Philosophica 63 (1999, 1) pp. 119-152

THE CREATIVE GROWTH OF MATHEMATICS

Jean Paul Van Bendegem

There is quite literally a world of difference between discovery in the (natural) sciences and discovery in mathematics. The former expression suggests a realist interpretation though certainly not a full-scale realism. Even the most moderate realist possible is willing to talk about discovery in some sense. However, mathematics is a different kettle of fish. If one dares to use the term 'discovery', then, necessarily, in one sense or another, one must be a mathematical realist. But this sort of realism is of a rather peculiar kind, as the world wherein the mathematical objects and/or entities are discovered, happens not to be this world. Therefore, there is a strong ontological claim intrinsically tied up with the word 'discovery'. Unfortunately, replacing the word 'discovery' by a more neutral expression such as 'creative growth' (and not by 'construction', for obvious reasons) does not really solve (or avoid) the fundamental problem, that is the following. It would be nice if one could argue that a particular philosophical position concerning the foundations of mathematics will not affect a description of what mathematicians do and why they do what they do, but such is not the case.

Nevertheless, I do believe it is possible to start from a minimal position. I will therefore in this paper assume, as a philosophical framework, a form of 'mild' constructivism, i.e., the position that mathematical objects, entities, including proofs, are human products and should, in first order, be analyzed as such. I consider this view to be minimal because it does not exclude forms of platonism or some other strong ontological claims about mathematical objects.

The structure of the paper is quite simple. I begin at the most general level – the mathematical community as a whole - and I go slowly down to the level of the working mathematician who is (among other things) trying to find a specific proof for a particular theorem. The 'afterthought' returns briefly to the philosophical question raised in this introduction.

1. Revolutions in mathematics?

There is a quite intriguing problem with the attempts to describe the development of mathematics at the large-scale level. In clear contrast with what happened in philosophy of science, one cannot help but to notice that in philosophy of mathematics, there is hardly any agreement. Often, Michael Crowe's *Ten 'laws' concerning patterns of change in the history of mathematics* is considered to be the starting point of the discussion about revolutions in mathematics. Rather surprisingly, the tenth and last 'law' states: 'Revolutions never occur in mathematics'. His basic argument is that 'a necessary characteristic of a revolution is that some previously existing entity (be it king, constitution, or theory) must be overthrown and irrevocably discarded. (Crowe, 1992: 19).

At the same time, however, Joseph Dauben is a firm defender of the occurrence of revolutions in mathematics (see, e.g., Dauben, 1992: chapters 4 and 5):

> Discovery of incommensurable magnitudes and the eventual creation of irrational numbers, the imaginary numbers, the calculus, non-Euclidean geometry, transfinite numbers, the paradoxes of set theory, even Gödel's incompleteness proof, are all revolutionary - they have all changed the content of mathematics and the ways in which mathematics is regarded. They have each done more than simply add to mathematics - they have each transformed it. In each case the old mathematics is no longer what it seemed to be, perhaps no longer even of much interest when compared with the new and revolutionary ideas that supplant it. (Dauben, 1992: 64).

Philosophers of science themselves - such as Thomas Kuhn, to quote the most obvious one - if they do talk about mathematics, their main purpose is to make clear that the natural sciences and mathematics should not be confused (see, e.g., Kuhn, 1977). Hence they often end up defending the non-revolutionary nature of mathematics.

To further complicate matters, as I said in the beginning, ontological issues are unavoidable. To give but one example: for Crowe, some sort of 'revolution' remains possible, viz.

> revolutions may occur in mathematical nomenclature, symbolism, metamathematics (e.g. the metaphysics of mathematics), methodology (e.g. standards of rigour), and perhaps even in the historiography of mathematics. (Crowe, 1992:19).

In other words, content-wise, there are no revolutions, but anything-else-but-content-wise, you can have as many as you want. I will not explore this fascinating theme any further in this paper, but rather turn to the common elements that all these authors seem to share, viz. the fact that mathematics does possess a large-scale structure.

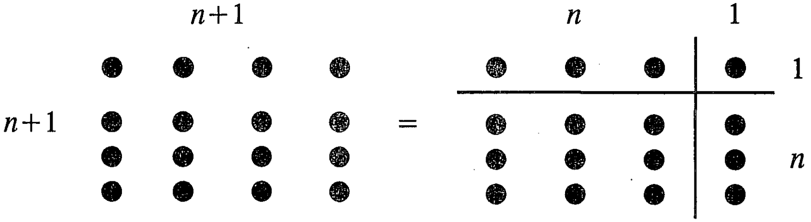
2. The large-scale structure of mathematics (if any)

The last sentence of the preceding paragraph is close to being tautological. For what would have to be the meaning of the statement that mathematics has no large-scale structure? The crucial feature that interests me – and I assume that the authors mentioned above, whatever their views, share this interest - is that this large-scale structure 'affects' the daily practice of mathematicians by imposing constraints on the kind of (more specific) mathematics that is being done. Examples of such constraints are:
(a) What are the relevant mathematical research themes, and research problems to look at?
(b) How are the results already obtained to be systematized?
(c) What are the global aims of a particular area of mathematics?
(d) What is to count as a mathematical proof? What are the standards of rigour, say, for mathematical proof?
(e) How is the history of (a part of) mathematics to be told?
Seen from this perspective, it becomes possible to identify major periods in the development of mathematics. A nice example of such an attempt to identify such periods is to be found in the work of Teun Koetsier. Let me briefly summarize his approach. Although he distinguishes three levels - the micro-level where the mathematician mainly spends his or her time proving theorems, the intermediate level where research projects are formulated, and the macro-level that identifies a particular period - I will

focus only on the macro-level. Koetsier, inspired by, though certainly not a blind follower of Imre Lakatos, speaks about *research traditions*:

> A mathematical research tradition is a group research activity, historically identifiable (in a certain period), characterized by common general assumptions (in the form of e.g. definitions and axioms) about the entities that are being studied in a particular fundamental mathematical domain, and it involves assumptions about the appropriate methods to prove properties of those entities. (Koetsier, 1991: 151).

An example may help to clarify his approach. Within Greek mathematics, Koetsier distinguishes two traditions which he calls the *Demonstrative Tradition* (DT) and the *Euclidian Tradition* (ET) in chronological order. A major point of difference between DT and ET is the fact that ET introduces the notion of proof as standard method for establishing mathematical truths. Koetsier claims that the method of proof of DT is non-deductive. It is based on a form of 'Anschauung'. The best example to illustrate this is the 'proof' of $(n+1)^2 = n^2 + 2.n + 1$, in Pythagorean fashion. Thus, to show that $4^2 = (3 + 1)^2 = 3^2 + 2.3 + 1$, it is sufficient to look at these two drawings:



Of course, if this is to count as a convincing method, we must assume that a particular case can be 'seen' as an arbitrary case. That is, I am supposed not only to grasp this figure (or rather its meaning) but also all other cases similar to it. Granted that sense can be made of 'proof by looking'[1], then it is obvious that the transition from DT to ET is a major

[1] The expression "proof by looking" is actually an entry in David Wells, 1991 and I quote: "Many simple arithmetical facts can be proved 'at sight', by examining a suitable figure" (198). If Koetsier is right (see his 1991: 188-190), one might just as well leave

one indeed. It should also be obvious that it is a progressive move.

As one might expect, not every philosopher and/or historian of mathematics agrees with the picture put forward by Teun Koetsier. I refer the reader to the work of Eduard Glas (especially, 1991a and 1991b) for a critique of Koetsier's approach. To be sure, neither Koetsier nor Glas are the last word on the subject. An approach along the lines of Philip Kitcher (see his 1983) is different from their views and, in addition, it is not straightforward to situate Kitcher's ideas within the broader field of evolutionary and/or naturalist epistemology, to quote but one of the many approaches in the field of epistemology (compare, e.g., with Rav, 1993).

