Proofs and Guarantees

JAMES ROBERT BROWN

The Viewpoint *column offers readers of* The Mathematical Intelligencer *the opportunity to write about any issue of interest to the international mathematical community. Disagreement and controversy are welcome. The views and opinions expressed here, however, are exclusively those of the author, The publisher and editor-in-chief do not endorse them or accept responsibility for them. Articles for* Viewpoint *should be submitted to the Editor-in-Chief, Marjorie Senechal.*

Let us assume what most mathematical readers would take for granted anyway: There are mathematical objects such as numbers and functions and there are objective facts about these objects, such as $3 < 5$ and the set of primes is infinite. Truth on this view is banal. "$3 < 5$" is true because the objects 3 and 5 are in the *less than* relation to one another, just as "Bob is shorter than Alice" is true, because Bob and Alice stand in the *shorter than* relation.

Why bother assuming this? There are plausible alternatives. We say: "Bishops move diagonally" is true and we say: "Sherlock Holmes lives at 221B Baker Street" is true. What makes them true, however, is a conventionally adopted rule in one case and a literary fiction in the other. Truth in mathematics, on the account I'm taking for granted, is no different than truth as normally understood in, say, physics. A proposition is true when it correctly tells us how things objectively are. I hope most readers are still with me, in spite of the mundane mathematical metaphysics so far. The interesting point comes next.

Why do we believe that $3 < 5$ and that there are infinitely many primes? Most would say that's an easy question with an obvious answer: *proof*. Here is a tougher question: Is proof the only sort of legitimate evidence in mathematics? Many will say—indeed, they will shout—yes, proof and proof alone is the source of mathematical evidence. Proofs are both necessary and sufficient. We know a theorem is true, they might add, when we have a proof, or we don't know it's true when we lack a proof—it's all or nothing.

A moment's reflection shows this is hopelessly wrong. Proofs have to start somewhere. There are axioms, postulates, or first principles that cannot themselves be proved without begging the question. So, in the case of arithmetic, where does the starting point, say, the Peano axioms (PA), come from? Nowhere. Usually they are just stated and theorem proving follows on from there. We can indeed derive PA, however, if we start from standard set theory. But this only pushes our problem back—where do the axioms of set theory come from? Rather than chase an infinite regress, let's stay focussed on PA. There are three rival answers to our question: Where do the PA axioms come from?

1. *The axioms of PA are self-evident.* Platonists look fondly on this assumption.
2. *The axioms of PA are conjectures that have the right consequences.* They imply things we believe independently and they systematize a large body of results. This parallels common attitudes to the natural sciences. We believe the principles of quantum mechanics because they organize experience and make a wide variety of testable predictions that have turned out to be true.

DOI 10.1007/s00283-017-9730-1

3. *The axioms of PA are arbitrary, like the rules of chess.* We have learned through experience which rules are the most fun to play with. None are objectively true.

Because the third proposed answer ignores the idea of truth, we shall ignore it. The first and second replies to the question each have a lot going for them. But there are concerns. Against the idea of self-evidence, empiricist philosophers claim we can see with the normal eye, but not with "the mind's eye," not even metaphorically. Mathematical knowledge, they insist, cannot be acquired by intuition or any other nonempirical method, so they chuck "self-evidence" out the window. By contrast, Platonists cheerfully bite the bullet and assert that we have the cognitive capacity to grasp facts about (some) abstract entities. Self-evidence stems from this intuition.

Where does PA come from? The second answer to this question requires that some consequences of the PA axioms be obvious, which brings us back to the first answer, that some of those consequences we would have to know by intuition. The first and second answers could both be right, as Gödel believed (Gödel 1947/1964). It does not really matter, however, which of these rival views is correct; the upshot is that *not everything can be proved*. There must be an unproven starting point. By the way, we need not be certain of our starting points. We are merely talking about reasonable belief, as we would in other fields, say, physics. We cannot hope for certainty anywhere else in life, so why require it in mathematics?

At this point, we could admit to massive ignorance and retreat to a weaker claim: We do not know that any theorem T is true simpliciter, but we do know that PA $\rightarrow$ T, and the evidence for this is indeed a proof. I suppose this would save the view that all mathematical evidence is simply proof, but it does so at the cost of near absurdity. Is anyone really agnostic about $2 + 3 = 5$, and willing only to give assent to PA $\rightarrow 2 + 3 = 5$?

Now what about proof itself? Even if we never made a mistake in any proof, we could still be seriously wrong. How so? Never mind calculation errors, which are hardly worth mentioning, since they are utterly uninteresting mistakes. Perhaps we're mistaken because we have changed an important concept. After *number*, the second most important concept in mathematics is probably *function*. Consider its history. Two centuries ago there were common conceptions of *function* that led to the theorem that all functions are continuous. There was nothing wrong with the proof of this theorem. Today, of course, we would reject the theorem, because we now consider *function* to be an arbitrary association between two sets. This allows such entities as the radically discontinuous Dirichlet function, $f(x)$, which equals 0 or 1, depending on whether x is rational or irrational. No proof, no matter how logically impeccable, can save a theorem from conceptual change. The most rigorously constructed edifice will collapse when a definition is tweaked, and definitions are tweaked because people have a better idea. Needless to say, we'll never be in a position to say with certainty that at last we have the right definition of a concept. The mathematical future, although remarkably stable, will always be precarious.

