lagrange:[26] 'If $\mathcal{G}$ is a finite group of order g and $\mathcal{H}$ is a subgroup of $\mathcal{G}$ of order h, then h divides g'. (Recall that the order of a group is the number of its elements. We use capital Roman letters for group elements, 'Id' for the identity element, and juxtaposition for the group operation.) Here are the steps of the proof. Consider complexes of the form $\mathcal{H}X$,[27] called right-cosets of $\mathcal{H}$, consisting of all products HX, with X a given element of $\mathcal{G}$, and H running through the elements of $\mathcal{H}$. One first shows:

Step (1): Any two right-cosets are either disjoint or coincide.

Step (2): Any right-coset $\mathcal{H}X$ has as many elements as $\mathcal{H}$, namely h.

Step (3): There exist elements $X_1 = \text{Id}, X_2, \ldots, X_k$ in G such that every element of $\mathcal{G}$ belongs to one of the distinct cosets $\mathcal{H}X_i$ where $1 \leq i \leq k$.

From these steps it follows that $\mathcal{G}$ is partitioned into k disjoint cosets of h elements each, hence $n = hk$, as claimed by Lagrange's theorem. This short proof is a good example of how a key concept—that of cosets—is intertwined through logical argumentation with methodological steps to yield the arithmetical relation as stated in the theorem. Each step requires a separate justification, based on the concepts involved. Step (3) is established with the aid of mathematical induction, a conceptual machinery belonging to arithmetic, and the final conclusion, linking the three steps, also depends on a theory of arithmetic. Here, the arithmetical machinery is called upon as a *subproof*, in the manner in which *subprograms* function in computer programming. All told, one sees that there is more technical information, more mathematical knowledge embodied in the whole proof with all its methodological links and inter-theoretical connections than in the statement of the theorem.

The third example to be discussed concerns Fermat's Last Theorem

[26] The theorem appears in a lengthy paper on the theory of equations and concerns the structure of *permutations*, the prototype and progenitor of the abstract group concept. See Joseph Louis Lagrange: '*Réfléxions sur la résolution algébrique des équations*' [1771] *Œuvres*, vol. 3, pp. 205–421, and the historical discussion in Wussing [1984], pp. 77–79. Notice that the statement of Lagrange's theorem is not even expressible in the language of first-order group theory, not to speak of deriving it from the group axioms.

[27] The term 'complex'—still in use—predates set-theoretical terminology, and means the same thing as *subset*. Thus, $\mathcal{H}X$ is a subset of $\mathcal{G}$.

(FLT). The story of this example will be a bit longer, but worth telling because of its ample epistemological implications.

The famous affirmation written by Pierre de Fermat *circa* 1637 states, in modern terminology, that the diophantine equation

$$x^n + y^n = z^n$$

has no solution in positive integers if $n > 2$.[28] Since the case $n = 4$ is easy to dispose of, one readily sees that it suffices to consider the Fermat equation when the exponent n is an odd prime p (see Edwards [1977] or Ribenboim [1979] for historical and technical details).

Fermat's Last Theorem counts as one of the most widely known mathematical problems. Simple to state, with prizes and fame having awaited whoever would prove it, FLT has for centuries opened the door for amateurs to rush in where masters feared to tread. When in 1816 a friend has suggested to Gauss to compete for the prize which the Paris Academy had proposed for a proof of FLT, Gauss wrote back: 'I am very much obliged for your news concerning the Paris prize. But I confess that Fermat's Theorem as an isolated proposition has very little interest for me, because I could easily lay down a multitude of such propositions, which one could neither prove nor dispose of.' (Quoted by Bell [1937], p. 261). Gauss foresaw correctly that major advances would first have to be made in algebraic number theory before any light could be shed on the Fermat conjecture. Gauss further elaborated in his letter: '... if I succeed in taking some of the principal steps in that theory, then *Fermat's Theorem will appear as only one of the least interesting corollaries.*" (Italics added.) And indeed, that turned out to be the case. Work on the Fermat conjecture resulted in the creation of the theory of ideals by Kummer, catalysing major subsequent advances in algebraic number theory. Nonetheless, only very special cases of FLT were settled with these powerful theories. Indeed, showing that an isolated diophantine equation, like the Fermat equation, does or does not admit a solution is of little significance for the growth of mathematical knowledge. What Gauss apparently had in mind was the creation of a *general theory* of diophantine equations. As a step in this direction, Hilbert proposed in his famous Paris lecture of 1900 as Problem Number 10 to find a general method—an algorithm—for determining, by a finite number of operations,

[28] It is known since antiquity that a square can be written as a sum of two squares (Pythagorean triplets). Fermat wrote in the margin of his copy of Diophantus, where this problem is given, the following famous words:

> On the other hand, it is impossible for a cube to be written as a sum of two cubes or a fourth power as a sum of two fourth powers or, in general, for any number which is a power greater than the second to be written as a sum of two like powers. I have a truly marvelous demonstration of this proposition which this margin is too narrow to contain. (Cf. Edwards [1977], p. 2)

the solvability or unsolvability in integers of an arbitrary diophantine equation with any number of unknowns and with integer coefficients. With more than half a century of developments in mathematical logic to build upon, Yuri Matiyasevich succeeded in 1969 in proving that no such algorithm can be found.[29] Using the techniques of Matiyasevich and those of other contributors, Baxa [1993] constructed a polynomial diophantine equation in 20 variables which has no solution in non-negative integers if and only if the Fermat exponential diophantine equation

$$x^{t+3} + y^{t+3} = z^{t+3}$$

has no (non trivial) integral solutions in the variables x, y, z, t. The reduction of the Fermat equation—which is exponential with arbitrary exponents n—to a polynomial equation is significant, though this method has not, for the time being, yielded a proof of FLT. (My refrain: a method, like virtue, is its own reward.)

Let us look at other approaches. Traditionally, FLT is split into two cases. The first case is said to hold if there is no primitive solution to the Fermat equation in integers x, y, z coprime to p. Case II holds if there is no primitive solution with p dividing xyz. One of the earliest results on FLT is a theorem of Sophie Germain (1832) which states that the first case of FLT holds for an exponent p if $2p+1$ is also a prime number. Thus, for example, Case I holds for $p = 3$, $p = 5$, but Germain's theorem gives no information for $p = 7$. Her method was the first general attack on FLT. With the development of high-speed computers, numerical methods were developed which enabled efficient numerical verifications of FLT up to a certain power. Thus Wagstaff showed in 1978 that FLT holds for all exponents $n \leq 125000$, and Lehman showed in 1981 that Case I holds for all $p \leq 6 \times 10^9$ (see Heath-Brown [1985b] for references). Note that the numerical approach to FLT required first the development of special number-theoretical and numerical methods, for a brute-force numerical attack could never prove that for a given exponent n there is no solution: one cannot just try out numerically all triplets x, y, z; for there are infinitely many to check.