Or perhaps, all of these approaches are fundamentally mistaken as they are looking in the wrong direction. If one is talking about structures, should one not therefore take the idea of structure seriously: in other words, a structuralist approach is what is needed for such a description. To be a bit more concrete, the Bourbaki programme could then be viewed as such a proposal, whether idealist or realist being a matter of further discussion (see, e.g., Corry, 1992). Or, for that matter, an approach such as the one promoted by Roman Duda (see Duda, 1997), namely, in terms of tensions and polarities: realism-idealism, finite-infinite, discrete-continuous, approximate-exact, certitude-probability, simplicity-complexity, unity-multiplicity.

To complete and complicate matters, I have not said anything - and will not within the framework of this paper - about the multiple relations between, generally speaking, mathematics and society, and between, more specifically and as an example, mathematics and the gender issue. All that has been said up to now, treats mathematics as an autonomous part of society 'obeying' only its internal 'laws', if such exist. But this can only be part of the story, which, once again, I am not going to complete (see Restivo 1983 and 1992, for more details). Nevertheless, from now on, I will assume that a (kind of) large-scale structure has been 'established' and that a mathematician operates within this framework.

out the "simple", for he claims that, according to Oskar Becker, there is a proof by looking of this arithmetical fact: any number of the form $2^n.(1 + 2 + 2^2 + \ldots + 2^n)$ such that $p = 1 + 2 + 2^2 + \ldots + 2^n$ is a prime, is perfect.

3. The transition from large-scale to micro-practice

Given the large-scale structure of the mathematical enterprise, how does it translate into everyday mathematical practice? It cannot be the case that every mathematician has a full-blown view of the whole of mathematics. It is generally agreed that with Henri Poincaré and David Hilbert the last of the generalists have left us. Thus there has to be an intermediate level. One possible way of viewing this level is sketched by Teun Koetsier. According to his model, on this level, we have *research projects*:

> A research project consists of a number of research goals together with a set of hints as to how one can reach the goals. The project includes a paradigmatic solution of a problem that shows the kind of goals and the effectiveness of the hints with respect to the goals. Large projects may very well encompass subprojects. (Koetsier, 1991: 154).

Within a research project operates, what he calls, the MMRT, the *methodology of mathematical research traditions*. Basically, it involves two elements:
(a) 'A mathematical research project or research tradition progresses heuristically if it produces conjectures (theorem candidates) of weight' (Koetsier, 1991: 159), and
(b) 'The preference of a rational mathematical community for a research project or a research tradition is proportional to its expected progress' (ibidem).

It is perhaps unnecessary to repeat a comment made before, but Koetsier's model is just one way of looking at things. No doubt different models are possible, but one way or another, they must incorporate some notion, similar to Koetsier's research project[2]. After all, this is the level where the brilliant and promising mathematics student's supervisor decides what topic is worth the effort. This implies in a very precise way,

[2] Thus, to a structuralist, the local structures can be viewed as substructures of the general large-scale structure. Note that one other problem I am completely ignoring, is whether the 'impetus' of the research projects or the substructures derives from the projects and/or structures themselves, and, if not, whether it comes from individual mathematicians, groups of mathematicians, and, if that is not the end of the story, whether other non-mathematical individuals and/or groups enter into the picture.

the possibility to evaluate the possible outcomes and the impact of the research to be undertaken on the mathematical community.

3.1. Some examples of research projects

The proof of the pudding, however, remains in the eating. Are there such examples of research projects to be found in 'real' mathematical life? Fortunately, the answer is without any discussion: yes. Here are some:

3.1.1. The Erlanger Program

No doubt, one of the most famous examples is the *Erlanger Program*, set up by Felix Klein. Saunders MacLane gives a short to the point description of this program:

> In geometry, Felix Klein proposed that the many varieties of space provided by non-Euclidean and other geometries could be classified and hence organized in terms of their groups of symmetries - the full linear group, the orthogonal group, the projective group, and others. (MacLane, 1986: 407).

Following the *Erlanger Program*, in more recent times, is the so-called *Langlands Program*. Basically, the idea is to use infinite dimensional representations of Lie groups as a tool to solve problems in number theory. Stephen Gelbart in an excellent expository paper writes the following:

> ... Langlands' program is a synthesis of several important themes in classical number theory. It is also - and more significantly - a program for future research. This program emerged around 1967 in the form of a series of conjectures, and it has subsequently influenced recent research in number theory in much the same way the conjectures of A. Weil shapes the course of algebraic geometry since 1948. (Gelbart, 1984:178).

In the same paper, the author emphasizes that

> ... more than one half of this survey will be devoted to material which is quite well known, though perhaps never before presented purely as a vehicle for introducing Langlands' program. (Gelbart, 1984: 179).

3.1.2. Hilbert's Program

Equally well known in the mathematical community is the general research project outlined by David Hilbert in his famous Paris speech in 1900, 'Mathematische Probleme' at the occasion of the International Congress of Mathematicians. Hilbert discusses twenty-three problems that effectively did determine to a large extent the mathematical activity in the first half of this century. Some of the most famous problems are:

- *Problem 1*: Cantor's continuum hypothesis, i.e., the question whether or not there are cardinalities between the countable and the cardinality of the reals.
- *Problem 2*: The consistency of arithmetic. No comment needed.
- *Problem 8*: The Riemann hypothesis, i.e., given the function $Z(s) = \Sigma\ 1/n^s$, where s is a complex number and n goes from 1 to infinity, one has to prove that the non-trivial solutions of $Z(s) = 0$ all have 1/2 as the real part.
- *Problem 10*: The Diophantine problem, i.e., to find a method to decide whether a set of equations such that all coefficients are integers (rationals), has integer (rational) solutions.

For more details, see Alexandrov (1971) and Browder (1976).

3.1.3. Finite Simple Groups

As this example shows, it is not necessary for a research project to start with conjectures. A project can be set up around a problem that has been solved. I may add here that few philosophers of mathematics take into account such cases, which I consider to be extremely relevant. The case I am referring to, is the Classification Theorem for Finite Simple Groups, also labelled the *Enormous Theorem*. The existing proof, some 15.000 pages long, consists of a series of papers, most published, though not all, written by a diverse group of mathematicians over a period of thirty years, writing in different styles, using different kinds of proof methods. Such a 'proof' can hardly be called a proof, as says Ronald Solomon:

> The state of the original proof is such that if everyone who worked on it should vanish, it would be very hard for future generations of mathematicians to reconstruct the proof out of the literature. (Cipra, 1996: 89).

Part of the explanation is that the simple groups come in four categories:

cyclic (of prime order), alternating, Lie-type (to be split up in sixteen families) and sporadic. The first three bring together an infinite number of simple groups, each with their own problems, proof methods and proof techniques, but, in addition, the sporadic simple groups are quite strange. There are precisely 26 of them, and the largest one has no less than some 10^{53} elements, the so-called *Monster*. It is fair to say that in some cases proof methods were designed to deal with this or that specific case. It then becomes clear what the aims of this research project are, started by Daniel Gorenstein (died in 1992), Richard Lyons and Ronald Solomon:

(i) To make uniform the different proof methods that have been used over the thirty year period. The expectation is that this will generate new proof ideas: 'By straightening out the strands of the original proof, Lyons and Solomon have already been able to stretch them further, proving some of the component theorems in considerably greater generality. They and others working on the second-generation proof have also found new applications of the original proof's techniques. (Cipra, 1996: 89).

(ii) To reduce the size of the proof to something like 5.000 pages, perhaps even shorter and to publish the proof as a *single* proof. This is also a rather surprising aim: apparently, proofs are not perceived as proofs, but are to be presented as such.

(iii) To eliminate all errors present. No comment needed.

For more details see Gorenstein, 1986.

3.1.4. Probability theory old and new

Probability theory in the 'old' style was formulated in terms of functions P, usually from a set of sentences S, defined in a particular language L, to the real interval [0,1], satisfying certain axioms, such as

P(A or not-A) = 1,
P(A and not-A) = 0,
P(A or B) = P(A) + P(B) - P(A and B), and so on.

This type of approach worked well in discrete cases, but in the continuous case, there were many problems (unless some geometric or other finitely expressible interpretation was available) to determine probabilities[3].