Mathematical rationality is based on much more than proof, whatever we think proof is. Mathematicians wonder about which problems to work on, or to give their students, and what techniques are most likely to succeed. They sit on grant-giving committees that evaluate the plausibility of various proposals, and they fund those they think sufficiently promising. As a body of *accomplishments*, mathematics might rest exclusively on proof (as already argued, this is highly questionable), but as an *activity*, mathematics depends heavily on hunch, plausibility, and conjecture. Most mathematicians believe that the Riemann hypothesis is true and that P = NP is false. They have good reasons for their beliefs, but they do not have proofs. It's important that they have good reasons, because this is what guides so much research and determines where resources go. The alternative is to make choices on a whim.

We now have three distinct reasons for thinking that proof (as normally understood) is only a part of the story in the growth of mathematics. First, proofs need a starting point that is itself unproven. Second, we might be proving things about the wrong concept. Third, some evidence for an alleged theorem guides research that might result in a proof, but the evidence itself is not a proof of that theorem. What are we to make of this?

Timothy Gowers has written interestingly and extensively on the philosophy of mathematics in various places. His views on evidence have been summed up in a slogan suitable for a bumper sticker: Proof = explanation + guarantee.[1]

Gowers himself and those who have discussed his work have focussed on "explanation," which is a hugely interesting and important notion in mathematics and philosophy. A proof provides evidence that a theorem is true, but some proofs also produce insight into what is going on. Gowers is trying to understand this phenomenon when he discusses explanation. I, however, will take a different tack: I will focus on "guarantee," which Gowers and others take to be the evidence that shows the theorem is certainly true. A proper proof that there are infinitely many primes is a guarantee that this is true. As proof is normally envisaged, we couldn't ask for better than this sort of guarantee. This is the gold standard. The natural sciences don't have a hope of matching it.

There is, however, another sense of "guarantee" that is in common use. A new toaster comes with a guarantee. This is not a promise that it will work perfectly. Rather, it is simply the promise that it will work *or* it will be fixed *or* replaced *or* our money will be refunded. This alternative sense of guarantee might turn out to be useful in understanding mathematical activity. With this in mind, let me jump to the main claim: proof = explanation + guarantee (in the toaster sense).

To make this plausible, we need one important assumption: mathematics is self-correcting. We do not assume the natural sciences are infallible, but we do

[1]Mazur 2012, 194. Mazur attributes this to Apostolos Doxiadis (in conversation), who took it to reflect Gowers's attempt to balance subjective explanation with objective proof or guarantee. I should add that when attempting to modify Gowers's account, I am still upholding a completely objective notion of guarantee. The slogan was expressed by Alan Robinson (2000) before Gowers's work appeared.

assume that as we go wrong, we shall eventually discover and correct our past mistakes and, in doing so, we continue to make progress. In short, progress is not monotonic. I don't want to disguise the significance of this assumption. From time to time, chess changes its rules, but in no sense is it making progress toward the truth, although it might be making progress in the sense of being more fun, more challenging, etc. I am assuming that the current concept of set is better than the one that led to the paradoxes, and that the current concept of function is better than earlier versions, not just a change in taste or fashion.

After we see proof this way, we can begin to look more kindly on other forms of evidence inside mathematics. Here is my alternative: A proof (evidence) is a guarantee in the toaster sense, not Gowers's. A proof is a good bet, but it does not give us certainty. If it fails, we can (eventually) fix it, or replace it, or withdraw it. The last of these is equivalent to refunding your money and acknowledging that the product is hopelessly faulty.

Proofs (evidence, guarantees) can come from a number of sources.

- Derivations, of course, which are endorsed by everyone
- Diagrams, pictures, thought experiments
- Computer proofs
- Statistical analyses
- Physical analogies

Proofs can lose their "guaranteed" status, or at least have that guarantee weakened. This can happen in a variety of circumstances.

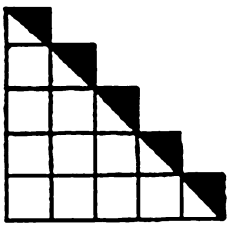
- Discovery of a counterexample. The theorem would be withdrawn (you get your money back).
- Discovery of coherent alternatives (e.g., non-Euclidean geometry) undermines the status of previously accepted self-evident axioms.
- Conceptual change (Change the definition of *function* and you undermine the theorem that all functions are continuous.)
- New discoveries in physics that undermine a previously accepted analogy.
- Bugs discovered in software used in a computer proof.

Some examples will illustrate and perhaps help to make the case.

Here is a picture proof of a well-known result.

Theorem: $1 + 2 + 3 + \ldots + n = n^2/2 + n/2$.

