Chapter 23: Proof and Proving

GILA HANNA AND H. NIELS JAHNKE
The Ontario Institute for Studies in Education of the University of Toronto, Canada and Institut für Didaktik der Mathematik der Universität Bielefeld, Germany

ABSTRACT

Proof is an essential characteristic of mathematics and as such should be a key component in mathematics education. Translating this statement into classroom practice is not a simple matter, however, because there have been and remain differing and constantly developing views on the nature and role of proof and on the norms to which it should adhere.

Different views of proof were vigorously asserted in the reassessment of the foundations of mathematics and the nature of mathematical truth which took place in the nineteenth century and at the beginning of the twentieth, a reassessment which gave rise to well-known and widely divergent philosophical stands such as logicism, formalism and intuitionism. These differences have now been joined by disagreements over the implications for proof of 'experimental mathematics', 'semi-rigorous mathematics' and 'almost certain proofs', concepts and practices which have emerged on the heels of the enormous growth of mathematics in the last fifty years and the ever-increasing use of computers in mathematical research. If these and earlier controversies are to be reflected usefully in the classroom, mathematics educators will have to acknowledge and become familiar with the complex setting in which mathematical proof is embedded. This chapter aims at providing an introduction to this setting and its implications for teaching.

It is not merely as a reflection of mathematical practice that proof plays a role in mathematics education, however. Proof in its full range of manifestations is also an essential tool for promoting mathematical understanding in the classroom, however artificial and unnatural its use there may seem to the beginner. To promote understanding, however, some types of proof and some ways of using proof are better than others. Thus this chapter also aims at providing an introduction to didactical issues that arise in the use of proof.

The chapter first discusses the great importance accorded in mathematical practice to the communication of understanding, pointing out the place of proof in this endeavour and the implications for mathematics teaching. It then identifies and assesses some recent challenges to the status of proof in mathematics from mathematicians and others, including predictions of the 'death of proof'. It also examines and largely seeks to refute a number of challenges to the importance of proof in the curriculum that have arisen within the field

A.J. Bishop et al. (eds.), International Handbook of Mathematics Education, 877 - 908

of mathematics education itself, sometimes prompted by external social and philosophical influences.

This chapter continues by looking at mathematical proof, and the mathematical theories of which it is a part, in terms of their role in the empirical sciences. There are important insights into the use of proof in the classroom that may be garnered through a deeper understanding of the mechanism by which mathematicians, nominally practitioners of a non-empirical science, make an indispensable contribution to the understanding of external reality.

Later sections examine the use of proof in the classroom from various points of view, proceeding from the premise that one of the key tasks of mathematics educators at all levels is to enhance the role of proof in teaching. The chapter first reports upon some ambivalent but nevertheless encouraging signs of a strengthened role for proof in the curriculum, and turns to a discussion of proof in teaching, offering a model defining its full range of potential functions. The important distinction between proofs which prove and proofs which explain is then introduced, and its application is presented at some length with the help of examples.

1. PROOF AND UNDERSTANDING

The most significant potential contribution of proof in mathematics education is the communication of mathematical understanding. One comes to appreciate the importance of this seemingly trite determination if one examines critically the view of proof adopted by the 'new math' movement of the 1950's and 1960's.

The belief implicit in the 'new math' was that the secondary-school mathematics curriculum better reflects mathematics when it stresses formal logic and rigorous proof. This belief rested upon two key assumptions:

a) that in modern mathematical theory there are generally accepted criteria for the validity of a mathematical proof; and
b) that rigorous proof is the hallmark of modern mathematical practice.

Both of these beliefs can be seen to be false (Hanna, 1983). First of all, even a cursory revisiting of the major accounts of the nature of mathematics (logicism, formalism, intuitionism and quasi-empiricism) makes it obvious that these significant schools of mathematical thought hold widely differing views on the role of proof in mathematics and on the criteria for the validity of a mathematical proof.

Second, an examination of mathematical practice shows clearly that in the eyes of practising mathematicians rigour is secondary in importance to understanding and significance, and that a proof actually becomes legitimate and convincing to a mathematician only when it leads to real mathematical understanding. According to Hanna (1983), mathematicians accept a new theorem only when some combination of the following holds:

1) They understand the theorem (that is, the concepts embodied in it, its logical antecedents, and its implications) and there is nothing to suggest it is not true;
2) The theorem is significant enough to have implications in one or more branches of mathematics, and thus to warrant detailed study and analysis;
3) The theorem is consistent with the body of accepted results;
4) The author has an unimpeachable reputation as an expert in the subject of the theorem;
5) There is a convincing mathematical argument for it, rigorous or otherwise, of a type they have encountered before (p.70).

Subsequent studies of a number of cases have confirmed the appropriateness of these criteria (Neubrand, 1989; Berggren, 1990). In light of both the theory and the practice of mathematics, then, teachers can be assured that they would be imparting to students a greater understanding of proof itself, not to mention the mathematical topic under consideration, if they were to concentrate upon the communication of meaning rather than upon formal derivation. A mathematics curriculum which aims to reflect the real role of rigorous proof in mathematics must present it as an indispensable tool of mathematics rather than as the very core of that science.