A. N. Kolmogorov was the first in 1933 to see the connection with measure theory and the theory of integrals. This led to a reformulation of probability theory in such a way that all the results of measure theory could be translated into probabilities. Thus, any handbook today will start with the definition of a probability space PS, being a triple $<S, F, P>$, where:

(i) S is a set (actually nothing more is needed, but occasionally this set is referred to as the *sample space*),

(ii) F is a set of subsets of S, satisfying the conditions: (i) $F \neq \varnothing$, (ii) if $A \in F$, then $S \backslash A \in F$, (iii) if $A_i \in F$, for $i = 1, 2, \ldots, n, \ldots$ then $\cup_i A_i \in F$. In other words, F is a σ-algebra, although in probability terms this is called the *event space*,

(iii) P is a *probability measure* on F, such that: (*) $P(A) \geq 0$, for all $A \in F$, (**) $P(S) = 1$, and (***) if $A_i \in F$, for $i = 1, 2, \ldots, n, \ldots$ and $A_i \cap A_j = \varnothing$, for $i \neq j$, then $P(\cup_i A_i) = \Sigma_i P(A_i)$.

Among other things, this new approach makes it possible to talk about singular distribution functions[4], apart from the already classically known discrete and continuous distributions.

3.1.5. Category theory

A recent research project is the project centered around *category theory*. To a certain extent, this may be viewed as the *Erlangen program* for set theory, as is clearly expressed in the words of Saunders MacLane:

> The situation bears some resemblance to that in geometry after the discovery of consistency proofs for non-Euclidean geometry showed that there was not one geometry, but many. This meant that geometries could be formulated with many different systems of axioms, some of which were relevant to higher analysis and some to physics. ...

[3] These confusions and difficulties are responsible for the immense, diversified, and amusing literature on paradoxes in probability theory, see, e.g., Northrop, 1978, especially chapter eight.

[4] An example may help. One needs a singular distribution function to solve this problem: On the kth toss of a fair coin a gambler receives 0 if it is a tail and $(2/3)^k$ if it is a head. Let X be the total gain of the gambler after an infinite sequence of tosses of the coin. The problem is solved in Grimmett & Welsh, 1994: 102-104.

> Similarly, the initial idea of a collection leads to substantially different versions of set theory, some of which ... have relevance to other parts of Mathematics, though not yet (?) to Physics. (MacLane, 1986: 385-386).

A category *C* consists of objects A, B, C, ... and arrows f, g, h, ... from objects to objects, satisfying the conditions:
(i) for each pair of arrows: if $f: A \to B$ and $g: B \to C$, then $g \circ f: A \to C$ exists, called the composition of f and g,
(ii) for every object A, there is a function $1_A: A \to A$, the identity arrow,
(iii) composition is associative: for all arrows f, g, and h, if the composition is defined, then $(f \circ g) \circ h = f \circ (g \circ h)$,
(iv) for every arrow $f: A \to B$, it is the case that $f \circ 1_A = f = 1_B \circ f$.
The power of category theory is truly impressive. Whatever theorem one manages to prove about categories, is applicable to at least the following cases (see MacLane, 1986: 387):
(i) The category where the objects are sets and the arrows functions from sets to sets,
(ii) The category where the objects are groups and the arrows homomorphisms between groups,
(iii) The category where the objects are vector spaces and the arrows linear transformations,
(iv) The category where the objects are topological spaces and the arrows continuous maps.

It is worth mentioning that together with the concepts of category theory, a new way of proving statements was introduced, sometimes referred to as *diagram chasing*. It is absolutely typical for a handbook on category theory to be overloaded with diagrams such as:

$$\begin{tikzcd}
A \arrow[r, "g"] \arrow[d, "f"'] & B \arrow[d, "j"] \\
C \arrow[r, "h"'] & D
\end{tikzcd}$$

Just by looking at the diagram, one can see that to go from the top left corner to the bottom right corner, can be done in two ways, therefore h°f = j°g.

Whether, in terms of Koetsier's model, one is entitled to talk about a research tradition rather than about a research project, is a difficult matter, both for mathematicians and philosophers to decide. For a discussion, see Bell, 1994.

This short survey of research projects has no pretence whatsoever of completeness. It is sufficient to consult, e.g., Dieudonné, 1987, especially chapter V ('Nouveaux objets et nouvelles méthodes'), for a wealth of examples.

3.2. The importance of proof methods

All of the above cases have been discussed mainly, though not exclusively, in terms of the problems that had to be solved. But one could equally well look at these examples from the point of view of (novel) proof methods. Very often, the focus of a research project is on the proof methods in the first place and on the problems or conjectures in the second place. Note, additionally, that the proof methods are novel for the domain under discussion. Very often, these methods are already existing in another domain, but the translation was lacking (as is the case, e.g., in the probability research project). Historically speaking, there is a multitude of cases, apart from the one discussed above, to be found:

3.2.1. Some historical examples of proof methods

(i) No doubt, the most famous case is the introduction of the proof *by reductio* in Greek mathematics. One might argue about the philosophical significance and the ontological-epistemological implications of this method, but everyone agrees that it marked a new way of looking at and working in mathematics.
(ii) Equally famous is the method of *infinite descent*, promoted by Pierre de Fermat for proving the non-existence of solutions of Diophantine equations. The basic idea is to prove that if a (integer) solution exists, then there must be another (integer) solution that is strictly smaller, obviously leading to a contradiction.

In terms of translations from one domain to another and thereby importing proof methods from the former to the latter, the two most famous cases are:

(iii) The *reformulation of geometry in algebraic terms* led to an entirely different view of geometry. Whether or not this development is to be situated with Descartes, it is definitely the case that proof methods from algebra could now be used for solving geometrical problems. As a simple case, it is sufficient to think about the classification of curves in algebraic terms. More specifically, think of the classification of curves of degree two. On the one hand, geometrically speaking, there is the well-known cone figure (attributed to Apollonios) intersected by a plane at different angles, and, on the other hand, the classification of curves of the form $ax^2 + bxy + cy^2 + dx + dy + e = 0$ on the basis of determinants and the like.

(iv) The *rigorization of* mathematics in the 19th century, especially of *differential and integral calculus*, made it possible to reformulate questions concerning derivatives and integrals in more abstract terms, thereby making room for proof methods that went beyond the geometrical. Actually, this case is quite similar to the probability example given above.

For (iii) and (iv), see Grattan-Guinness, 1997 for more detail and further references.

3.2.2. Some present-day examples of proof methods

One might perhaps be tempted to say or to claim that today at least we finally have a single set of proof standards, but that is definitely not the case. Within the mathematical community itself, deep discussions are taking place concerning the following problems (for a general discussion, see Hersh, 1997: part one, chapter 4):

(i) Is a proof that involves the use of computers to be considered a proof? The most interesting case that started the whole discussion was, of course, the four-colour theorem (or conjecture?). As part of the proof consists of a computer program[5], to a number of mathematicians the proof does not deserve to be called such. The debate is still running. See

[5] To be a bit more precise: the proof comes in two parts. The first part - a classical mathematical masterpiece - shows that the set of all maps to be coloured can be reduced to a finite set of maps, such that if the finite set can be coloured, so can all of them. The second part consists of a computer program that actually colours every map in the finite set. One therefore has no other choice than to run the program and see if the final answer is yes or no. A rather amazing situation. See Appel and Haken, 1989.

Tymoczko, 1986 for more details.
(ii) What is the value of probabilistic proofs? Are these to be considered as proofs? The answer to the latter question has to be yes. After all, one does prove statements such as 'If test T, involving a choice of k numbers, is performed on a given number n, and the answer is yes, then the number n is prime, with a probability of 1 - 1/4^{k}'. The more intriguing question is the former one: what does a proof like that tell us? Is it interesting to know that a number is *very likely* a prime number? See, e.g., Ribenboim, 1989: 107-128, for a clear presentation.
(iii) What is the value of a 'video-proof'? I have to add here that, although it is claimed that video-proofs introduce an entirely new and novel way of doing mathematics, video-proofs are nothing but modern technological man's version of proofs-by-looking that were mentioned above. Perhaps the question should be phrased more generally: Can there be 'experimental' proofs? See my 1990b for some discussion and examples.