The proof is the following diagram:



I leave it to readers to figure out how it works. Note that even though the diagram is a special case $n = 5$, after we grasp the proof we see that it holds for all n. I find this picture proof just as persuasive as a proof by mathematical induction. (For more on this example and others like it, see Brown 1999/2008).

I won't bother with a computer proof. They are well known, starting with the proof of the four-colour theorem. Even those who dislike the whole idea of computer proofs will acknowledge the valuable data generated by computers. For instance, we now know that Goldbach's conjecture holds up to 4×10^{18}.

The twin primes conjecture says: *There are infinitely many numbers p such that p and p + 2 are both primes.* There is no standard proof of this, but there is a simple and quite convincing argument for its truth. Primes seem to be distributed randomly, and there are infinitely many of them. So we should expect them to pop up over and over again, spaced arbitrary distances apart, including being spaced two numbers apart. Thus, there are infinitely many twin primes. Of course, this proof is only a guarantee in the toaster sense.

Physical analogies come in many varieties. The Pigeon Hole Principle says, *If n + 1 pigeons are distributed in n pigeon holes, then one hole has at least two pigeons.* It can be derived from set theory, but none would say that their confidence had gone up having seen such a proof. The physical analogy is wholly convincing. There are more sophisticated examples, such as mirror symmetry. Physicists found physically equivalent string theories that could be modelled by Calabi-Yau manifolds that mirrored one another. Mathematicians were initially sceptical, but have been won over to the existence of this mirror symmetry.

These issues are not new. When the four-colour theorem was proved in the 1970s, there was plenty of heated discussion among mathematicians, philosophers, and computer scientists. A few years ago there was another heated discussion among mathematicians and theoretical physicists about legitimate methods. (See Jaffe and Quinn 1993, Atiyah, et al. 1994, and Thurston 1994.) These exchanges took parts of mathematics for granted and then debated how to go on from there. Are computer proofs or physical analogies legitimate forms of mathematical evidence? These are interesting questions that are far from being settled. What they overlook or even take for granted is the starting point itself, the unproven axioms and first principles that are the points of departure for a standard proof (i.e., a derivation). As soon as we realize that first principles or axioms cannot be guaranteed in the sense of complete certainty, then we must acknowledge that they can only be guaranteed in the toaster sense. And when we realize this, we must further acknowledge that there can be no rationale for wanting Gowers-type guarantees, infallible proof techniques, to apply to fallible axioms. In short, it's toasters all the way.

I want to close with a confession. I feel somewhat uneasy about where I have arrived. I planned less, but after we acknowledge the fallibility of the initial axioms or other first principles and we also acknowledge that central definitions can have an evolving history, then it's hard to put on the brakes. All the rest follows on naturally, which, I admit, can be disconcerting. But it can also be liberating.

ACKNOWLEDGEMENTS

Thanks to Mark Colyvan, Mary Leng, and Jan Zwicky for useful comments on an earlier draft and for the occasional cheeky slur (especially from Mary), which sometimes turned out to be usefully thought provoking.

Department of Philosophy
University of Toronto
Toronto
Canada
e-mail: jrbrown@chass.utoronto.ca

REFERENCES

Atiyah, M., et al. (1994) ''Responses to 'Theoretical Mathematics: Towards a Cultural Synthesis of Mathematics and Theoretical Physics' by A. Jaffe and F. Quinn,'' *Bulletin of the American Mathematical Society*, Vol. 30, No. 2, 178–211.

Brown, J.R. (1999/2008) *Philosophy of Mathematics: A Contemporary Introduction to the World of Proofs and Pictures*, London and New York: Routledge.

Gödel, K. (1947/1964) ''What is Cantor's Continuum Problem?,'' reprinted with additional remarks in P. Benacerraf and H. Putnam (eds.), *Philosophy of Mathematics*, Cambridge: Cambridge University Press (1964).

Gowers, T. (2000a) ''Rough Structure and Classification,'' *Visions in Mathematics*, GAFA 2000 Special Volume Part 1, Alon et al. (eds.), 79–117.

Gowers, T. (2000b) ''The Two Cultures of Mathematics,'' in Arnold et al. (eds.), *Mathematics: Frontiers and Perspectives*, American Mathematical Society, 67–78.

Jaffe, A. and F. Quinn (1993) '''Theoretical Mathematics': Toward a Cultural Synthesis of Mathematics and Theoretical Physics,'' *Bulletin of the American Mathematical Society*, Vol. 29, No. 1, 1–13

Mazur, B. (2012) ''Visions, Dreams, and Mathematics,'' A. Doxiadis and B. Mazur (eds.), *Circles Disturbed: The Interplay of Mathematics and Narrative*, Princeton: Princeton University Press.

Robinson, J.A. (2000) ''Proof = Guarantee + Explanation,'' *Intellectics and Computational Logic* (*to Wolfgang Bibel on the Occasion of his 60th Birthday*), Dordrecht: Kluwer, 277–294.

Thurston, W. (1994) ''On Proof and Progress in Mathematics,'' *Bulletin of the American Mathematical Society*, Vol. 30, No. 2, 161–177.