From the Book *Proof and Other Dilemmas*
Bonnie Gold & Roger A. Simons, Editors
MAA 2008

3
On the Roles of Proof in Mathematics

Joseph Auslander
Department of Mathematics
University of Maryland

From the Editors

This third perspective on proof comes from a mathematician with a more traditional perspective than Borwein’s. The author brings his considerable experience both in developing his own proofs and in reviewing others’ to questions about the roles of proof. His discussion on the roles of proof contains some interesting new ideas, such as proof as exploration and proof as justification of definitions—ideas that are relevant to us as we think about how we teach mathematics. At the end he offers some extended illustrations of his main points, from his experience working in topological dynamics and ergodic theory.

Joseph Auslander is a Professor Emeritus of Mathematics at the University of Maryland. He has published extensively in topological dynamics and ergodic theory. He is the author of Minimal Flows and Their Extensions (1988) and co-editor with Walter H. Gottschalk, of Topological Dynamics, an international symposium (1968). He has published two reviews of books in the philosophy of mathematics: What is Mathematics, Really? by Reuben Hersh, Where Mathematics Comes From: How the Embodied Mind Brings Mathematics into Being by George Lakoff and Rafael E. Núñez. Those reviews appeared in SIAM Review (2000) and American Scientist (2001), respectively. With Bonnie Gold, he organized a panel for the winter 2001 joint mathematics meetings in New Orleans on “The Philosophy of Mathematics: That Which is of Interest to Mathematicians,” which led to the founding of POMSIGMAA. He was the first Secretary of POMSIGMAA, and gave a talk, “When is a Proof a Proof?” at the POMSIGMAA contributed paper session in January 2004.
In this article, I will make, and try to justify, the following points.

Deductive proof is almost the defining feature of mathematics. Mathematics without proof would not be mathematics. This is so although mathematics consists of more than proof, and proof occurs in other disciplines.

Proof is necessary for validation of a mathematical result. But there are other, equally compelling reasons for proof.

Standards of proof vary over time, and even among different mathematicians at a given time. The question of “when is a proof a proof?” is a complex one. This has always been an issue, but it is particularly so now in the light of computer assisted proofs and very long proofs.

1 Proof as a Defining Feature of Mathematics

I am writing as a working mathematician, not as a philosopher. My approach to proof is consistent with the viewpoint, cogently put forth by Reuben Hersh [1997] and Paul Ernest [1998], that mathematics is socially constructed. That is, it has been constructed by humans, and is part of human culture. Therefore I will focus on what mathematicians actually do. This is what Hersh calls “practical proof—the argument that convinces the qualified skeptical expert” rather than formal proof.

Thomas Hales clarifies this distinction well [Hales www.]:

“Traditional mathematical proofs are written in a way to make them easily understood by mathematicians. Routine logical steps are omitted. An enormous amount of context is assumed on the part of the reader. Proofs, especially in topology and geometry, rely on intuitive arguments in situations where a trained mathematician would be capable of translating those intuitive arguments into a more rigorous argument.” This is distinguished from formal proof where “all the intermediate logical steps are supplied” and “no appeal is made to intuition.”

I will not try to give a precise definition of mathematics; the definitions I’ve seen are either too restrictive or too inclusive, but certainly the use of deductive proof is an essential feature. Mathematics is not just about “results.” (One might refer to the belief in the primacy of results to the exclusion of anything else as the “Vince Lombardi” approach, after the football coach who said that “winning is the only thing.”)

Mathematics is a process, which includes definitions, conjectures, examples, numerical evidence, statements of theorems, modelling, algorithms, and proofs, as well as heuristic arguments which fall short of proof. These are all woven together. In particular the proof is inextricably bound up with the result; indeed one can’t really separate them. This is part of the aesthetics of mathematics, but it also has “practical” consequences. Proofs often contain “subresults,” as well as implicit or explicit lemmas, which are of interest in themselves. These would be lost if one just catalogued “results.” Moreover, often a proof yields more than is explicitly stated, and it may point the way to new theorems. This is illustrated by Hillel Furstenberg’s proof of the Szemeredi theorem, which will be discussed below.