To conclude this paragraph, the general and hence not too detailed picture is that mathematics can be viewed as a network of research projects, whereby larger parts of the network form research traditions. The function of a project is to generate, firstly, problems, conjectures, i.e., work that needs to be done, and, secondly, an agreement on the methods and standards to be used to handle the problems. This is, roughly speaking, the environment wherein a mathematician performs his or her daily task.

4. A day in the life of a mathematician

On the micro-level, individual mathematicians set out to prove theorems, to formulate conjectures, to check proofs or theorems proved by other mathematicians, to search for counter-examples to disprove a statement, and so on. The basic question to be asked is: how do they do it? Given a statement A, how do you go about it to find (or construct) a proof? In short, the question of heuristics has to be dealt with.

As one might expect, there are several suggestions, ideas, and proposals. No doubt, the most familiar one is Lakatos' *method of proofs and refutations*. In his own words:

> Rule 1. If you have a conjecture, set out to prove it and to refute it. Inspect the proof carefully to prepare a list of non-trivial lemmas (proof-analysis); find counterexamples both to the conjecture (global counterexamples) and to the suspect lemmas (local counterexamples).
> Rule 2. If you have a global counterexample discard your conjecture, add to your proof-analysis a suitable lemma that will be refuted by the counterexample, and replace the discarded conjecture by an improved one that incorporates that lemma as a condition. Do not allow a refutation to be dismissed as a monster. Try to make all 'hidden lemmas' explicit.
> Rule 3. If you have a local counterexample, check to see whether it is not also a global counterexample. If it is, you can easily apply Rule 2. (Lakatos, 1976: 50).

However, this cannot be the whole story. What, for instance, is a mathematician supposed to do if no proof is to be found in the first place? As an example, let me briefly summarize some aspects of the history of *Fermat's Last Theorem* (FLT) (for more details, see my 1987).

4.1. Fermat's last theorem

In a first phase, instead of tackling the general problem, proofs were found for particular cases: thus, it was shown that $x^n + y^n = z^n$ did not have integer solutions for n = 3, 4, 5, 7, 14. In these proofs the method of infinite descent was crucial (see above). One has to wait for Sophie Germain who, in 1823, showed the following. To formulate the theorem it is necessary to make the following distinctions:

- the equation is restricted to prime numbers p, thus:

$$x^p + y^p = z^p,$$

- the first case of FLT states that there are no x, y, z, such that p does not divide x.y.z and $x^p + y^p = z^p$ (the second case is, obviously, the one where p does divide x.y.z).

Germain's theorem says the following:

> For every odd prime p such that 2.p + 1 is also a prime, the first case holds.

With some additional theorems, Germain and Legendre were able to deal with all prime numbers < 100. As one might expect, the problem is to determine how many primes p there are such that 2.p + 1 is also a prime, a very difficult problem indeed. I must add here that the technique to split up a theorem in subcases and to treat these separately, is an almost continuous characteristic of the history of FLT. For example, in the next breakthrough by Eduard Kummer, because he had transposed the problem to the domain of complex numbers, another division was made into regular primes and irregular primes. The theorem Kummer arrived at stated boldly: If the prime p is regular, then FLT holds.

The point of importance to note here is that FLT has now entered a new domain: it is no longer a problem in number theory but a problem in complex number theory. This is a second constant phenomenon to be observed: a problem such as FLT remains in a specific domain and 'migrates' to another domain if no interesting results are found. However, deciding whether a prime p is regular is about as difficult as deciding whether it is such that 2.p + 1 is also prime. Nevertheless, it would enable mathematicians in the years to follow to raise the upper bound to 125.000.

But FLT did not remain in this domain, another 'migration' took place. Rewriting the equation as follows:

$$(x/z)^p + (y/z)^p = 1, \text{ or}$$
$$X^p + Y^p = 1,$$

FLT says that this curve does not go through rational points. We enter the domain of algebraic number fields and from this domain, the area of elliptic curves, modular forms, where finally a proof would be found (see Wiles, 1995). Note that top mathematicians involved such as Gerd Faltings, Gerhard Frey, Ken Ribet, even Andrew Wiles[6], were not really working on FLT, but on other problems that as a corollary would prove FLT.

What I want to emphasize is that the search for a proof - the initial

[6] In the case of Andrew Wiles there is even a curious twist to the story. Already as a child he wanted to prove FLT, but in his mathematics study he was strongly advised not to waste time on this problem. Rather he should use his talents for important problems in elliptic curves and modular forms. However, after Ribet's theorem that showed the connection between the two, Wiles realized he was after all working on his dream project. It is worth noting that in the famous Wiles' paper of 1995, though FLT is mentioned in the title, FLT itself is only referred to in the introduction.

step in Lakatos' model - apparently happens in a methodical way (or methodical ways). Thus, it should be possible to set up rules and guidelines. Some of these rules will be rather evident - splitting up your problem into different cases, was already advised by Polya (see further) - but the suggestion to look for 'translations' of your problem in other domains and fields, thereby encouraging a 'migration' is perhaps less trivial.

I will not go into any details, but similar stories can be told about other open problems in mathematics. I refer the reader to Echeverria (1996) for a beautiful treatment of Goldbach's conjecture.

But even that cannot be the whole story. Proofs are curious things. It is perhaps trivial to say that it takes a mathematician to see one if there happens to be one, but they definitely use more criteria than mere formal correctness, as the summarized account of the following case shows (for more details, see my (1988)).

4.2. Apéry and the Riemann Zeta Function

Suppose you attend a seminar where a mathematician presents a proof to some of his colleagues. Suppose further that what he is proving is an important mathematical statement. Now the following happens: as the mathematician proceeds, his audience is amazed at first, then becomes angry and finally ends up disturbing the lecture (some walk out, some laugh, ...). Nevertheless, the proof is formally speaking (nearly) correct. What has happened?

Roger Apéry investigated the Riemann Zeta Function, $Z(s) = \Sigma_n 1/n^s$, where s is a complex number and n goes from 1 to infinity (the same function in Hilbert's eighth problem, see above). There is no doubt that this is an important subject in the mathematical community. More specifically, he was interested in the integer values, Z(n). Some results were known, such as:

$$\text{For } n = 2k,\ Z(2k) = (-1)^{k-1}(2\pi)^{2k}B_{2k}/(2.(2k)!),$$

where B_{2k} is the 2k-th Bernoulli number, i.e., the 2k-th coefficient in the equation: $x/(e^x-1) = \Sigma\ B_i x^i/k!$.

Example: For $n = 2$, $k = 1$ and, given that $B_2 = 1/6$, we find that:

$$\Sigma_n\ 1/n^2 = Z(2) = (-1)^0(2\pi)^2/6.2.2!$$

$$= 1.4.\pi^2/6.2.2$$
$$= \pi^2/6,$$

a well-known result.

However, much less is known about the odd values. Are Z(3), Z(5), ..., in general, Z(2n+1), rational or irrational? The problem was known to Euler but neither Euler nor mathematicians after him managed to handle the problem. In June 1978, Roger Apéry presented a proof of the irrationality of Z(3). It is this proof that provoked the strange reaction of his colleagues.

If the question does not sound too silly: what was wrong with Apéry's formally correct proof? Mathematicians gave the following comments:

(i) The proof was 'mysterious' and consisted of a series of 'miracles'. Thus, e.g., Apéry uses the following series, defined recursively:

$$n^3u_n = (34n^3 - 51n^2 + 27n - 5)u_{n-1} - (n-1)^3u_{n-2}.$$

Apéry claimed the following: if one starts with $u_0 = 1$ and $u_1 = 5$, then all u_n are integers! This is indeed very surprising as each u_n is of the form A/n^3. Therefore the right-hand-side must be divisible by n^3, for all n[7].

(ii) The proof offers no clues at all for other values of Z(s) for s = 2n+1. Apparently, mathematicians consider proofs that do not have this property as proofs of low quality.

(iii) Part of the disbelief in Apéry's proof had to do with the fact that he did not use any 'new' methods. In short, the proof could have been found by Euler. So why did Euler not find the proof or anybody soon after that?

After rewriting the proof (done by other mathematicians) the result has now been accepted and generalizations have been found (see Apéry, 1996: 58)[8].

