Michael Atiyah: The Role of Proof

5

Michael Atiyah, actually Sir Michael Atiyah, is one of the great mathematicians in the world. He has received awards from the Fields Medal to the Abel Prize, for his seminal work in many aspects of algebraic geometry, topology, and operator theory. Besides his deep and beautiful results he has some striking insights into the nature of proof. For example, one of his quotes is:

> I think it is said that Gauss had ten different proofs for the law of quadratic reciprocity. Any good theorem should have several proofs, the more the better. For two reasons: usually, different proofs have different strengths and weaknesses, and they generalise in different directions—they are not just repetitions of each other.

We will talk about the $\mathsf{P} = \mathsf{NP}$ question, and not even mention the major and minor claims to prove them different—or equal—that arose during 2010.

At the time of the major proof claim by Vinay Deolalikar, Ken and I both spoke to various reporters. Some were from the online media and some from the print media. Both types of reporters asked good questions, and in general we had an interesting discussion. But one or two asked a question that I really had trouble answering. The question was not an obvious one like: what is polynomial time, or what is NP? The question was:

> *Why is proving* $\mathsf{P} \neq \mathsf{NP}$ *an important result?*

The trouble I had is simple: if most believe that $\mathsf{P} \neq \mathsf{NP}$ is true—perhaps obviously true—then why care if it gets proved? Yes, it is a famous problem, with a large monetary prize. No doubt whoever first proves the result will be showered with many awards and honors. But, still why the huge interest in proving something that we know is correct?

I have thought about this quite a bit, and have some insights that I would like to share with you about their question. I wonder if you have other thoughts.

R.J. Lipton, K.W. Regan, *People, Problems, and Proofs*,
DOI 10.1007/978-3-642-41422-0_5, © Springer-Verlag Berlin Heidelberg 2013

5.1 Does Any Proof Matter?

So why do we really care if there is suddenly a proof that $\mathsf{P} \neq \mathsf{NP}$? As many of you know, I am less sure than most that $\mathsf{P} \neq \mathsf{NP}$. So perhaps the answer *for me* is it would be important because I have great doubts about it. But, I have already discussed a number of times and in different ways why I am skeptical about the conventional wisdom.

I can think of several different reasons why a proof of $\mathsf{P} \neq \mathsf{NP}$ would potentially really matter. The first has to do with the nature of proofs in mathematics. Let me explain.

I had the honor of meeting Atiyah a few years ago, and we had a chance to talk about the nature of proofs. One story he told me in private was quite telling. He told me that he had, many years earlier, proved a technical theorem about finite groups. He felt very sure the proof was correct, but sometimes late at night he would lie awake with some doubts. The proof was not a high-level proof; instead it relied on a detailed analysis of the group structure. Since the proof was so technical and filled with case analysis he never felt that he really knew why the theorem was true.

Years later he found *the proof*. He realized that his theorem was true for a much larger class of groups than finite: it was true for compact algebraic groups. Further, the proof there was high-level, was clear to an expert, and relied on no magic calculation, nor any case analysis. He said now he *knew* the original theorem was correct, and he could sleep better at night.

He further said that the role of proof, in his opinion, is not to "check-off" that a statement is correct. The role is to give insight into *why* the statement is correct. As you might imagine he was not very interested in machine proofs—at the time we discussed Thomas Hales' proof of the Johannes Kepler Conjecture. While he understood the potential need for such computer proofs, he really wanted to know why it was true.

5.2 Does a Proof of $\mathsf{P} \neq \mathsf{NP}$ Matter?

Yes it does. Here are my three foremost reasons to think that such a proof could be very important.

- **A Proof Would Tell Why:** Even those who are sure that $\mathsf{P} \neq \mathsf{NP}$ would like to know why this is so. This is exactly Atiyah's point. A proof would give us insight into why there can be no efficient search for SAT.
- **A Proof Could Give Us New Methods:** Perhaps the best reason is the hope that a proof that $\mathsf{P} \neq \mathsf{NP}$ would have to use new tools in the proof. These tools would hopefully shed light on computation in general. They could yield insights into the fundamental nature of computation. This is the best reason, in my opinion, for wanting a proof.

There are many examples in mathematics where this is exactly what has happened. The proof of a great result has many times created new tools and techniques that have raised the curtain and allowed us to see for the first time new insights into other problems. Certainly it would be wonderful if this were the case with a proof of $\mathsf{P} \neq \mathsf{NP}$.

For example, Andrew Wiles' proof of Fermat's Last Theorem and Grigori Perelman's proof of the Poincaré Conjecture have changed their respective fields. Wiles' proof of Fermat has led to other fundamental advances in number theory, well beyond solving the one famous family of Diophantine equations.

However, not all mathematical proofs of great conjectures use new techniques. There have been many solutions of longstanding open problems that used *no* new techniques. These were often very clever results, but the provers did not need new methods and tools. They were able to resolve the conjecture using well-known methods—their proofs may have been very clever, but they did not change the landscape.

I have no idea how often the latter happens, but it does happen. Some friends who are experts on the Riemann Hypothesis once told me their greatest fear is: what if someone came along with a clever proof, but one that "just" used known technology in a clever way? They would then know that the Riemann Hypothesis is true, yet they would be quite disappointed.

Hopefully, this will not happen with $\mathsf{P} \neq \mathsf{NP}$. Hopefully.

- **A Proof Helps With Goals of Security:** In many cases this means *only* that the authors of a paper have proved that breaking their system implies that some hardness assumption, such as on factoring, is wrong. Even a proof that $\mathsf{P} \neq \mathsf{NP}$ would not rule out that such assumptions are false: recall that factoring is not known to be NP-complete. I think, however, that a proof of at least $\mathsf{P} \neq \mathsf{NP}$ would be of some comfort to cryptographers. Their special hardness assumptions might still be unproved, but a proof would move us closer to perhaps one day really having provable security.

5.3 Open Problems

Are these good reasons? What are your reasons?

5.4 Notes and Links

Original post:
http://rjlipton.wordpress.com/2010/08/18/proofs-proofs-who-needs-proofs/
Kepler Conjecture:
http://en.wikipedia.org/wiki/Kepler_conjecture
See Chap. 1 for more on Vinay Deolalikar's claimed proof. The first post on our blog about it was:
http://rjlipton.wordpress.com/2010/08/08/a-proof-that-p-is-not-equal-to-np/