As John Franks [1989] eloquently puts it “a proof is not some kind of super spell checker that merely validates mathematical facts…Proofs (are) the central content of mathematical knowledge…Who would be satisfied if God were to announce that the Riemann hypothesis is true, but deny us the proof?” (Regarding the last point, we might ask if we would be satisfied if
A computer "announced" that a theorem had been proved, but we couldn't see the proof. See the section on "Proof as Certification" for more about this.

Another gloss on this topic was stated by the biologist Richard Lewontin [2005] writing in the New York Review of Books: "Science, indeed scholarship in general, is a domain in which the integrity of the process is more important than... any particular result. This is... a question of the very survival of the process of investigation." Lewontin in this passage was concerned with issues of honesty and fraud in science, but the point holds in a more general context.

As was mentioned above, mathematics is not only about proof. Moreover, the notion of proof also occurs in other areas (in other sciences of course—physical, biological, and social—and also such disciplines as law and history) but it has a somewhat different meaning, and different methods are used to attain it. These are characterized by a mixture of deductive reasoning and empirical evidence. Debates about the relation of these are at the heart of the philosophy of science.

I should say at the outset that I am definitely not asserting that proofs in mathematics are in some sense more "valid" than those in other disciplines. Rather, there are different methods of arriving at conclusions, and that deductive proof is central to mathematics to a much higher degree than in other areas. This is in spite of some challenges to this central role and even some predictions of the "death of proof."

We might accept as a provisional definition of proof a (valid) sequence of deductions, starting with the hypothesis, and arriving at the conclusion. Somewhat more formally [Kitcher 1984, p. 38] "We can now define a proof as a sequence of statements such that every member of the sequence is either a basic a priori statement or a statement which follows from previous members of the sequence in accordance with some apriority-preserving rule of inference."

This is somewhat at variance with our earlier emphasis on "practical proof," and in fact this tension is one of the things that makes the issue interesting. Nevertheless, mathematicians do feel that their proofs essentially accomplish what Kitcher describes (as the quotation from Hales in Section 1 points out). In fact, it's fair to say that this is a necessary and sufficient condition for a proof. That is, if this is achieved, we have a proof, and if it isn't there is no proof.

In a sense, that's all there is to it. As Gian-Carlo Rota [1996] puts it, "Mathematical proof does not admit degrees. A sequence of steps in an argument is either a proof, or it is meaningless... The mathematical notion of proof is strikingly at variance with notions of proof in... law, everyday conversation, and physics."

However, I will argue that the situation is more complex than Rota makes it out to be. While any two mathematicians will agree in the abstract what a proof is, it's when one gets down to cases that problems may arise. Many of these can be reduced to "how do we know that a theorem has in fact been proved?" For example, what about "Proof: Obvious," or "Proof: This follows from the previous lemma?" At the other extreme, how do we evaluate a 15000 page proof, which may itself rely on papers the author hasn't read? Or a proof dependent on an unpublished or unobtainable paper? Or, a hot topic these days, a proof making use of computer calculations?

The issue of proofs in elementary and secondary school mathematics has been much discussed. Many (this writer included) lament the lack of emphasis on proofs in today's high school geometry classes, in contrast to what occurred in previous generations. The following quotation of Ken Ross [1998] addresses this point.

"While science verifies through observation, mathematics verifies through logical reasoning. Thus the essence of mathematics lies in proofs... It should be emphasized that results in mathematics follow from hypotheses... Moreover, beginning in the 8th
grade, students should distinguish between inductive and deductive reasoning, be able to identify the hypothesis and conclusion in a deduction, test an assertion with examples, realize that one counterexample is enough to show that an assertion is false, and recognize whether something is being proved or merely given a plausibility argument.”

2 The Roles of Proof

Mathematicians have a range of views on the role of proof in mathematics. Several of these views are illustrated by the following quotations, in which I have italicized words that emphasize the role of proof being mentioned.