[7] There is an intriguing historical remark to be made. The inspiration for this type of series, Apéry had found in the work of Ramanujan, the famous Indian mathematician. However, for the latter, the term 'miracle' is precisely used as a positive qualification.

[8] The recognition afterwards for his result has apparently wiped out the bad memories of the occasion itself. François Apéry, his son, makes no mention of the incident, but writes that: 'The proudest moment of his career was his proving, at more than 60 years of age, the irrationality of Z(3).' (Apéry, 1996:58).

In summary, as one might expect, the processes that lead to new mathematical results and insights, are complicated, diversified, hard to understand and to grasp and, quite simply, tricky. Therefore, although for some limited sets of problems, a Polya set of heuristics may be helpful, it does not really address the hard issues.

To some extent, the same can be said for work being done in the field of psychology. The main focus is still on the development and growth of mathematical concepts in children and, occasionally, something is said about adults and about professional mathematicians, e.g., in Tall (1991). It does seem odd that the Hadamard book is still being referred to, although it dates from 1945 (strangely enough, also the publication year of Polya's *How to Solve It* and that too is still being referred to). That procedures such as generalization or reducing the problem to simpler cases can be extremely helpful and fruitful, does not really need any comment. But to move beyond that, is the core problem. Without going into any details (once more, I am afraid), it may seem rather ironic that one of the oldest approaches to the problem is still doing very well: *the method of analysis and synthesis*. For a recent overview, see Otte & Panza, 1997.

4.3. Math world or mad world?

Perhaps this is the right moment to return to one of my initial claims, viz. the fact that one's philosophical view of mathematics - both ontological and epistemological - will co-determine one's ideas about the growth and development of mathematics. Mathematical realists will happily compare the universe of numbers, sets and geometrical figures with the material world we are part of, but the comparison has to be treated extremely carefully. For, if the mathematical universe is a real universe, then it is a funny one, to say the least. In our material universe, it is pretty safe to generalize from time to time. After all, ravens do turn out to be black, and birds, notwithstanding Tweety and his friends, do tend to fly. However, math world is a mad world. Here are a few examples. (a) and (b) are well-known within the mathematical world, whereas (c) is a rather more general observation.

4.3.1 Approximation of the distribution of prime numbers

Let $\pi(n)$ be the function that counts the number of prime numbers $\leq$ n.

Let Li(n) - the logarithmic integral - be the function:

$$\int_2^n (1/\ln(x))dx, \text{ where } \ln(x) \text{ is the natural logarithm of } x.$$

The prime-number theorem says that Li(n) is an extremely good approximation of $\pi(n)$ (to be precise: Li(n) is asymptotically equal to $\pi(n)$).

For finite values for n, one notes, by direct calculation, that, although the difference is small, Li(n) > $\pi(n)$. Calculations up to 10^9 showed that this is the case. It seemed more than reasonable to conclude that this is always the case. Which it is not. Littlewood has shown that the difference Li(n) - $\pi(n)$ changes sign *infinitely many* times! The first estimate for what value of n this is supposed to happen, was given by Skewes. He arrived at the impressive number

$$10\hat{}(10\hat{}(10\hat{}34))),$$

meaning that a change of sign has to take place before this number. This upper bound was improved to $6{,}69.10^{370}$, still a quite impressive number. See Devlin (1988: 207-213) for more details.

4.3.2 Mertens Conjecture

If n is a natural number, then either n is divisible by the square of a prime, p^2, or not. In the latter case, we call n square-free. Now we define a function m(n) as follows:

- if n is not square-free: m(n) = 0
- if n is square-free and the number of primes in n is even: m(n) = 1
- if n is square-free and the number of primes in n is odd: m(n) = -1.

Example: m(6) = m(2.3) = 1, m(9) = 0, m(11) = -1.
Finally, define the function M(n) as follows:

$$M(n) = m(1) + m(2) + \ldots + m(n).$$

Mertens Conjecture claims that:

$$|M(n)| < \sqrt{n}.$$

Straightforward checking reveals that the inequality is satisfied for values of n into the billions. However, there is a counter-example for a value of n in the order of 10^{65}.

4.3.3. As equal as can be, yet different

To a certain extent, one expects to be 'fooled' almost all of the time. Think of the real numbers, that, classically speaking, come in two sorts: the algebraic reals and the transcendental reals. The former ones can be defined in terms of polynomials of a certain degree - e.g., $\sqrt{2}$ is one of the solutions of $x^2 - 2 = 0$ - whereas the latter ones are not so definable. Therefore to show that a specific real number is transcendental is not an easy task.

However, one of the criteria to be used is this:

> Given a number r, if there exists an infinite sequence of distinct rational numbers p_i/q_i, such that
> $|r - p_i/q_i| < 1/q_i^{ni}$ where n_i goes to infinity as i does,
> then r is transcendental.

This means that some transcendental numbers can be approximated almost arbitrarily close to rational numbers. Hence, to make the distinction will be extremely difficult and very often one expects that numerical calculations will lead one into an entirely wrong direction.

Another stunningly nice example, involving the two best known transcendental numbers, viz., π and e, is this (from Borwein & Borwein, 1992: 827). The following formula gives the correct value for π up to 42 billion digits and only then do things go wrong:

$$\pi = [(1/10^5)[\Sigma_n e^{-n^2/10\hat{}10}]]^2, \text{ where n goes from } -\infty \text{ to } \infty.$$

What is the point of these examples and comments? Even if we were to find a high quality set of heuristics that are able to deal with a mass of mathematical problems, one must still be prepared for the odd and queer thing every now and then. In other words, it is true that heuristics are not supposed to guarantee success in all cases, but, if one fails occasionally, one hopes for the best. In the math universe, the best thing to do is to fear for the worst.

I will not explore this line of approach any further and instead I will look at an alternative that has been developed in recent years: computer programs that prove theorems for you.

5. Success and failure of automated reasoning

Although the focus of this paragraph will be on automated reasoning, I will throw a brief look at some other approaches, again not aiming at being exhaustive. No doubt, one of the most famous programs, written by Douglas Lenat, is *Automatic Mathematician* (AM). This program does not prove theorems, it operates at a deeper level, namely the generation of new concepts on the basis of given concepts and the formulation of possibly interesting conjectures.

5.1. Artificial mathematician

The basic structure of AM is fairly simple: a small collection of basic, rather general notions and an extensive set of heuristics to apply to these concepts. Some examples:
(a) Suppose that two sets A and B are given, as well as a function f: A x A → B. Thus f(a,b) = c. In this case, an interesting heuristic is to see what happens if the two arguments are identified, thus obtaining a function g: A → B. If, e.g., f is multiplication, a.b = c, then g is the square function $a^2 = c$.
(b) Given any function f: A → B, see what happens if f is applied repeatedly (if such is possible, of course), say $f^n = f°f°f \ldots °f$ (n times). If, e.g., f is addition, thus f: N x N → N and the previous heuristic is applied, then we have the function g: N → N, such that g(a) = 2a. Repeated applications of g, produce functions that map a onto 2a, 3a, ..., na, in other words a basic multiplication appears.
(c) Given any function f: A → B, see what happens with the inverse function, if it exists. Thus, if multiplication is defined, a.b = c, division will be produced by this heuristic, taking into account the impossible case a/b, where b = 0.
(d) Given any function f: A → B, look at extreme cases, i.e., if some concept or other takes on values in a given range, look at the end-values to see what happens. Thus, e.g., if the notion of divisor is available, then one can construct the function d that maps numbers onto the number of divisors of that number (this function actually exists in number theory and

is a quite fundamental function). One extreme case is to look for the minimum of d(n). Clearly the lowest value is 2, thus those n for which d(n) = 2 are special. In fact, they are nothing else but the prime numbers.

(e) Given any function f: A → B, and a set of specific values of f, look for a pattern and formulate the conjecture that all values confirm to the proposed pattern. Example: continuing with the function d in the above example, suppose we look at the n, such that d(n) = 3. If AM generates a number of examples for this function, arguments such as 4, 25, 121, ... will come up. These are all squares, hence the conjecture: 'If d(n) = 3, then n = m^2, for some m' (which happens to be the case). There is actually an even stronger conjecture possible: 'd(n) = 3 if and only if n = m^2, where m is a prime'.