Important advances over the last 15 years in algebraic geometry and in analytic number theory yielded as a by-product new ways for studying the Fermat equation. First, Faltings [1983] stunned the mathematical world with his proof of Mordell's conjecture (1922) concerning rational points on curves of genus ≥ 2. It follows as a corollary from the Mordell-Faltings theorem that for a fixed $n > 2$, the Fermat equation can have at most a finite number of solutions. Elaborating further, Heath-Brown [1985a] showed that FLT holds for 'almost all' exponents n. That means that if $N(x)$ is the number of $n \leq x$ for which FLT fails, then $\lim_{x\to\infty}\frac{N(x)}{x} = 0$.

[29] Cf. Matiyasevich [1993] for details and recent developments of his method.

Still, FLT could fail for infinitely many exponents n. Coming from an entirely different direction, the researches of É. Fouvry in analytic number theory enabled him to apply his methods to obtain a sharp estimate in an inequality studied by Adleman and Heath-Brown [1985], thereby settling Case I of Fermat's Last Theorem *for infinitely many exponents* (see Fouvry [1985]). This is the first time in the history of the Fermat conjecture that a proof for one of the two cases was obtained for infinitely many exponents (see the expository article by Heath-Brown [1985b]).

The crowning triumph over the Fermat gadfly belongs to algebraic geometry, in particular to the theory of modular elliptic curves—a topic of intensive research since the fifties (see Lang [1995]). The remarkable connection between Fermat's Last Theorem and the theory of elliptic curves was first established by Hellegouarch [1972] who associated with the Fermat equation

$$\text{(F)} \qquad a^p + b^p = c^p$$

(with $p > 3$, a, b, c relatively prime) an elliptic curve of the form

$$\text{(E)} \qquad y^2 = x(x - a^p)(x + b^p).$$

(Permuting a, b, and c, changing sign if necessary, one can assume that b is even and $a \equiv -1 \pmod 4$). This connection was discussed again in an Oberwolfach lecture by G. Frey in 1985 who sketched an intricate argument from which it would follow that the semistable elliptic curve (E) was *non-modular*. Since a famous conjecture of Shimura and Taniyama states that every elliptic curve over $\mathbf{Q}$ is modular, the existence of the Hellegouarch-Frey curve (E) contradicts the Shimura-Taniyama conjecture.[30] Hence a proof of the Shimura-Taniyama Conjecture would imply the non-existence of the Hellegouarch-Frey curve (E), and hence the non-existence of a solution to the Fermat equation (F). The argument of Frey [1986] was completed with significant additional results by Ribet [1990], thereby proving conclusively:

(R) Shimura-Taniyama Conjecture → Fermat's Last Theorem.

Though as noted before, FLT is insignificant (historical interest apart), the Shimura-Taniyama conjecture is, in the words of Lang [1995], 'one of the most important [conjectures] of the century'. One can thus understand the great excitement in the audience when in his famous Cambridge lecture of June 1993, Andrew Wiles announced that he has succeeded in proving the

[30] See Ribet [1995] for details and bibliographical references. Important background information about the history of the Shimura conjecture is in Lang [1995].

Shimura-Taniyama conjecture. The theory which Wiles developed for proving the Shimura-Taniyama conjecture fills over one hundred printed pages (see Wiles [1995]). Fermat's Last Theorem follows now by *modus ponens* from the Shimura-Taniyama-Wiles Theorem and (R). The report by Ribet [1993] of Wiles's epoch-making proof ends with the following significant words:

> Wiles's proof of Taniyama's conjecture represents an enormous milestone for modern mathematics. On the one hand, it illustrates dramatically the power of the abstract 'machinery' we have amassed for dealing with concrete Diophantine problems. On the other, it brings us significantly closer to the goal of tying together automorphic representations and algebraic varieties.

Let us take stock. The starting point of my third example was an open problem: to determine whether a certain diophantine equation, the Fermat equation, admits solutions in positive integers. I have mentioned diverse methods and theories which have been developed in order to settle the Fermat conjecture, notably methods of algebraic number theory, numerical analysis, diophantine representations, density arguments, tools from analytic number theory, and finally, the intricate theory of modular elliptic curves. With the exception of the proof *via* the Shimura-Taniyama conjecture, none of these approaches settled FLT, yet each attempt enriched mathematics with new concepts and techniques. Without consulting the proofs, no list of theorems could convey the links, inter-theoretical connections, strategies and overall mathematical knowledge embodied in these methods. The passage from equation (F) to the elliptic curve (E) is particularly instructive: it is neither a theorem nor the result of applying a rule of logic. As I keep stressing, such topic-specific moves are standard in mathematical discourse and are habitually introduced with the innocent looking imperative 'Let...', or 'Consider...'. I have referred to such steps as *moves* by analogy to moves in a game of chess. Moves are made in conformity to the rules of the game, but no rule ever suggests which is the appropriate move to be made in a given situation. In the first example with Euclid's proof, the key move consists in considering the number $p_1p_2\dots p_n+1$; in the proof of Lagrange's theorem, the crucial step resides in introducing cosets and decomposing a group as a direct sum of right-cosets. Such typical moves are always *part of a proof* and bring to light the *intentional* components in a proof: they have no independent logical justification other than serving the purpose of constructing bridges between the initially given data, or between some intermediate steps, and subsequent parts of the argument. But the bridges are conceptual, not deductive in the sense of logic. In the example of Euclid's proof, the initial data are the given primes p_1, p_2, ..., p_n. We construct the 'bridge' by considering the number $p_1p_2\dots p_n+1$; and only *then* argue that this number is either a prime or divisible by a prime distinct from any of the p_i. In the proof of

Lagrange's theorem, the decomposition into cosets is a construction with the *purpose* to relate the number of elements in a group with the number of elements in a subgroup. Such constructions are, as already mentioned, transferable 'technologies' to other proofs. Whereas Euclid could still list a finite number of postulates upon which his constructions are based, we are not any more in a position to set forth such a list: in general, constructions in the course of a proof are creative moves *ab initio*. Once more we see how misleading the Euclidean model can be in the epistemology of mathematics. To return to the Hellegouarch-Frey curve (E), needless to say that it does not suffice just to write down the elliptic curve (E) with a, b and p as parameters coming from (F). The crux is to show that (E) has certain properties, namely, that it is a semistable *non-modular* elliptic curve. The argument turned out to be so intricate, with numerous intermediate constructions and links to be established, that Frey had to leave parts of the proof to be completed by experts in the theory of modular curves—a challenge met by Ribet [1990].