Hyman Bass [2003]: “The characteristic that distinguishes mathematics from all other sciences is the nature of mathematical knowledge and its certification by means of mathematical proof... it is the only science that thus pretends to claims of absolute certainty.”

Gian-Carlo Rota [1993, p. 93]: “Mathematicians cannot afford to behave like physicists, who take experimental verification as confirmation of the truth.”

In fact, the physicist Steven Weinberg [2001] makes essentially the same point as Rota: “You give up worrying about certainty when you make that turn in your career that makes you a physicist rather than a mathematician.”

David Gale [1990]: “The main goal of science is to observe and then to explain phenomena. In mathematics the explanation is the proof... the theorem-proof methodology... is the only methodology we have.”

Philip Davis and Reuben Hersh [1981, p. 151]: “Proof serves many purposes simultaneously... (It is) subject to a constant process of criticism and revalidation. Errors, ambiguities, and misunderstandings are cleared up by constant exposure. Proof is respectability. Proof is the seal of authority... (It) increases understanding by revealing the heart of the matter. Proof suggests new mathematics. Proof is mathematical power, the electric voltage of the subject which vitalizes the static assertions of the theorems.”

Saunders Mac Lane [Responses 1994, p.190]: “Intuition is glorious, but the heaven of mathematics requires much more... Mathematics rests on proof—and proof is eternal.”

There is no doubt that the overwhelming majority of mathematicians is committed to proofs in the traditional sense, and endorses the sentiments, if not the exact wording of the above quotations. Later, I’ll express reservations about some of the assertions.

I would like to single out several (not unrelated) roles of proof, including certification (or validation), explanation, and exploration.

2.1 Proof as Certification

We accept that a purported result is correct when we hear that it has been proved by a mathematician we trust and “validated” by experts in the author’s mathematical specialty. This is the case even if we haven’t read the proof, or more frequently when we don’t have the background to follow the proof. As an extreme, perhaps hackneyed, example, mathematicians accept Wiles’ proof of Fermat’s last theorem because number theorists have “certified” it to be correct. While certification is the most “primitive” or “elementary” aspect of proof, it is worthwhile looking at this role more closely. It is an indication that we are part of a community whose members trust one another. In fact, mathematics could not be a coherent discipline, as opposed to a random collection of techniques and results, without the process of certification.
3. On the Roles of Proof in Mathematics

Usually, certification of a result is a consequence of its appearance as a paper in a refereed journal. In fact, we might agree that this is a necessary condition for certification. In this case it is generally accepted that the "burden of proof" (the pun is inevitable) has shifted, and the result is presumed correct, unless there is a compelling reason to believe otherwise. It should be emphasized that it's necessary that one is convinced that a competent mathematician has worked out the proof, rather than it being "announced" by "God" (as in the quotation from John Franks earlier).

However, this process is far from perfect, and should be regarded as provisional. For one thing, it is well known that standards of refereeing vary widely. Some papers—for example, the proof of Fermat's last theorem, and Hales' proof of the Kepler conjecture discussed below—concern famous problems, and thus have received intense scrutiny. Other papers receive more routine treatment. Ralph Boas, who was for many years the editor of Mathematical Reviews, is said to have remarked that of the new results in papers reviewed most are true but the corresponding proofs are perhaps half the time wrong.

An interesting example was the published assertion by Waraszkiewicz [1937], that a homogeneous plane continuum is necessarily a simple closed curve. This "result" was generally accepted, and in fact a more general assertion was published by Choquet [1944]. However, a counterexample was provided by Bing [1948]. (Another example will be discussed in the section "Four Examples.")

Also, referees are generally told that it is not their job to determine whether a paper is correct—this is the responsibility of the author—although the referee should be reasonably convinced. The referee is typically asked to determine whether the paper is worthwhile. Of course this begs the question somewhat. If the result is not correct, then the paper is not worthwhile. In the case of very long papers, referees usually don't try to check every line. Robert MacPherson, an editor of the Annals of Mathematics says "I try to understand the internal logic of the proof and do consistency checks." [Szpiro 2003, p. 208] Moreover, there are (presumably refereed) papers in respectable journals where the claimed result is false (in some cases not so noted for many years).