It is not easy to evaluate the values and shortcomings of AM in a few lines. I refer the reader to Boden's, 1990: 206-209, for a balanced judgment. Let me just mention that AM does not escape the horror of all computer scientists: combinatorial explosion. Unless additional meta-heuristics are fed into the system, AM will generate concept after concept, conjecture after conjecture, all things interesting and also all things uninteresting. But that, of course, is not a particular critique of AM, but of programs, intended to model a creative process, in general.

A lot of attention has been given to programs that are capable of checking existing proofs. No doubt, one of the most famous is the AUTOMATH program, developed by N.G. de Bruijn. But equally impressive are programs such as Mathematics Understander (MU) developed by Edmund Furse, and ONTIC, developed by David A. McAllester (see his (1989)). In the same range, are programs such as MACSYMA, REDUCE, MATHEMATICA, and so many others. An interesting overview is presented in Johnson et al. (1994). I will not discuss these programs but, instead, focus my attention on the underlying ideas of automated reasoning[9].

[9] There is one thing I must mention. In many of these approaches, the author or authors emphasize the double use of bottom-up and top-down strategies. In terms of looking for proofs, this translates into: (i) start from the axioms and derive as much as you can keeping in mind the conclusion you want to reach, and (ii) start with the conclusion and reason backwards keeping in mind what your axioms are. If there is an overlap somewhere, you will have the backbone of a proof. The thing worth mentioning is that

5.2. Automated reasoning

One of the major advantages of automated reasoning (AR) is that the *basic* ideas are extremely easy to explain. However, spelling out the basics, is only a minor part of the whole undertaking of AR. To illustrate the basis, I will first say a few things about classical propositional logic (PC) and then about classical first-order predicate logic (PL)[10].

5.2.1. Automated reasoning in propositional calculus

Classical logic has the extremely nice property that every formula A can be rewritten in a standard format A-*cnf*, the conjunctive normal form. A formula in A-*cnf* format consists of a series of conjunctions (possibly empty), each conjunct itself is a series of disjunctions (possibly empty), and the members of the disjunctions are either letters p, q, r, ... or negated letters. Thus, e.g., the formula

$$(p \supset q) \supset (\sim q \supset \sim p)$$

becomes

$$(p \vee q \vee \sim p) \; \& \; (\sim q \vee q \vee \sim p).$$

If we drop the conjunctions, then we are left with clausal forms:

(i) $p \vee q \vee \sim p$
(ii) $\sim q \vee q \vee \sim p$.

Why is this interesting? Because one can show that all logical *rules* can be reduced to one *single* rule, the so-called resolution rule:

> Suppose that two formulas are given in *cnf* format and such that:
> (i) $A_1 \vee A_2 \vee \ldots \vee p \vee \ldots \vee A_n$

this procedure is nothing but a modern translation of the well-known method of analysis and synthesis. One is tempted to say: *nihil novi sub sole.*

[10] The ideas about AR here presented are taken from Wos et al., 1992, and from Bundy, 1983.

(ii) $B_1 \vee B_2 \vee \ldots \vee {\sim}p \vee \ldots \vee B_m$,

then one can conclude to:

(iii) $A_1 \vee A_2 \vee \ldots \vee A_n \vee B_1 \vee B_2 \vee \ldots \vee B_m$.

In words: if in two formulas one has an occurrence of a letter p and the same letter with negation, then the two clauses can be joined into a new clause deleting p and the negation of p.

With this material at hand, it becomes easy to prove theorems. One of the standard ways is through refutation. If one has to show that B follows from a set of premisses $A_1, A_2, \ldots, A_n$, rewrite all premisses and the negation of the conclusion in *cnf* format and try to find a contradiction - indicated by the *empty* clause, f - by successive applications of the resolution rule.

Example: show that $p \supset s$ follows from $(p \vee q) \supset r$ and $r \supset s$

The translation in *cnf* format gives the following clauses:

1. $\sim p \vee r$
2. $\sim q \vee r$
3. $\sim r \vee s$
4. p
5. $\sim s$

Application of the resolution rule gives:

6. $\sim r$ (from 3 and 5)
7. $\sim p$ (from 1 and 6)
8. f (contradiction, from 4 and 7).

Of course, since PC is decidable (although NP-hard), we know that this method will always produce correct answers. For PL the situation is more interesting.

5.2.2. *Automated reasoning in predicate logic*

First the good news. As in PC it is possible to rewrite any formula in a standard format. I will not go into details, but generally speaking the standard format, the so-called prenex normal form (*pnf*) has all the quantifiers in front and then a quantifier-free expression in *cnf* format. Just as in PC it is possible to work with (as good as) one single rule, the full resolution rule. So it seems that we can do the same things as in PC.

However, as we know, PL is not decidable, therefore repeated applications of the rule do not necessarily lead to certain success. Mathematics needs at least PL, so there is the challenge. Basically, two options are open:

(a) *Find restricted cases*: There are parts of PL that are decidable, hence for these cases an algorithm can be formulated.

(b) *Search for heuristics*: Find additional "rules" that can help to give guidance to the search for the empty clause.

It would be extremely unfair to take one page or half a page in order to evaluate the virtues and faults of AR. I will list a few of the successes for the simple reason that most of mathematicians, logicians and philosophers are deeply convinced that the general value of AR is close to zero. And it has to be said, there are some nice results.

(i) One of the really impressive and extremely recent results is the solution to the problem of *Robbins algebras*. The question is quite simple. Given the following axioms, that define a Robbins algebra:

(R1) $(\forall x)(\forall y)(x + y = y + x)$,
(R2) $(\forall x)(\forall y)(\forall z))((x + y) + z = x + (y + z))$,
(R3) $(\forall x)(\forall y)(-(-(x + y) + -(x + -y)) = x)$,

show that you have a Boolean algebra.

As the other way is easy to show, the question comes down to showing that Robbins algebras are the same as Booleans algebras. I refer the reader to McCune, 1997, for an overview of this problem and how the solution was found. I will limit myself to some general remarks. The basic approach has been to find additional statements A such that the Robbins axioms together with A produce a proof of the equivalence with a Boolean algebra. The problem was then reduced to proving A from the axioms (R1), (R2), and (R3). This history in itself is quite intriguing. Here is a list of some of these formulas:

(A1) $(\forall x)(--x = x)$,
(A2) $(\exists y)(\forall x)(y + x = x)$,
(A3) $(\exists y)(\forall x)(1.x = x)$,
(A4) $(\forall x)(x + x = x)$,
(A5) $(\exists x)(x + x = x)$,

$$(A6)\ (\exists x)(\exists y)(x + y = y).$$

Especially (A4) through (A6) are fascinating, as each one is weaker than its predecessor. Note that this practice of looking for intermediate statements is standard practice among human mathematicians.

(ii) AR programs are extremely good at generating counter-examples and finite models. One might perhaps think that this is trivial, but it is not. For the simple reason that a blind generation of all possibilities, even if finite, is exponentially difficult. Thus a guided search is needed. Using this technique, it has been possible to answer some questions in the theory of finite semi-groups (see Wos et al., 1992: 320-323). Looking outside of the domain of mathematics, this technique has proven its worth in formal logic.

(iii) Inspired by AR and other programs, some curious results have appeared. Bailey et al., 1997, discuss diverse methods for calculating the decimals of π and observe that most identities converge far too slow[11]. Thus, better identities are needed. On the one hand, the work of Ramanujan has been a source of inspiration, and, on the other hand, for the purpose of calculating individual digits, a computer method (called 'PSLQ') was used to generate new identities, such as (where i runs from 0 to infinity):

$$\pi = \Sigma_i\ (1/16^i)[4/(8i+1) - 2/(8i+4) - 1/(8i+5) - 1/(8i+6)]$$

Apart from the fact that this sort of identity makes one think of Apéry's proof, it is important to realize that the program looks for identities on the basis of numerical identity and then a proof was searched for.

For similarly inspired work, see Wilf & Zeilberger, 1990. They present a general method for generating identities where the proof can be automatically checked.

Finally, I might add that AR gives a nice formal idea of *reasoning by analogy*. Suppose that a proof of a statement A follows a particular route, selected by the heuristics applied, then you obtain a proof schema.