Fermat's Last Theorem is a statement about natural numbers, a system considered to be situated at the very bottom of the mathematical hierarchy—one recalls Kronecker's famous aphorism.[31] On the other hand, the proof of FLT by Andrew Wiles *via* the Shimura-Taniyama conjecture brings into play some of the most advanced and intricate mathematical theories, and hence is situated on the top of the mathematical hierarchy. It is a most remarkable discovery that the assumed existence of relatively prime integers a, b, c and a prime $p > 3$ such that $a^p + b^p = c^p$ contradicts the statement that every semistable elliptic curve over $\mathbf{Q}$ is modular. This link was revealed through 'a marvellous proof'—but not the one Pierre de Fermat thought he had found! Could the development of mathematics be conceivable without proofs, the generators and very *carriers* of mathematical knowledge? But there still remains the question of how secure the carriers are. This will be our next concern.

The Reliability of Mathematical Knowledge

Consider the construction of a skyscraper. In order to secure the stability of the edifice, it has to be seated on solid foundations and erected stagewise, level after level, from the bottom to the top. Call the model of such a structural stability and reliability *skyscraper grounding*.

The construction of a spaceship, on the other hand, is rather different. It is fabricated out of numerous components, each component being separately manufactured and tested for correct functioning and reliability. The spaceship as a whole is an assemblage of the individual components,

[31] '*Die ganzen Zahlen hat der liebe Gott gemacht, alles andere ist Menschenwerk.*' (The whole numbers were made by the good Lord, all the rest is works of humans.) Reported by H. Weber in *Math. Ann.* **43** (1893), p. 19.

constructed under the guidance of system engineers to insure that all the components function coherently in unison. Call the model of the resulting structural stability and reliability *systemic cohesiveness.*

Formalised mathematical theories would, *par excellence*, possess skyscraper grounding provided that the underlying axioms are consistent. Thus, it is paramount for such grounding to *prove* the consistency of the axioms. This is indeed what Hilbert proposed first for *axiomatic theories* in his famous 1900 address in Paris as Problem Number 2.[32] With the subsequent developments in mathematical logic, the concept of a *formalised theory* crystallised (that is, an axiomatic theory in which also the logical machinery is axiomatised), and Hilbert's Problem Number 2 received its ultimate formulation in Hilbert's program, with the tacit subsidiary assumption that every mathematical proof can be converted into a formal derivation in a suitable formal system (Hilbert's Thesis). In view of the known fate of the Hilbert program as originally conceived, and yet with the still persistent belief in Hilbert's Thesis, one can legitimately ask what could be gained *epistemologically* even if complete formalisation of every part of mathematics were always possible or feasible. Concerning the actual *versus* the fictitious gains from formalisation and the mechanisation of reasoning, Kreisel [1985], p. 145, reminds us:

> Certainly, *if* one is operating on masses of meaningless symbols as one says, then the possibility of formalisation or mechanisation is a pretty obvious prerequisite for precision. But it would be odd, so to speak illogical, to conclude from this that the reliability of an argument is enhanced by ignoring everything one knows about the subject matter, and by treating it as a manipulation of meaningless symbols! In fact, the practically absolutely essential method of *cross checks*, comparing steps in an argument with one's background knowledge or reinterpreting formulas (in Hilbert's terms: by using 'impure' methods), gives new meaning to the argument. (Italics in original)

With so many cracks in *logicist* foundationalism, skyscraper grounding of mathematical knowledge has lost its credentials. Are we then obliged to surmise that mathematical theories are just *conjectural*, awaiting (or dreading) an empirical Mill to grind out a falsifier and put all to nil? Is, after the brilliant proof by Andrew Wiles, the Shimura-Taniyama conjecture still conjectural? Certainly, errors can creep in, to be duly corrected. Though no mathematical theory has ever been refuted—what could ever be a potential *falsifier* of, say, the theory of modular curves?—the mathematical community does provide *selectors* on the social level, cross-checking for

[32] In the words of Hilbert [1900]:

> ...I wish to designate the following as the most important among the numerous questions which can be asked with respect to the axioms: *To prove that they are not contradictory, that is, that a finite number of logical steps based upon them can never lead to a contradictory result.* (Italics in original)

mistakes and weeding out errors and unfruitful approaches.[33] Nor are we to forget that due to shifts in interests, an inevasible process of fossilisation or eventual death may befall any mathematical theory, as Fisher [1966] has documented in the case of the death of invariant theory. (But a referee pointed out that invariant theory has been resuscitated due to developments in chaotology.)

As skyscraper grounding of mathematics is unattainable and Popperian fallibilism founders under the weight of the cumulative stability of mathematical knowledge—no phlogiston-like case histories ever known—let us see why systemic cohesiveness is a more viable model for the reliability of mathematical knowledge.

In discussing the nature of proofs, I have particularly stressed their epistemic function in generating conceptual innovations, establishing contextual links and as methodologies for solving problems. These aspects are often neglected for failure to distinguish between proofs and derivations. None of what has been said so far is intended to neglect the *logical components* of proofs: indeed, these components are the nuts and bolts for holding together the conceptual framework engendered by the *methodological components* of proofs.

Some proofs, in particular those in which symbol manipulations play a central role, come close to formal derivations.[34] But in general, the logical structure of a proof differs substantially from a derivation. One of the salient features of a logical deduction in the course of a proof is that the deduction depends on an understanding and on prior assimilation of the *meanings* of the concepts from which certain properties are to follow logically. It won't do to say that in practice this is just a matter of using the *definitions* of the concepts in the course of a proof; for we are back at the issue of grasping the meaning of the definition and of using it 'logically' on the basis of that understanding. Anybody who has taught mathematics knows that even in a graduate course or research seminar, writing on the board a formal definition without detailed explanations of the intended meaning is a sure way to block comprehension. And let it be added that we are still in the dark on how consensus is reached on correct logical

[33] De Millo, Lipton and Perlis [1979], p. 272, put it succinctly: '... insofar as it is successful, mathematics is a social, informal, intuitive, organic, human process, a community project'. And further down: 'There is simply no way to describe the history of mathematical ideas without describing the successive social process at work in proofs. The point is not that mathematicians make mistakes; that goes without saying. The point is that mathematicians' errors are corrected, not by formal symbolic logic, but by other mathematicians.'