The issue of the refereeing process—real and ideal—in mathematics is fascinating and largely unexplored. Gossip on this topic abounds but I know of no systematic study.

Certification of a result allows us to use it in further research. In theory, one just checks the hypotheses, and if they are appropriate to the given situation, applies the result and goes on from there. This may be necessary (one can't develop all of mathematics each time one writes out a proof) but it brings along certain dangers. For reasons which aren't entirely clear, applying a result mechanically, without an understanding of the proof, can lead to errors. For example, sometimes one is fooled by notation. (This is borne out by my own experience. In fact, on one occasion I was attempting to apply something I had proved earlier without thinking it through carefully, and I made an elementary error.)

The point is that a mathematician is not absolved from understanding the proof, even when the result in question has been accepted by the mathematical community. When one uses a result in one's own research or teaching, the stakes are higher. It then becomes necessary to understand at least the basic outlines of the proof. One requires a higher degree of certainty for the use of a result than is obtained by the passive acceptance of it.

This was put well by Daniel Biss [2004]: "No honest mathematician uses a result simply because it has been published. Rather we use results we trust are true... the defining threshold for this notion is... a complex mélange of what has been published, what has been accepted as true by a larger community, and... what we believe ourselves to understand."
There is a recent tendency for (some) mathematicians to post their papers on preprint servers. Frequently this is preliminary to the submission of these papers to a journal (in which case it's not particularly different from the former practice of the distribution of preprints, allowing access of the results to researchers in the field prior to publication), but in some cases there is no intention of submission to a journal. Even given the imperfect process of refereeing, this somewhat undermines the certification of the results in question.

2.2 Proof as Explanation

Our second role of proof is explanation. This is what concerns most mathematicians. One should be able to follow at least the broad outlines of the argument, and be confident that one can fill in the details. As Andrew Gleason [Yandell 2001, p. 150] points out, "Proofs really aren't there to convince you that something is true ... they're there to show you why it is true."

Ideally this is what proof is all about. Almost by definition, a proof is supposed to explain the result. Now, it must be admitted that not all proofs meet this standard. To some extent this is in the eye of the beholder. Indeed sometimes the conviction that a result is correct may arise not from the proof, but from (say) numerical evidence, illuminating examples, or visual representation. Such considerations have often led to the development of new, more understandable, proofs.

The great mathematician Paul Erdős spoke of "The Book" in which "God" maintained the "perfect" proofs of theorems. In fact there is a real book, appropriately titled *Proofs from THE BOOK* by Martin Aigner and Gunter Ziegler [1999] which presents many proofs in this spirit. Erdős collaborated on this book shortly before his death, and many of the proofs are due to him.

The first chapter consists of six different proofs of the infinity of primes, starting with the familiar proof due to Euclid. The sixth proof, due to Erdős, proves more, namely that the sum of the reciprocals of the primes diverges. (The first proof of this fact was given by Euler.) Erdős' proof is by contradiction—suppose the sum converges. If $p_1, p_2, \ldots$ is the sequence of primes written in increasing order, then there is a $k$ such that $\sum_{i \geq k+1} \frac{1}{p_i} < \frac{1}{2}$. Call $p_1, \ldots, p_k$ the small primes, and the others the big primes. For a fixed $N > 0$ let $N_b$ be the number of $n \leq N$ which are divisible by at least one big prime, and $N_s$ the number of such integers with only small prime divisors. Clearly $N = N_b + N_s$. On the other hand, Erdős shows, by an intricate combinatorial argument, that for a suitable $N$ (in fact $2^{k+2}$), $N_b + N_s < N$, which gives the contradiction.

2.3 Proof as Exploration

The above proof is also an example of the third role of proof, that of exploration. Every mathematician knows that when he/she writes out a proof, new insights, ideas, and questions emerge. Moreover, the proof requires techniques which may then be applied to the consideration of new problems. What makes this topic interesting, and somewhat complex, is that there is not always a hard line between explanation and exploration. Often the hallmark of a good proof is that it proves more than the statement of the theorem, as the Erdős proof illustrates.