[11] If someone happens to be interested, according to the paper of Bailey et al. (1997), the current 'record' is 6.442.450.938 decimals. However, now (= June 1998) the correct number is close to $51{,}5.10^9$ decimals. This impressive result has been achieved by Yasumasa Kanada.

This schema can be used as the proof frame for a proposition similar to A.
Example: Think of proof by infinite descent (see above). This is indeed a proof schema that can be applied to any Diophantine problem as a heuristic. For a nice and interesting example, see Melis, 1998.

5.3. Proofs from the unexpected

What goes for humans, goes for machines. At least in this case. It is obvious that automated reasoning does shed new light on what the search for and the nature of a mathematical proof is. At the same time, I wish to repeat my comment made before that the mathematical universe, if there is any such thing at all, is a strange place. The same goes for proofs. I do not doubt that many proofs are standard and do not involve anything strange or bizarre, but, nevertheless, occasionally one must wonder. To end this section, let me present a few of such proofs[12].

Example 1
The following definition is given. For n a natural number, define S(d) as the sum of its divisors. Then three cases are possible:
(i) $S(d) = 2n$, the number is perfect,
(ii) $S(d) > 2n$, the number is abundant,
(iii) $S(d) < 2n$, the number is deficient.
Prove that every even number greater than 46 can be expressed as the sum of two abundant numbers. (Honsberger, 1970: Essay Fourteen).

Confronted with this problem for the first time, it seems a reasonable strategy to take two abundant numbers a and b and to wonder what properties their sum $a + b$ must have. Although this might perhaps be successful, a rather direct solution is given through proving the following lemma:

> If a number n is perfect or abundant, then its multiples are abun-

[12] It is almost inevitable that the example should be given of the chess-board with two opposite corners removed and the problem to solve is to show that the board cannot be covered with bricks that cover exactly two squares. As everybody gives this example, one might have the impression that this is the only example. Hence, I present here three different examples.

dant. (I leave the quite simple proof to the reader).

The next step is to write the number n as 6k + m, where m = 0, 2 or 4. If m = 0, then n = 6k = 6k' + 6k", and, as 6 is a perfect number, n is abundant. If m = 2, then n = 6k' + 20, and, as 20 is abundant, so is n. If m = 4, then n = 6k' + 40, and, as 40 is abundant, so is n. QED.

Example 2

Consider 18 consecutive natural numbers, smaller than 1.000. Show that at least one of these numbers is divisible by the sum of its digits.

The shortest proof I know relies on the simple fact that if the number is abc then $a + b + c \leq 27$. Exclude 999 (no problem for 999 is divisible by 27), then $a + b + c < 27$. In a row of 18 numbers, there is at least one multiple of 18. That number is divisible by 9 and by 2, hence the sum of its digits is divisible by 9, thus a + b + c = 9 or 18. QED

Example 3

This problem is truly my favourite, because things cannot get any simpler than this. Consider a real function $f: R \rightarrow R$. A real function f is *symmetric* if f(x) = f(-x), *anti-symmetric* if f(x) = -f(-x). Show that any real function is the sum of a symmetric and anti-symmetric function.

Probably one would tend to 'subtract' from f a symmetric function g and then try to show that f - g is an anti-symmetric function under certain conditions. Whereas the answer is just this:

$$f(x) = [f(x) + f(-x)]/2 + [f(x) - f(-x)]/2$$

Obviously f(x) + f(-x) = f(-x) + f(x) and f(x) - f(-x) = -[f(-x) - f(x)]. QED

Generally speaking, it is this sense of unexpectedness that seems quite difficult to be captured by AR. But do note at the same time that human mathematicians consider these proofs to be ingenious as well. Freely translated, this means that they themselves did not expect a proof of this kind. So, once again human and machine meet.

6. Afterthought

The contents of this paper are of an almost entirely descriptive nature. I have tried to bring together some elements that must be part of such a description, if it claims to be representative of mathematical practice as we know it. All this being said and done however, there is a subsequent question to consider: is mathematical practice, as it is, the best we have? Is there room for improvement? Is it possible that not all aspects of the proof idea have been explored? I have no other choice than to reiterate a comment made several times in the course of this text: to answer these questions, one's philosophical views enter into the picture. If, e.g., one believes that there is such a thing as the ideal proof, and one believes that this ideal is humanly reachable, then there will be a moment where things can improve no further[13]. If, however, one believes that mathematics is (nothing but) a human product, then, on the basis of this description, it does leave room for further reflection and it opens the possibility of 'planning' mathematics itself in a particular direction.

This last idea is not ludicrous at all. I end this paper by mentioning the interesting but not enough mentioned work done by van Gasteren in her 1990, where she proposes that mathematicians should try to present their proofs in such a way that maximum clarity is achieved. One of her motives is that such proofs are easier to check using automated reasoning programs and thus a certain division of labour within the mathematical community can be installed. After all, whether one likes it or not, mathematics is a social phenomenon from this perspective as well.

Vrije Universiteit Brussel

[13] In my (1993) I have presented a sketch of this ideal mathematical community (IMC). Its basic characteristics are: (a) in the IMC, all members are equal, (b) the IMC is relatively isolated from the rest of society, (c) all members of the IMC share the same idea of the existence of a unique mathematical universe U (independent of the question whether this is actually the case) and the task of mathematics is the search for a complete description of U, (d) all members share the idea that there is a unique or preferred language L wherein this description is formulated, (e) for any mathematical statement, if there is a proof, then it can, in principle, be found by any mathematician, (f) any proof of any statement can be checked by any mathematician, and, finally, though optional, (g) how the proof is to be found is mostly a matter of some kind of innate capabilities. Do note that the description of the IMC is a lot poorer than the real(istic) community.

REFERENCES

The list of references is quite extensive. It is not meant to impress the reader but it is the consequence of the set-up of this paper. I have tried to cover as many areas as possible, each time with indications where to proceed therefrom if the discussion in this paper is unsatisfactory for the reader.

Alexandrov, P.S. (ed.) (1971). *Die Hilbertschen Probleme*. Leipzig: Akademische Verlagsgesellschaft, Geest & Portig.

Apéry, François (1996). 'Roger Apéry, 1916-1994: A Radical Mathematician'. *The Mathematical Intelligencer*, vol. 18, 2, 54-61.

Appel, Kenneth & Wolfgang Haken (1989). *Every Planar Map is Four Colorable*. Providence: AMS (Contemporary Mathematics, vol. 98).

Bailey, D.H.; J.M. Borwein; P.B. Borwein & S. Plouffe (1997). 'The Quest for Pi'. *Mathematical Intelligencer*, vol. 19, 1, 50-57.

Bell, John L. (guest ed.) (1994). *Categories in the Foundations of Mathematics and Language*. Special issue of *Philosophia Mathematica*, vol. 2, first third.

Boden, Margaret (1990). *The Creative Mind*. London: Sphere Books.

Borwein, Jonathan & Peter Borwein (1992). 'Some Observations on Computer Aided Analysis'. *Notices of the AMS*, vol. 39, 8, 825-829.

Browder, Felix E. (ed.) (1976). *Mathematical Developments Arising from Hilbert Problems*. Providence: AMS. (Proceedings of Symposia in Pure Mathematics, vol. 28).

Bundy, Alan (1983). *The Computer Modelling of Mathematical Reasoning*. New York: Academic Press.

Cipra, Barry (1996). *What's Happening in the Mathematical Sciences, 1995-1996, volume 3*. Providence: AMS.

Corry, Leo (1992). 'Nicolas Bourbaki and the Concept of Mathematical Structure'. *Synthese*, 92:315-348.

Crowe, Michael (1992): 'Ten 'laws' concerning patterns of change in the history of mathematics'. In: Gillies, Donald, 15-20 (originally published in 1975).

Dauben, Joseph: 'Conceptual revolutions and the history of mathematics: two studies in the growth of knowledge.' In: Gillies, Donald, 49-71 (originally published in 1984).

Devlin, Keith (1988). *Mathematics: The New Golden Age*. Harmondsworth: Penguin.