[34] Notice however: though it takes, for example, just three simple lines to prove that a left identity of a group (whose existence is postulated) is also a right identity, and hence is unique, a formal derivation of this result in a Hilbert-style quantification system takes at least 15 lines (and lots of explaining, as I know from experience in teaching logic).

inferences in meaning-dependent informal deductions.[35]

Consider once more Lagrange's theorem, as discussed in Example 2 above. Let us analyse the proof from the point of view of systemic cohesiveness: the spaceship model. At the outset, there was a problem: is there any relationship between the number of elements of a finite group and the number of elements of a subgroup? The solution of the problem calls first for *methodological moves*: the invention or the application of the concept of right or left cosets, and the idea of decomposing a group with respect to cosets. The proof strategy (the *systemic* plan) now requires three preliminary steps—the 'fabrication' of *reliable components*. In Step (1) one has to prove disjointness of the cosets, which amounts to showing that for every X and Y in $\mathcal{G}$,

$$\neg(\mathcal{H}X \cap \mathcal{H}Y = \emptyset) \longrightarrow (\forall Z)(Z \in \mathcal{H}X \leftrightarrow Z \in \mathcal{H}Y).$$

The argument is straightforward, and it is easy to isolate the logical part from the technical part which uses the group axioms. Once Claim (1) is justified, we put it on the shelf as a certified, reliable component. We do the same with Claim (2) and Claim (3). I won't elaborate the details but notice that in establishing Claim (2), we have to go into our 'storehouse' and use the certified 'machinery' for bijection as a valid rendering of the intuitive notion of 'same number of elements'. For Claim (3) we have to pick from the 'storehouse' the 'machinery' of mathematical induction and other arithmetic tools. Once the three claims have been established with the aid of certified tools taken from the 'storehouse', they can be added to the shelf as certified reliable components. Now we can use these components safely and fit them together with a clinching argument to get the final result: the order of a subgroup divides the order of the whole group.

In general, from the perspective of systemic cohesiveness, in constructing a proof we avail ourselves of constituents whose reliability has already been tested, parts of existing mathematical knowledge whose coherence results from previous proofs. Thanks to the logical components of proofs, the outcome of the new proof can now be safely added *qua warranted assertions* to the fabric of mathematical knowledge. Rather than viewing mathematics as well founded—in the technical sense of the term, in the manner of skyscraper groundedness, the model of systemic cohesiveness views mathematical knowledge cohesively strung together like a multidimensional Möbius band. To recapitulate, the function of the *logical component* of proofs is to guarantee and preserve the coherence of the whole system. Individual mathematicians graft the results of their research to the body of existing mathematics. But beware of an infectious or defective

[35] Promising avenues of research are in sight from work in cognitive science (see Johnson-Laird and Byrne [1991]).

graft: the collective immune system of the mathematical community will sooner or later detect the pathogen—and we are not bereft of killer cells ready to pounce!

Let us look again at the Hilbert Bridge. It spans two realms: on one side of the bridge is the formal realm of syntactic objects; on the other side is the realm of informal mathematical discourse. Many notions receive a sharper delineation under the above division into two realms by considering them as occurring in pairs. We have already considered the pair ⟨derivation, proof⟩, with derivations belonging to the formal realm and proofs to the informal realm. Another important distinction, encapsulated in the pair ⟨consistency, coherence⟩, emerges from the preceding discussion, where *consistency* is attributable to formalised theories and *coherence* to informal ones. As has already been stressed, a characteristic feature of the formal realm is that metalogical concepts—such as derivation and consistency—can be given precise technical definitions. But by their very nature, metatheoretical notions pertaining to the informal realm, such as proof and coherence, can not be *defined* technically: they can only be explicated, exemplified, and conveyed in the manner in which meanings are communicated, understood and assimilated (cf. Thomas [1991]). Skyscraper groundedness hinges on Hilbert's Thesis, and to be credible, requires consistency proofs of every formalised theory. As we now know, such 'grounding', paradoxically, can only be done from above. Rather than enlisting the aid of angels, systemic cohesiveness is earth-bound, and as a model for the reliability of mathematical knowledge is sustained by philosophical arguments. The endeavours of this section are intended to be nothing more than a sketch of an epistemological program. But by separating the two realms of the formal and informal, by seriously questioning Hilbert's Thesis, and in rejecting skyscraper groundedness of mathematical knowledge with its underlying assumption of the 'standard view', I hope to encourage a debate which focuses on actual *mathematical practice*. Imre Lakatos deserves all the credit for having pioneered in this task, though his conclusion that ultimately all mathematical knowledge is conjectural *à la* Popper is unwarranted. Quite to the contrary, the history of mathematics confirms and reconfirms that mathematical knowledge is *cohesively soldered* thanks to the methodological and logical components of proofs. Proofs as we know them are the heart of mathematics, the generators, bearers, and guarantors (*modulo* collective verifications) of mathematical knowledge. Still, over the last twenty years, various assertions have been made to the contrary—mostly by influential science journalists—ranging from the claim by Kolata [1976] that the secure notion of mathematical proof is due for revision, and all the way to the provocative article by Horgan [1993], proclaiming outright the 'death of proof' and treating Andrew Wiles's proof of Fermat's Last Theorem as a 'splendid anachronism'. Science journalists are not the only ones who have come up with provocative statements. Thus, within the mathematical community, Zeilberger [1993] has proclaimed the coming of the age of a 'semi-rigorous mathematical culture' and 'probably true theorems'.[36] Let us look at some of the technical developments which have spurred such claims.

Probabilistic Algorithms: A Source of Misunderstanding

Probabilistic algorithms, whether they are conceived for primality testing or for spot-checking formal derivations and computer programs, are constructed and validated by the customary, rigorous mathematical proof techniques and often draw upon deep and intricate mathematical theories. Such algorithms are tools for probabilistic analyses, in the manner of industrial quality control, which turn out to be appropriate for certain applications.[37] Yet the very function and nature of probabilistic algorithms have frequently been misinterpreted, particularly in popularised accounts, and their emergence has been cited as 'evidence' that mathematicians were about to relax their standard of proof and settle for 'probably true theorems', or forgo rigour altogether.