A fascinating example of proof as exploration is the story of the proof of the alternating sign matrix conjecture, a topic on the boundary of algebra and combinatorics. An alternating sign matrix (ASM) is a square matrix of 0s, 1s, and −1s such that the sum of the entries in each row and each column is 1 and the nonzero entries in each row and each column alternate in sign. These are generalizations of permutation matrices. The ASM conjecture (now the ASM theorem)
concerns the number $A_n$ of such $n \times n$ matrices, which is given by $A_n = \prod_{0 \leq j \leq n-1} \frac{(2j+1)}{(n+j)!}$. (In contrast, there are $n!$ permutation matrices.)

The history of the proof is brilliantly developed in David Bressoud’s book *Proofs and Confirmations* [Bressoud 1999]. (The title was inspired by Imre Lakatos’ book *Proofs and Refutations* [Lakatos 1976] which in turn was adapted from Karl Popper’s *Conjectures and Refutations* [Popper 1963].) Bressoud presents the proof as an exploration, and in fact the chapter containing the proof is entitled “Explorations.” He is referring to the development of the proof of the ASM conjecture, which he’s presenting the way it developed historically.

Woven into the narrative are classical antecedents of the ASM conjecture, including an algorithm for the evaluation of determinants due to Charles Dodgson (Lewis Carroll), the appearance of many participants (including Mills, Robbins, Rumsey, Stanley, Andrews, and Zeilberger) as well as other results and conjectures. In fact, the ASM conjecture is one of fourteen related conjectures, two of which are still unproved. (One of these was “checked by one of the largest army of reviewers any paper has seen: 88 referees and one computer.”)

Bressoud writes that the ASM proof “lay in unexpected territory and revealed a host of new insights and engaging problems.” The unexpected territory included plane partitions, symmetric functions, and hypergeometric series. Indeed, it turns out that physicists were interested in ASMs, but they called them six vertex models or square ice.

The strategy of the proof was to try to find a one-to-one correspondence between $n \times n$ ASMs and descending plane partitions with largest part less than or equal to $n$. (Plane partitions are partitions of integers arranged as a two dimensional array, with certain restrictions. Some of the other conjectures concern generating functions - namely power series whose coefficients count the number of certain plane partitions.)

### 2.4 Proof as Justification of Definitions

Still another reason for proof, closely connected to teaching, is the justification for mathematical definitions. (I am indebted to my colleague Paul Green for this observation.) For example, one proves that the sum and product of continuous functions is continuous to confirm that the $\varepsilon - \delta$ definition is successful in capturing the intuitive idea of continuity. Similarly, the proof of the intermediate value theorem justifies the definition of the real number system. Yet another example is the use of the fundamental theorem of calculus to show that there is a real valued function whose derivative is $e^{-x^2}$. What is involved here is the very definition of a function. It demonstrates that a function need not be given by a simple formula, which is something we want to drive home to students. Only a formal proof can guarantee its existence and allow it to be studied.

Proofs also develop and underscore connections between different branches of mathematics, frequently to the benefit of both areas. Well known instances of this phenomenon are combinations of algebra and topology, and of combinatorics and number theory. In “Four Examples,” we’ll discuss in detail Furstenberg’s proof on the Szemerédi theorem, which combines ergodic theory and combinatorial number theory.

### 2.5 The Dieudonné-Katznelson Encounter

It is frequently asserted that one can fill in the details of an informal argument to obtain a formally correct proof. To quote Bourbaki [1968, p. 8]: “In general [a mathematician] is content to bring the exposition to a point where his experience and mathematical flair tell him that translation
into a formal language would be no more than an exercise of patience (though doubtless a very tedious one)." As if in reply, Hersh [1997, p. 52] says "It may be true. It's a matter of faith."