Dieudonné, Jean (1987). *Pour l'honneur de l'esprit humain. Les mathématiques aujourd'hui*. Paris: Hachette.

Duda, Roman (1997). 'Mathematics: Essential Tensions'. *Foundations of Science*, vol. 2, 1, 11-19.

Dunham, William (1990). *Journey Through Genius. The Great Theorems of Mathematics*. New York: John Wiley & Sons.

Echeverria, Javier (1996). 'Empirical Methods in Mathematics. A Case Study: Goldbach's Conjecture.' In: Munévar, Gonzalo (ed.), *Spanish Studies in the Philosophy of Science*. Dordrecht: Kluwer Academic, p.19-55.

Gelbart, Stephen (1984). 'An Elementary Introduction to the Langlands Program'. *Bulletin (New Series) of the American Mathematical Society*, volume 10, number 2, 177-219.

Gillies, Donald (ed.) (1992). *Revolutions in Mathematics*. Oxford: Clarendon Press.

Glas, Eduard (1981). *Wiskunde en samenleving in historisch perspectief.* Muiderberg: Coutinho.

Glas, Eduard (1991a). 'Lakatos revisited'. *Kennis en Methode*, XV, 3, 307-311.

Glas, Eduard (1991b). 'Koetsiers verfijnde metamethodologie - een repliek'. *Kennis en Methode*, XV, 4, 404-405.

Gorenstein, Daniel (1986). 'Classifying the Finite Simple Groups'. *Bulletin (New Series) of the AMS*, 14:1-98.

Graham, L.A. (1959). *Ingenious Mathematical Problems and Methods*. New York: Dover Publications.

Grattan-Guinness, Ivor (1997). *The Fontana History of the Mathematical Sciences*. London: Fontana Press.

Grimmett, Geoffrey & Dominic Welsh (1994). *Probability. An Introduction.* Oxford: Clarendon Press.

Hersh, Reuben (1997). *What is Mathematics, Really?* London: Jonathan Cape.

Honsberger, Ross (1970). *Ingenuity in Mathematics*. Washington: New Mathematical Library, MAA.

Johnson, Jeffrey; Sean McKee & Alfred Vella (eds.) (1994). *Artificial Intelligence in Mathematics*. Oxford: Clarendon Press.

King, Jerry P. (1992). *The Art of Mathematics*. New York: Plenum Press.

Kitcher, Philip (1983): *The Nature of Mathematical Knowledge*. Oxford: Oxford University Press.

Koetsier, Teun (1991). *Lakatos' Philosophy of Mathematics. A Historical Approach*. New York/Amsterdam: North-Holland. (Studies in the History and Philosophy of Mathematics, volume 3).

Kuhn, Thomas (1977). *The Essential Tension. Selected Studies in Scientific Tradition and Change*. Chicago: University of Chicago Press.

Lakatos, Imre (1976). *Proofs and Refutations*. Cambridge: Cambridge University Press.

Langley, Pat; Herbert A. Simon, Gary L. Bradshaw & Jan M. Zytkow (1987).

Scientific Discovery. Computational Explorations of the Creative Processes. Cambridge, Mass.: MIT.

Lenat, D.B. (1980). 'AM: Discovery in Mathematics as Heuristic Search'. In: R. Davis & D.B. Lenat (eds.). *Knowledge-Based Systems in Artificial Intelligence.* New York: McGraw-Hill, 3-228.

MacLane, Saunders (1986). *Mathematics. Form and Function.* Heidelberg: Springer.

McAllester, David A. (1989). *ONTIC. A Knowledge Representation System for Mathematics.* Cambridge, Mass.: MIT.

McCune, William (1997). 'Solution of the Robbins Problem'. *Journal of Automated Reasoning*, vol. 19, no.3, 263-276.

Melis, Erica (1998). 'The Heine-Borel Challenge Problem. In Honor of Woody Bledsoe'. *Journal of Automated Reasoning*, vol. 20, 3, 255-282.

Munévar, Gonzalo (ed.) (1996). *Spanish Studies in the Philosophy of Science.* Dordrecht: Kluwer Academic (BSPS volume 186).

Northrop, Eugene P. (1978). *Riddles in Mathematics.* Harmondsworth: Penguin.

Otte, M. & M. Panza (eds.) (1997). *Analysis and Synthesis in Mathematics.* Dordrecht: Kluwer.

Polya, Georg (1945). *How to solve it. A new aspect of mathematical method.* Princeton: Princeton University Press. [New York: Doubleday Anchor Books, 1957.]

Rav, Yehuda (1993). 'Philosophical problems of mathematics in the light of evolutionary epistemology.' In: Restivo, Sal et al (eds.). *Math Worlds: New Directions in the Social Studies and Philosophy of Mathematics.* New York: State University New York Press, 80-109.

Restivo, Sal (1983). *The Social Relations of Physics, Mysticism, and Mathematics.* Dordrecht: Reidel.

Restivo, Sal (1992). *Mathematics in Society and History.* Dordrecht: Kluwer Academic.

Restivo, Sal; Jean Paul Van Bendegem & Roland Fischer (eds.) (1993). *Math Worlds: New Directions in the Social Studies and Philosophy of Mathematics.* New York: State University New York Press.

Ribenboim, Paulo (1989). *The Book of Prime Number Records.* Heidelberg: Springer.

Schoenfeld, Alan H. (1985). *Mathematical Problem Solving.* New York: Academic Press.

Stewart, Ian (1987). *The Problems of Mathematics.* Oxford: Oxford University Press,. Oxford.

Tall, David (ed.) (1991). *Advanced Mathematical Thinking.* Dordrecht: Kluwer (Mathematics Education Library).

Taylor, Richard and Andrew Wiles (1995). 'Ring-theoretic properties of certain

Hecke algebras'. *Annals of Mathematics*, Second Series, vol. 141, 3, 553-572.

Tymoczko, Thomas (ed.) (1986). *New Directions in the Philosophy of Mathematics*. Stuttgart: Birkhäuser.

Van Bendegem, Jean Paul (1987). 'Fermat's Last Theorem seen as an Exercise in Evolutionary Epistemology'. In: Werner Callebaut & Rik Pinxten (eds.), *Evolutionary Epistemology*. Dordrecht: Kluwer, 337-363.

Van Bendegem, Jean Paul (1988). 'Non-Formal Properties of Real Mathematical Proofs'. In: Arthur Fine and Jarrett Leplin (eds.), *PSA 1988. Volume One.* East Lansing: PSA, 249-254.

Van Bendegem, Jean Paul (1990a). 'Characteristics of Real Mathematical Proofs'. In: A. Diaz, J. Echeverria and A. Ibarra (eds.), *Structures in Mathematical Theories*. San Sebastian: Servicio Editorial Universidad del País Vasco, p.333-337.

Van Bendegem, Jean Paul (1993). 'Foundations of Mathematics or Mathematical Practice: Is One Forced to Choose?' In: S. Restivo, J.P. Van Bendegem & R. Fischer (eds.), p.21-38.

Van Bendegem, Jean Paul (1996): 'Mathematical Experiments and Mathematical Pictures'. In: Igor Douven & Leon Horsten (eds.), *Realism in the Sciences. Proceedings of the Ernan McMullin Symposium Leuven 1995*. Louvain Philosophical Studies 10. Leuven: Leuven University Press, p.203-216.

van Gasteren, A.J.M. (1990). *On the Shape of Mathematical Arguments*. Heidelberg: Springer.

Wells, David (1991). *The Penguin Dictionary of Curious and Interesting Geometry*. Harmondsworth: Penguin Books.

Wilder, Raymond L. (1981). *Mathematics as a Cultural System*. Oxford: Pergamon Press.

Wiles, Andrew (1995). 'Modular elliptic curves and Fermat's Last Theorem'. *Annals of Mathematics*, Second Series, Vol. 141, 3, 443-551.

Wilf, Herbert S. & Doron Zeilberger (1990). 'Towards computerized proofs of identities'. *Bulletin (New Series) of the AMS*, vol. 23, 1, 77-83.

Wos, Larry; Ross Overbeek; Ewing Lusk & Jim Boyle (1992). *Automated Reasoning. Introduction and Applications*. New York: McGraw-Hill.