Consider first primality testing. If one wants to determine whether an integer $n > 1$ is a composite or prime number, the most direct method consists of dividing n by each d, $1 < d < n$. If no such d is a factor of n, it follows that n is prime (by definition of prime number); otherwise, conclude that n is composite. For large n, the number of steps in such a calculation becomes prohibitive. At the turn of this century, it took Frank Cole 'three years of Sundays', even with numerous shortcuts and use of tables, to show that

$$2^{67} - 1 = 193707721 \times 761838257287$$

and conclude from it that $2^{67} - 1$ is not a Mersenne prime. (The interest in primes of the form $2^n - 1$ goes back to Euclid.) Gauss, in his *Disquisitiones Arithmeticae* proposed in Sect. 6, §329, the problem of finding efficient methods for primality testing and offered some of his own. Number-theoretical interests apart, large prime numbers are currently used for the construction of secure public-key cryptosystems and pseudorandom generators. Such practical applications require computationally efficient algorithms for primality testing. (The book by Kranakis [1986] summarises the main techniques in this domain.) Since cryptosystems operate with probabilistic margins of security, it is obviously in line with the intended applications to allow for primality tests with a trade-off between computational ease and a small margin of possible errors in identifying very large

[36] For rebuttals, see Andrews [1994], Krantz [1994], and Thurston [1994].

[37] In industrial quality control a sample is subjected to certain tests, and on the basis of statistical methods one estimates the probability that the manufacturing process functions as expected within preset limits of allowable errors.

prime numbers. Such tests, known as Monte-Carlo primality tests, were first developed by Solovay and Strassen [1977] and by Rabin [1976]. Let me describe Rabin's test, following Rabin [1980].

Let $n > 1$ be an integer. Call b a *witness for the compositeness* of n if:
(i) $1 \leq b < n$;
(ii) (a) $b^{n-1} \not\equiv 1 \pmod{n}$, <u>or</u>
(b) there exists k such that $(n-1)/2^k = m$ is integral, and the greatest common divisor of $b^m - 1$ and n is > 1 and $< n$.

Clearly, if n is a prime number, no witness for the compositeness of n exists: (ii)(a) cannot hold because for every prime p and $1 \leq x < p$, $x^{p-1} \equiv 1$ (mod p) by Fermat's little theorem; condition (ii)(b) cannot hold either because it affirms the existence of a proper divisor of n. Given n and $1 \leq b < n$, it is computationally easy to determine whether b is a witness for n. (Precise bounds for the number of steps are given by Rabin.) The crux of the whole method is that if n is composite then witnesses abound. Indeed, Rabin proved (Th. 1) that if n is a composite integer > 4, the number of witnesses for n is at least $\frac{3}{4}(n-1)$.

Consider now the following algorithm for testing an integer $n > 4$: pick k numbers *at random* between 0 and n, say $0 < b_1, b_2, \ldots, b_k < n$. Test in turn each b_i. If any is a witness, declare that n is composite; if none is a witness, declare that n is a prime. (Since Rabin's algorithm uses randomisation within the computation—just like the Solovay-Strassen algorithm—such algorithms are referred to as *probabilistic algorithms.*)

How reliable is Rabin's primality test? If n is a prime number, we saw that no witness exists, hence the algorithm gives the correct answer (barring computational errors). But what happens if n is actually composite? It could happen that just no witness occurs among the k test numbers $b_1, \ldots, b_k$ which were chosen at random between 0 and n, hence the algorithm incorrectly declares n to be prime. But given the frequency of witnesses for composite numbers, Rabin proved (Th. 2) that the probability of such an error is smaller than $1/2^{2k}$. Thus, for instance, if 50 numbers $b_1, b_2, \ldots, b_{50}$ are chosen at random, the probability that the algorithm declares an actual composite number to be prime is at most $1/2^{100}$, a very small number indeed. Now Rabin ([1980], p. 129) explicitly warns that

> this last statement does *not* mean that an integer n asserted as prime by use of 50 random numbers is prime with probability at least $1 - 1/2^{100}$. Such an interpretation is nonsensical since n is either prime or not.

The probabilistic statement refers to the *reliability of the algorithm* as a function of the number of test cases. In principle, one can always test deterministically whether an integer is prime or composite; it just happens that for certain applications, such as secure encrypting—a probabilistic problem to begin with—Monte-Carlo methods are well suited. Clearly, such a technical result is devoid of epistemological implications. Yet some saw in it a major shift in mathematicians' criteria of proof.[38] Further extrapolations were quick to come. De Milo, Lipton and Perlis ([1979], p. 273), describe (without subcribing to) the probabilist view—a radical form of fallibilism—in the following words:

> The probabilists argue that since any very long proof can at best be viewed as probably correct, why not state theorems probabilistically and give probabilistic proofs?

Let us see where this leads to. I assume that the probabilist envisions that numerical probabilities be assigned to the 'truth' and 'proof value' of theorems according to some workable scheme, else the whole venture just rests on empty verbiage. Now suppose I prove a theorem T 'probabilistically' and wish to assign a numerical probability to the validity of T. In the course of my proof, say I have used known theorems θ_1, $\theta_2, \ldots$, θ_n with unequal weights, where each θ_i in turn was proven probabilistically on the basis of theorems τ_{i1}, $\ldots$, τ_{in}, each of which has a certain probability of validity, and so on. How could one extract all these probabilities as the proof tree is traced further and further back, in order to calculate the conditional probability that theorem T is 'true'? And what if our theorems of probability theory are themselves only 'true' with given probabilities, how is all this going to be taken into account and according to what procedure and with what degree of confidence? Even our miraculous PYTHIAGORA would throw her arms up in despair at the prospects of catering to a probabilist!

Let me rèturn to the symposium paper of Rabin [1976] in which he introduced the concept of a probabilistic algorithm. In the concluding remarks, Rabin suggested that probabilistic algorithms be developed for verifying the correctness of computer programs.[39] Since then much important work has been done in developing methodologies for program verifications. As programs were also developed for generating formal derivations—known as computer-assisted proofs—it was natural to extend these techniques to verifications of formal derivations. These new algorithms test random samples of a derivation or program, just as Rabin's primality test operates on random samples, but the underlying mathematics is much more intricate. One of the recent pioneering papers in this direction by Arora and Safra [1992] is entitled 'Probabilistic checking of proofs; A new characterization

[38] Reporting in *Science* on the Symposium on New Directions and Recent Results in Algorithms and Complexity, held at Carnegie-Mellon University in April 1976, where Rabin presented his paper, Kolata [1976] gave her report the spectacular title 'Mathematical Proof: The Genesis of Reasonable Doubt', and concluded with these words: 'And mathematicians may have to revise their notion of what constitutes strong enough evidence to believe a statement to be true'. Obviously, something is due for revision, but it is not mathematicians' notion of proof!