In this connection, let me turn to a personal recollection. In 1971, the distinguished mathematicians Yitzhak Katznelson and Jean Dieudonné visited the University of Maryland for a semester. Katznelson gave a course in ergodic theory, to which Dieudonné was a faithful attendee (as was I). Katznelson's lectures were well organized, although somewhat informal. Dieudonné (who had been a member of Bourbaki) didn't give Katznelson a moment's peace. He kept saying "That is not a proof" or sometimes "That's a nice presentation of the idea—now let's see the proof" and made Katznelson go over the argument until it was accomplished to his (Dieudonné's) satisfaction.

I'm certainly not saying that Dieudonné was more "rigorous" than Katznelson. Katznelson's proofs definitely met the standards of mathematical discourse. There are many acceptable styles of proof. (One might imagine Dieudonné lecturing, with Alonzo Church in the audience, who would say that Dieudonné's arguments were not proofs.)

Dieudonné had a high regard for Katznelson and the course (as he told me) and probably thought that the latter's arguments were essentially correct. But Dieudonné was not playing games. I'm sure he was serious in asserting that Katznelson's arguments fell short of proof, and felt that it was worth the class time for the development of one which was acceptable to him.

2.6 The Jaffe-Quinn Article

An extremely interesting discussion of various issues concerning proof was initiated by an article in the Bulletin of the American Mathematical Society by Arthur Jaffe and Frank Quinn [1993], and the responses it generated [Responses 1994]. The article (henceforth referred to as JQ) is entitled "Theoretical mathematics: towards a cultural synthesis of mathematics and theoretical physics." JQ use the term "theoretical mathematics" for "speculative and intuitive work" (this terminology was much criticized by a number of the respondents) and "rigorous mathematics" for "proof oriented work." While they agree that mathematics is "nearly characterized by the use of rigorous proofs" (which they unequivocally endorse) they call attention to "a trend towards basing mathematics on intuitive reasoning without proof" and say that this "may be the beginning of fundamental changes in the way mathematics is organized."

JQ contrast mathematics with physics. In the latter there is a "division of labor" between experimenters and theoreticians. But "the mathematical community has not undergone a bifurcation into theoretical and rigorous branches."

There is at least an implication by JQ that such a "bifurcation" would be desirable. But the lack of it is not accidental, and I doubt that it can be created by fiat. Of course there always has been a speculative and intuitive component to mathematics (and JQ correctly point to this as one of mathematics' "success stories") but I don't think there can be a division of mathematicians into two kinds, as there is in physics. That is, in general a mathematician's work is both intuitive and rigorous. Certainly there are individuals—Mandelbrot (one of the respondents) and Feigenbaum come to mind—whose main activity is "theoretical," but it's doubtful that there will be an entire community of such.

A year later the Bulletin printed a number of responses to JQ (by pure and applied mathematicians, physicists, and a historian of mathematics), as well as a separate article by Bill Thurston. These were in turn followed by a response by JQ.
While some of the responders are in substantial agreement with IQ, there are attacks from both the “right” and the “left.” Mac Lane felt that physics is not a good model for mathematics. (The quote from Mac Lane in the section “The Roles of Proof,” above, is part of his response.) Moe Hirsch (presumably tongue in cheek) suggests that “published mathematics . . . like good wine, should carry a date. If after ten years no errors have been found the theorem will be generally accepted” and that one should “attach a label to each proof, e.g., computer aided, mass collaboration, formal, informal, constructive, fuzzy, etc.”

A particularly negative response was by Benoit Mandelbrot. He finds IQ “appalling” and refers to rigorous mathematicians as “Charles” mathematicians (since the AMS office in Providence is on Charles Street). He characterizes mathematical rigor as “besides the point and usually distracting, even where possible.”

Richard Palais, the editor of the Bulletin, wrote that (“with mixed feelings”) the Bulletin would no longer publish “controversial” articles. (Such would be restricted to the Notices of the American Mathematical Society.) One wonders about the subtext of this decision.

3 Computers and Proof

There is no question that computers are having a profound impact on mathematical practice. Perhaps their main role has been in experimentation, production of pictures, data, and the generation of conjectures. But computers have been used in some controversial proofs.