Several mathematicians have expressed similar points of view quite explicitly (Manin, 1977; Kline, 1980; Davis and Hersh, 1981, 1986). Particularly interesting in this regard is a more recent paper by William Thurston (1994). Along with 15 other mathematicians, Thurston was responding to an article by Jaffe and Quinn (1993), who had cautioned against weakening the standards of proof. Jaffe and Quinn had proposed that heuristic work in mathematics be labelled 'speculation' or 'theoretical mathematics', to distinguish it from what they regard as proper mathematics, in which theorems are proven rigorously.

Thurston maintained that in attempting to answer the question 'What is it that mathematicians can accomplish?', one should not begin with the question 'How do mathematicians prove theorems?'. He pointed out that the latter question carries with it two hidden assumptions:

a) that there is a uniform, objective and firmly established theory and practice of mathematical proof; and
b) that the progress made by mathematicians consists of proving theorems (p.161).

According to Thurston (1994), neither of these assumptions will stand up to careful scrutiny. One will note that these hidden assumptions are in effect the same as the assumptions of the 'new math' discussed above.

Thurston (1994) also dismissed as a caricature the popular view of mathematical progress usually referred to as the definition-theorem-proof (DTP) model. For Thurston the right question to ask was: 'How do mathematicians advance human understanding of mathematics?'. And he added: 'We [mathematicians] are not trying to meet some abstract production quota of definitions, theorems and proofs. The measure of our success is whether what we do enables people to understand and think more clearly and effectively about mathematics' (p.163).

It is perhaps necessary to point out that stressing the importance of understanding is not in any way a criticism of formal proof as such. Thurston himself made this clear:

> I am not advocating the weakening of our community standard of proof; I am trying to describe how the process works. Careful proofs that will stand up to scrutiny are very important. ... Second, I am not criticizing the mathematical study of formal proofs, nor am I criticizing people who put energy into making arguments more explicit and more formal. These are both useful activities that shed new insights on mathematics (p.169).

Not all agree with Thurston on this point, however. A number of recent developments in the practice of mathematics, all of them reflecting in some way the growing use of computers, have caused some mathematicians and others to call into question the continuing importance of proof.

1.1 Challenges to Proof from Mathematics

The computer has acted as a leavening agent in mathematics, reviving an interest in algorithmic and discrete methods, leading to increased reliance on constructive proofs, and making possible new ways of justification, such as those that make use of computer graphics (Davis, 1993). The striking novelty of its uses, on the other hand, has lent a tone of urgency to the discussions among mathematicians about its implications for the nature of proof (Tymoczko, 1986; Jaffe and Quinn 1993; Thurston, 1994).

Indeed, the use of the computer has led some to announce the imminent death of proof itself (Horgan, 1993). On the basis of interviews with several mathematicians, Horgan made this prediction in a thought-provoking article entitled 'The death of proof' that appeared in the October 1993 issue of *Scientific American.* He claimed that mathematicians can now establish the validity of propositions by running experiments on computers, and maintained that it is increasingly acceptable for them to do mathematics without concerning themselves with proof at all.

One of the developments that prompted Horgan's announcement is the use of computers to create or validate enormously long proofs, such as the recently published proofs of the four-colour theorem (Appel and Haken) or of the solution to the party problem (Radziszowski and McKay). These proofs required computations so long they could not possibly be performed or even verified by a human being. Because computers and computer programs are fallible, then, mathematicians will have to accept that assertions proved in this way can never be more than provisionally true.

A second and particularly fascinating development is the recently-introduced concept of zero-knowledge proof (Blum, 1986), originally defined by Goldwasser, Micali and Rackoff (1985). This is an interactive protocol involving two parties, a prover and a verifier. It enables the prover to provide to the verifier convincing evidence that a proof exists without disclosing any information about the proof itself. As a result of such an interaction, the verifier is convinced that the theorem in question is true and that the prover knows a proof, but the verifier has zero knowledge of the proof itself and is therefore not in a position to convince others. (In principle, a zero-knowledge proof may be carried out with or without a computer.)

Here is an illustration of this concept taken from Koblitz (1994). Assume a map is colourable with three colours and the prover has a proof, that is, a way of colouring the map so that no two countries with a common boundary have the same colour. The prover wants to convince another person that there is a proof (a way of colouring the map) without actually revealing it, by letting the other person verify the claim in another way.

The prover first translates the problem into a graph consisting of vertices (countries) and edges (common boundaries). This means that the prover has a function f: $V \rightarrow \{R, B, G\}$ that assigns the colours R (red), B (blue), and G (green) to vertices (countries) in such a way that no vertices joined by an edge have the same colour. The prover also has two devices: Device A, which sets each vertex to flash a colour (R, B, or G), and Device B, which chooses a random permutation of the colours and resets each vertex accordingly. (A permutation might cause all green vertices to switch to blue and all blue vertices to red, for example).

The interaction between prover and verifier then proceeds as follows. To convince the verifier that there is a proof, the prover keeps the colours hidden from the verifier's view, but allows the verifier to grab one edge at a time and see the colours displayed at the two ends (the vertices) by Device A. The verifier starts by grabbing any edge, looking at the colours at the ends and noting that they are different. The prover then uses Device B to permute the colours randomly; the permutation is unknown to the verifier. After the permutation, the verifier again grabs any edge and verifies that the colours at the ends are different. The prover again permutes the colours. The two repeat these steps until the verifier is satisfied that the prover knows how to colour the map (has a proof).

This interaction does not tell the verifier how to colour the graph, nor does it reveal any other information about the proof. The verifier is convinced that