[39] Strictly speaking, correctness of programs cannot be verified algorithmically because even the halting problem is recursively unsolvable. The intended meaning is verification of the correctness of all *instances* of a computation, but I shall not insist in the sequel on such technicalities.

of NP'. For the specialist, there is no risk of confusion in the use of the word 'proofs' in the title: clearly, the paper is about formal computations and their complexity classification. But some can and have taken this type of work as a methodology for probabilistically verifying mainstream mathematical proofs, confounding proofs with formal derivations. And this indeed happened with the work surveyed by Babai [1994] on *transparent proofs* (read: *transparent derivations*). Intuitively, a formal derivation is called *transparent*, or *holographic*, if it can be verified with large confidence by a small number of spot-checks. The crux of the method consists of first transforming a formal derivation into transparent format through a sequence of encodings, ending in a collection of *numerical tables* which represent the derivation. The resulting transparent format of the formal derivation can then be tested for correctness through a constant number of *randomised spot-checks*. (For details and precise technical formulations, see Babai [1994].)

Can such algorithms be used to verify a standard mainstream mathematical proof? First, the proposed proof will have to be completely formalised, because the automatic proof checker operates only on syntactical objects appropriately encoded. I have already stressed in a previous section that there is no proof, in the technical sense, of Hilbert's Thesis, *i.e.*, the thesis that *every* informal mathematical proof can be completely formalised. This is an article of faith, and the number of believers in it is constantly dwindling. And even if such a complete formalisation were in principle possible, who will do it and who will guarantee that the formalisation has been carried out correctly, *before* being fed into the computer for computer verification? Let us ignore for a moment all these impediments, and suppose that we have such a formalisation of a significant standard mathematical proof which we wish to check for correctness by the algorithms discussed by Babai (*op. cit.*). In addition to loading the computer with the formal derivation, suitably expressed, one also has to load the machine with quite an appendix, every item of which must be *completely formalised.* As to the size of such an appendix, Babai ([1994], p. 33, footnote 2) writes (though just in a footnote):

> ...theorem-candidates [for computer verification] will tend to be very long: they will have to incorporate the definitions, basic concepts, notation, and assumptions of the given area (*e.g.*, a few volumes of Bourbaki); furthermore, they should include general axiom schemes of mathematics (say, ZF), the axioms and inference rules of logic, procedures to implement logic, *etc.*

When all this is done—hoping that Hilbert's Bridge did not collapse under the load of what a drove of mules had to lug across—the happy moment arrives: we hit the return key of the computer and wait for the verdict. When the computer halts, the final verdict appears on the screen: '*accepted*', or, '*not accepted*', as the case may be. Since the algorithm is probabilistic, the program also calculates the probability that the *algorithm* did not err in its verdict (to be distinguished from the probability that the *verdict* is correct). And where does all this lead to? Back to the myth of PYTHIAGORA, though of a subtler sort. It is a myth because of the irrealistic assumptions which we have already enumerated plus the assumptions in the just quoted passage from Babai. No, this is not the way to verify standard proofs with all their semantic elements. Reliability does not come from first formalising all our mathematical books and papers and then feeding all together with a formalised version of a proof-candidate to a computer for a probabilistic verification in order to yield a 'probably true theorem', whatever that could mean. As Thurston ([1994b], p. 170) writes:

> Our system is quite good at producing reliable theorems that can be solidly backed up. It's just that the reliability does not primarily come from mathematicians formally checking formal arguments; it comes from mathematicians thinking carefully and critically about mathematical ideas.

And again (in [1994a]):

> ...mathematical truth and reliability come about through the very human process of people thinking clearly and sharing ideas, criticizing one another and independently checking things out.

While the work reported by Babai is devoid of epistemological consequences concerning *proofs*, it does have far reaching consequences for computer science. Its major significance concerns the computer intractability of approximate solutions of a wide range of discrete optimisation problems, as the title of Babai [1994] already indicates. Paradoxically, it is just such *negative results*, like proofs of mechanical undecidability in logic, which doom PYTHIAGORA to the realm of a myth—a myth which happens to be quite pernicious if not seen as such.

Mathematics is a collective art: the social process of reciprocal cross-checks seems to be the only way to weed out errors and guarantee the overall coherence and stability of mathematical knowledge. 'Mathematics is indeed done in a social context,' writes Thurston [1994a], 'but the social process is not something that makes it *less* objective or true: rather the social process *enhances* the reliability of mathematics, through important checks and balances.' (Italics in original) We eschew the pitfalls of social relativism because there are *objective criteria* for judging the correctness of an argument. An individual mathematician may overlook or make an unwarranted assertion, but consensus is eventually reached once the error is pointed out. Logical reasoning is not at the whim of culture: biological evolution has endowed us with a mental apparatus adequate for judging the soundness of a deduction (see Rav [1989; 1993]). How else could we judge whether the basic rules of logic are sound? Certainly not by consulting rules of logic or having a computer 'tell' us!

To conclude, I have endeavoured to show that mathematical proofs are a cognitive and epistemic entity *sui generis*: the methodological components of proofs generate, catalyse and systematise mathematical knowledge, while the logical components endow mathematics with systemic cohesiveness and logical coherence.[40]

References

ALCHOURRON, CARLOS E., and ANTONIO A. MARTINO [1987]: 'Lógica sin verdad', *Theoría (San Sebastián)* **7**, 7–43.

ADLEMAN, LEONARD, and D. R. HEATH-BROWN [1985]: 'The first case of Fermat's Last Theorem', *Invent. Math.* **79**, 409–416.

ANDREWS, GEORGE E. [1994]: 'The death of proof? Semi-rigorous mathematics? You've got to be kidding!', *Math. Intelligencer* **16**, No. 4, 16–18.

ARBIB, MICHAEL A. [1990]: 'A Piagetian perspective on mathematical construction', *Synthèse* **84**, 43–58.

ARORA, SANJEEV, and SHMUEL SAFRA [1992]: 'Probabilistic checking of proofs: A new characterization of NP', *Proc. 33rd Annual IEEE Symp. Computer Science*, pp. 2–33.

BABAI, LÁSZLÓ [1994]: 'Transparent proofs and limits to approximations', in A. Joseph *et al.* (eds.), *First European Congress of Mathematics (Paris, July 6–10, 1992)*, Vol. I. Basel: Birkhäuser, pp. 31–91.

BAXA, CHRISTOPH [1993]: 'A note on Diophantine representation', *Amer. Math. Monthly* **100**, 138–143.

BELL, ERIC T. [1937]: *Men of Mathematics*. New York: Simon and Schuster.

BETH, EVERT W. [1968]: *The Foundations of Mathematics*, (Second revised edition). Amsterdam: North-Holland.

CORCORAN, JOHN [1973]: 'Gaps between logical theory and mathematical practice', in M. Bunge (ed.), *The Methodological Unity of Science*. Dordrecht: D. Reidel, pp. 23–50.