The relation between computers and proof is quite complex, and is still being sorted out. This paper will consider only a few such cases. It is interesting that Rota, in a passage following the quotation cited in the section “The Roles of Proof,” above, says that it is because of computers that proof is “more indispensable than ever” (since “conjectures in number theory may fail for integers . . . beyond the reach of . . . computers”). There are some mathematicians, notably Paul Halmos and Pierre Deligne, who completely reject the use of computers. For example, Deligne has written “I don’t believe in a proof done by a computer . . . I believe in a proof if I understand it.” [Szpiro 2003, p. 21] In the same spirit, Eugene Wigner is reported to have said [Robertson 2003, p. 80] “It’s nice to know that the computer understands the problem. But I would like to understand it, too.” On the other hand, Thomas Hales says “I now feel that computer proofs are vital to the progress of mathematics.” [Szpiro 2003, p. 212]

I take an intermediate point of view. Regardless of anyone’s feelings (even Deligne’s), one cannot wish the use of computers in proofs. Mathematicians will use them if they find them necessary, or even convenient, and it’s necessary to come to terms with this phenomenon. On the other hand, it’s somewhat disingenuous to say that there is no difference between a calculation done by a computer and one done “by hand.”

The issue is not whether one should “believe” a proof making use of a computer. Indeed, it may well be the case that a computer calculation is more reliable than a traditional one, especially if the latter is very long (witness the competing attempts at proving the Kepler conjecture, discussed below). Some of the same processes as in traditional proofs, for example modifications of the original argument, and repeated scrutiny, occur with computer proofs, and confirm the truth of the claimed assertion.

Moreover, there are certain proofs which just couldn’t be accomplished without a computer. One such is the much discussed proof of the four color theorem, by Appel and Haken. The problem was reduced to several thousand cases, which were then checked by the computer.
The point is that it is necessary to recognize that there are tradeoffs involved here, namely the achievement of results versus the understanding of the reasons for their proofs. Even a rote computation in a traditional proof involves a certain amount of thinking. In the case of replication of a computer argument we cannot determine easily what hidden assumptions or errors lie in the shared bits of coding or hardware. At some point in the proof, a result is true because the computer “said so.”

With regard to computers and proof, the story of the Kepler conjecture on sphere packing is particularly striking. (In my opinion, it is an order of magnitude more interesting than the four color theorem, although the latter was the first well known problem to make use of the computer for its solution).

The conjecture is that the densest way to pack spheres is the hexagonal close (or “green grocers”) packing. This is a four hundred year old problem, the oldest problem in discrete geometry, which was also part of Hilbert’s 18th problem. There was a disputed proof (by Hsiang), and then a very long, computer assisted proof (by Hales), which is apparently correct. And the latter has led to conjectures and proofs of new results. All of this is recounted in detail in the excellent book *Kepler’s Conjecture* by George C. Szpiro (2003).

A proposed proof, by Wu-Yi Hsiang [1993], was actually published. This proof made no use of the computer, just tools from (relatively) elementary geometry and calculus. The consensus of the mathematical community is that the attempted proof is incorrect, although Hsiang still stands by it. The proof that is now generally accepted is by Thomas Hales, with significant help from his student Samuel Ferguson. It consists of six papers, as well as a computer program. It was submitted to the *Annals of Mathematics* (in fact it was solicited by the *Annals*) and a team of 12 referees worked on it for four years. They returned a report saying that they were unable to completely certify the proof, although they were 99 percent certain of it.

In fact, the *Annals* has published Hales’ proof [Hales 2005], although not the computer code on which it was based. The original plan was to publish it with a disclaimer, but after Hales reorganized it, it appeared as a single (more than one hundred page) paper, without a disclaimer. On the first page, Hales writes, “Here we describe the top-level outline of the proof and give sources of details of the proof. The latter are to appear as several papers in *Discrete and Computational Geometry*.”