DE MILLO, RICHARD A., RICHARD J. LIPTON, and ALAN J. PERLIS [1979]: 'Social processes and proofs of theorems and programs', *Communications of the ACM* **22**, 271–280.

DETLEFSEN, MICHAEL [1992a]: 'Poincaré against the logicians', *Synthèse* **90**, 349–378.

——— (ed.) [1992b]: *Proof, Logic and Formalization*. London: Routledge.

——— (ed.) [1992c]: *Proof and Knowledge in Mathematics*. London: Routledge.

——— [1993]: 'Poincaré vs. Russell on the rôle of logic in mathematics', *Philosophia Mathematica* (III) **1**, 24–49.

DICKSON, LEONARD E. [1919]: *History of the Theory of Numbers*. (3 vols.) Reprinted 1971, New York: Chelsea.

EDWARDS, HAROLD M. [1977]: *Fermat's Last Theorem. A Genetic Introduction to Algebraic Number Theory*. Berlin: Springer.

[40] The author wishes to thank Paul Ernest and Robert Tragesser for their detailed critical comments on the first version of this article. Also, the helpful suggestions by Bernadette Deshommes and Steven Krantz are gratefully acknowledged.

ERNEST, PAUL [1994]: 'The dialogical nature of mathematics', in P. Ernest (ed.) *Mathematics, Education and Philosophy*. London: Falmer Press, pp. 33–48.

FAIR, DAVID [1984]: 'Provability and mathematical truth', *Synthèse* **61**, 363–385.

FALTINGS, GERD [1983]: 'Endlichkeitssätze für abelsche Varietäten über Zahlkörpern', *Invent. Math.* **77**, 349–366. Erratum, *ibid.* **78** (1984), 381.

FISHER, CHARLES S. [1966]: 'The death of a mathematical theory: a study in the sociology of knowledge', *Arch. History Exact Sci.* **3**, 137–159.

FOUVRY, ÉTIENNE [1985]: 'Théorème de Brun-Titchmarsh: application au théorème de Fermat', *Invent. Math.* **79**, 383–407.

FREY, G. [1986]: 'Links between stable elliptic curves and certain diophantine equations', *Ann. Univ. Saraviensis. Ser. Math.* **1**, 1–40.

GÖDEL, KURT: *Collected Works* (S. Feferman, Editor-in-Chief). Volume I (1986). Volume II (1990). Volume III (1995). Oxford: Oxford University Press.

HADAMARD, JACQUES [1914]: 'Un travail de Jean Merlin sur les nombres premiers', *Bulletin des sciences mathématiques* **39**, 121–136.

HALBERSTAM, HEINI and HAND-EGON RICHERT [1974]: *Sieve Methods*. London: Academic Press.

HALLETT, MICHAEL [1984]: *Cantorian Set Theory and Limitation of Size*. Oxford: Oxford University Press.

HEATH, THOMAS L. [1956]: *The Thirteen Books of Euclid's Elements*, (translated from the text of Heiberg, with introduction and commentary), second edition. New York: Dover.

HEATH-BROWN, ROGER D. [1985a]: 'Fermat's last theorem for "almost all" exponents', *Bull. London Math. Soc.* **17**, 15–16.

——— [1985b]: 'The first case of Fermat's last theorem', *Math. Intelligencer* **7**, No. 4, 40–55.

VAN HEIJENOORT, JEAN (ed.) [1967]: *From Frege to Gödel*. Cambridge, Mass.: Harvard University Press.

HELLEGOUARCH, YVES [1972]: 'Courbes elliptiques et équations de Fermat', Doctoral Thesis, Besançon, France.

HENKIN, LEON, PATRICK SUPPES, and ALFRED TARSKI (eds.) [1959]: *The Axiomatic Method, with Special Reference to Geometry and Physics* (Proc. Intern. Sympos. Univ. of California, Berkeley). Amsterdam: North-Holland.

HILBERT, DAVID [1900]: 'Mathematische Probleme', *Nachrichten Königl. Gesell. Wiss. Göttingen, Math.-Phys. Klasse*, 253–297; English trans. (Mary W. Newson): 'Mathematical problems', *Bull. Amer. Math. Soc.* **8** (1902), 437–479.

——— [1926]: 'Über das Unendliche', *Math. Annalen* **95**, 161–190; English translation: 'On the infinite', in van Heijenoort [1967], pp. 367–392.

HILBERT, DAVID, and WILHELM ACKERMANN [1928]: *Grundzüge der theoretischen Logik*. Berlin: Springer. English trans. by L. M. Hammond *et al.* [1950]: *Principles of Mathematical Logic*. New York: Chelsea Publishing Co.

HODGES, WILLIAM [1985]: *Building Models by Games*. Cambridge: Cambridge University Press.

HORGAN, JOHN [1993]: 'The death of proof', *Scientific American* **269**, No. 4, 92–103.

JOHNSON-LAIRD, PHILIP N., and RUTH M. J. BYRNE [1991]: *Deduction*. Hove and London: Lawrence Erlbaum Associates.

KITCHER, PHILIP [1981]: 'Mathematical rigor—who needs it?' *Noûs* **15**, 469–493.

——— [1984]: *The Nature of Mathematical Knowledge*. Oxford: Oxford University Press.

KLINE, MORRIS [1953]: *Mathematics in Western Culture*. Oxford: Oxford University Press.

——— [1972]: *Mathematical Thought from Ancient to Modern Times*. Oxford: Oxford University Press.

KOLATA, GINA BARI [1976]: 'Mathematical proof: The genesis of reasonable doubt', *Science* **192**, 989–999.

KOLMOGOROV, ANDREJ N. [1933]: *Grundbegriffe der Wahrscheinlichkeitsrechnung*, Ergebnisse der Mathematik, Vol. 2, Fasc. 3. English trans. by N. Morrison [1950]: *Foundations of the Theory of Probability*. New York: Chelsea Publishing Co.

KÖNIG, DENES [1936]: *Theorie der endlichen und unendlichen Graphen*. Leipzig: Akademische Verlagsgesellschaft. Reprinted 1950, New York: Chelsea Publishing Co.

KRANTZ, STEVEN G. [1994]: 'The immortality of proof', *Notices Amer. Math. Soc.* **41**, 10–13.

KREISEL, GEORG [1970]: 'Principles of proof and ordinals implicit in given concepts', in A. Kino *et al.* (eds.), *Intuitionism and Proof Theory* (Proc. Conf., Buffalo, N. Y., 1968). Amsterdam: North-Holland, pp. 489–516.

——— [1985]: 'Mathematical logic: tool and object lesson for science', *Synthèse* **62**, 139–151.

LAKATOS, IMRE [1962]: 'Infinite regress and the foundations of mathematics', *Aristotelian Society Proceedings, Supplementary Volume* **36**, 155–184.

LANG, SERGE [1995]: 'Some history of the Shimura-Taniyama conjecture', *Notices Amer. Math. Soc.* **42**, 1301–1309.

MACKENZIE, J. D. [1980]: 'Why do we number theorems?', *Australasian J. Philosophy* **58**, 135–149.

——— [1981]: 'Dialogue and proof', in J. N. Crossley, (ed.), *First Australian Conference on the History of Mathematics (Clayton, 1980)*. Clayton: Monash University, pp. 159–167.

MAC LANE, SAUNDERS [1992]: 'Is Mathias an ontologist?', in *Set theory of the continuum (Berkeley, Calif. 1989). Math. Sci. Res. Inst. Publ.* **26**. New York: Springer, pp. 119–122.

MATIYASEVICH, YURI V. [1993]: *Hilbert's Tenth Problem*. Cambridge, Mass.: MIT Press.

MERLIN, JEAN [1911]: 'Sur quelques théorèmes d'arithmétique et un énoncé qui les contient', *Comptes Rendus Acad. Sci. Paris* **153**, 516–518.

MOORE, GREGORY H. [1989]: 'Towards a history of Cantor's continuum hypothesis', in D. E. Rowe and J. McCleary (eds.), *The History of Modern Mathematics*. Vol. I. Boston: Academic Press, pp. 79–121.

——— [1990]: 'Introductory Note to 1947 and 1964' in K. Gödel, *Collected Works II*, pp. 154–175.

RABIN, MICHAEL O. [1976]: 'Probabilistic algorithms', in J. F. Traub (ed.), *Algorithms and Complexity: New Directions and Recent Results*. New York: Academic Press, pp. 21–40.

——— [1980]: 'Probabilistic algorithm for testing primality', *J. Number Theory* **12**, 128–138.

RADEMACHER, HANS [1964]: *Lectures on Elementary Number Theory*. New York: Blaisdell.

RAV, YEHUDA [1989]: 'Philosophical problems of mathematics in the light of evolutionary epistemology', *Philosophica* **43**, No. 1, 49–78. Reprinted in S. Restivo *et al.* (eds.), *Math Worlds*. Albany, N.Y.: SUNY Press (1993), pp. 80–109.

RIBENBOIM, PAULO [1979]: *13 Lectures on Fermat's Last Theorem*. Berlin: Springer.

RIBET, KENNETH A. [1990]: 'From the Taniyama-Shimura Conjecture to Fermat's Last Theorem', *Ann. Fac. Sci. Toulouse Math.* **11**, 116–139.

——— [1993]: 'Wiles proves Taniyama's conjecture; Fermat's Last Theorem follows', *Notices Amer. Math. Soc.* **40**, 575–576.

——— [1995]: 'Galois representations and modular forms', *Bull. Amer. Math. Soc.* (N. S.) **32**, 375–402.

ROTMAN, JOSEPH J. [1973]: *The Theory of Groups* (2nd ed.). Boston: Allyn and Bacon.

SCRIBA, CHRISTOPH J. [1980], 'Viggo Brun in memoriam (1885–1978)', *Historia Mathematica* **7**, 1–6.

SHAPIRO, STEWART [1991]: *Foundations without Foundationalism: A Case for Second-order Logic*. Oxford: Clarendon Press.

SIMPSON, STEPHEN G. [1988]: 'Partial realization of Hilbert's Program', *J. Symbolic Logic* **53**, 349–363.

SMORYNSKI, CRAIG [1991]: *Logical Number Theory*. I. Berlin: Springer.

STEINBRING, HEINZ [1991]: 'The concept of chance in everyday teaching: Aspects of social epistemology of mathematical knowledge', *Educational Stud. Math.* **22**, 503–522.

THOMAS, ROBERT S. D. [1990]: 'Inquiry into meaning and truth', *Philosophia Math.*(II) **5**, 73–87.

——— [1991]: 'Meaning in ordinary language and in mathematics', *Philosophia Math.*(II) **6**, 3–38.

THURSTON, WILLIAM P. [1994a]: 'Letter to the Editors', *Scientific American* **270**, No. 1, 5.

——— [1994b]: 'On proof and progress in mathematics', *Bull. Amer. Math. Soc.* (N. S.) **30**, 161–177.

VEGA, LUIS [1993]: '¿Pruebas o demostraciones? Problemas en torno a la idea de demostración matemática', *Mathesis* **9**, 155–177.

——— [1995]: 'Demostraciones clásicas', *Theoría (San Sebastián)* (2) **10**, No. 24, 79–101.

WANG HAO [1974]: *From Mathematics to Philosophy*. London: Routledge & Kegan Paul.

——— [1978]: 'In memoriam Kurt Gödel: 28 April 1906–14 January 1978'. *Math. Intelligencer* **1**, No. 3, 182–185.

——— [1981]: 'Some facts about Kurt Gödel', *J. Symbolic Logic* **46**, 653–659.

WANG YUAN (ed.) [1984]: *Goldbach Conjecture*. Singapore: World Scientific Publishing Co.

WILES, ANDREW [1995]: 'Modular elliptic curves and Fermat's Last Theorem', *Ann. of Math.* **141**, 443–551.

WOODIN, W. HUGH [1994]: 'Large cardinal axioms and independence: The continuum problem revisited', *Math. Intelligencer* **16**, No. 3, 31–35.

WUSSING, HANS [1984]: *The Genesis of the Abstract Group Concept.* Trans. by A. Shenitzer. Cambridge, Mass.: MIT Press. (Original [1969]: *Die Genesis des abstrakten Gruppenbegriffes.* Berlin: VEB.)

ZEILBERGER, DORON [1993]: 'Theorems for a price: tomorrow's semi-rigorous mathematical culture', *Notices Amer. Math. Soc.* **40**, 978–981. Reprinted in *Math. Intelligencer* **16** (1994), No. 4, 11–14; 76.

ABSTRACT. Ordinary mathematical proofs—to be distinguished from formal derivations—are the locus of mathematical knowledge. Their epistemic content goes way beyond what is summarised in the form of theorems. Objections are raised against the formalist thesis that every mainstream informal proof can be formalised in some first-order formal system. Foundationalism is at the heart of Hilbert's program and calls for methods of formal logic to prove consistency. On the other hand, 'systemic cohesiveness', as proposed here, seeks to explicate why mathematical knowledge is coherent (in an informal sense) and places the problem of reliability within the province of the philosophy of mathematics.