The Szpiro book has a chapter entitled “But is it really a proof?” There does seem to be a strong consensus that the Kepler conjecture is now proved—that it is “certified.” There is considerably less agreement as to whether it meets the criterion of “explanation.” For example, the mathematician and science writer Ian Stewart likens Hales’ proof to a telephone directory, in contrast to Wiles’ proof of Fermat’s last theorem, which he compares to “War and Peace.”

In this case, how are we to decide if the “telephone book” nature of Hales’ proof is inherent to the problem?

This type of thing is unprecedented in mathematics. Regardless of one’s feelings about the use of computers in proof, it must be recognized that Hales’ work is a major scientific achievement. The story is not over; although the proof has appeared in print, there will very likely be simplifications that will really embed the result into mathematics.

The proofs of the four color theorem and the Kepler conjecture definitely fall within the traditional framework of proof as a sequence of deductions, although the computer plays an essential role. But there is another trend which in fact challenges the accepted dichotomy between a proof and an argument which falls short of proof. This is not concerned with the computer as an aid to proof, but rather envisions computer calculations as replacing proof.
3. On the Roles of Proof in Mathematics

One of the most provocative challenges to traditional proof was put forth by Doron Zeilberger in an article “Theorems for a price: tomorrow’s semi-rigorous mathematical culture.” [Zeilberger 1993] (As we’ll see, “for a price” is meant literally.) The tone is set by Zeilberger’s much quoted (and by now notorious) statement that in the future “rigorous old style mathematicians . . . may be viewed by mainstream mathematicians as a fringe sect of harmless eccentrics.” He continues: “The computer has already started doing to mathematics what the telescope and microscope did to astronomy and biology . . . In the future mathematicians will not care about absolute certainty, since there will be so many exciting new facts to discover.” After presenting a number of identities which were proved by, or with the aid of, a computer, he envisions an abstract of a paper (c. 2100); “We show in a certain precise sense that the Goldbach conjecture is true with a probability larger than 0.9999 and that its complete truth could be determined with a budget of $10 billion.” (Perhaps intentionally, there is no explanation of this assertion by the 2100-era mathematician.)

I should mention that Zeilberger is an outstanding mathematician, and in fact was one of the participants in the solution of the alternating sign matrix conjecture. But on this question I think he is quite wrongheaded.

Zeilberger’s article was reprinted in the Mathematical Intelligencer, where it is followed by a response from his friend and collaborator George Andrews [1994]. Andrews’ article is entitled (in part) “You’ve got to be kidding.” He challenges Zeilberger’s evaluation of the role of the computer in the discovery and proof of the various identities, and says moreover that Zeilberger “ignores the insight provided by proof” and “has produced exactly no evidence that his Brave New World is on the way.”

As for Zeilberger’s assertion that important theorems can be proved “for a price”—I don’t believe it. Mathematics just doesn’t work that way. Although mathematicians are no more immune to the lure of money than anyone else, one can’t imagine a “crash program” to prove the Riemann hypothesis or the twin prime conjecture. It’s true that there is now a well publicized monetary prize for such proofs, but there is no reason to think that the proofs will be attained any earlier on that account.

Another proponent of this trend is the geologist Douglas Robertson [2003]. Robertson’s point of view is similar to Zeilberger’s (he might be termed “Zeilberger lite”). Interestingly, he is extremely frank and explicit about what may be lost by this process. “Just as astronomers had to accept the idea that the telescope vastly extends the reach of the naked eye, mathematicians will have to accept the idea that the computer similarly extends the reach of the human mind.” [Robertson 2003, p. 81] He also says that the understanding of the reasons behind such a computer proof “may not be attainable.” Robertson asserts that computers will throw light on whether π is a normal number.1 (This is very doubtful, in my opinion. No amount of computer calculation can settle this question.)

4 Four Examples
The examples which I’ll discuss at some length are from topological dynamics and ergodic theory, areas of which I have some knowledge.

---

1 A number is said to be normal (say to base 10) for which every finite sequence in the decimal expansion occurs with the “right” limiting frequency. For example, the occurrence of 57 has limiting frequency .01. Normal numbers have full Lebesgue measure, but are of first category.