A Note on Mathematical Proof

Stephen Taylor

September 6, 2006

Abstract

The purpose of this note is to define the term "mathematical proof" and to outline the logical structure of mathematical writing.

Consider a court of law, in which a man has been charged with a crime. The prosecution establishes the defendant was at the crime scene during the time the crime was committed and has three eye witnesses testify that he indeed committed the crime. Moreover, the defendant's fingerprints were found on the weapon used in the crime. Has the prosecution proven that the defendant committed the crime? The answer is no. They may have "proven beyond any reasonable doubt" that they have identified the culprit; however, the following counter-example is possible:

The three witnesses are conspiring with the prosecution, have tampered with the evidence, and given false testimony for their own interests.

Such a situation is improbable but not impossible. Thus from the standpoint of a court, the prosecution may have "proven" the defendant committed the crime in question, but mathematically we have found a counterexample to the argument. Therefore the conclusion fails to be mathematically proven. To further understand the idea of mathematical proof, we need to understand the following concepts:

Axioms are the heart of mathematics and any type of logical argument. An axiom is a statement that is accepted as true without need for justification. For example, the axioms of the real numbers found on pages three and four of the text are the starting point for the development of calculus.

Definitions are a type of axiom. Uniform definitions are necessary in mathematics so everyone understands an idea in the same way. For instance, suppose I ask a group of twenty people to define the word "happiness." More than likely, I would get twenty similar but different definitions. Now suppose I defined the "set of integers" to be

$$\mathbb{Z} = \{0, \pm 1, \pm 2, \pm 3, \ldots\}$$

and asked twenty math students to define the set of integers for me. Assuming all accepted my definition as an adequate representation for what they believed the integers are, I would get twenty identical responses. Note I could have just as well defined the set of integers to be

$$\mathbb{Z} = \{2.3, \pi^e, 6i, \Gamma(3.2), \zeta(3 + 2.1i)\}.$$

I would hope everyone would disagree with this definition. Then as a group we would have to agree on a precise definition of "the set of integers". If we could not, it would be impossible to build a logical structure and hence a mathematics around this idea.

After axioms and definitions are established we are ready to do actual mathematics. We seek to use these ideas to mathematically prove new ideas which we will call **theorems**. There are two special types of theorems called **lemmas** and **corollaries**. A lemma is a theorem used to mathematically prove what the author considers to be a more important theorem. A corollary is a theorem which is a specific instance of a more general theorem.

Thus in order to understand the idea represented by the word "theorem" we need to understand what is meant by mathematical proof. **Mathematical proof**, is the process of concluding new true statements from axioms and definitions via sound logical argument. For our purposes, we will interpret "sound logical argument" to mean mathematical steps consistent with established axioms and definitions.

For instance consider the following pseudo-theorem:

Theorem 1. *If* $x = 1$ *and* $y = 2$ *then* $0 = 2$

Proof:

$$0 = \frac{y - 2x}{y} = \frac{y - 2x}{y} \cdot \frac{xy - 2}{xy - 2} = \frac{xy^2 - 2y - 2x^2y + 4y}{xy^2 - 2} = \frac{4}{2} = 2$$

□

This theorem is obviously false since by definition zero and two are not equivalent ideas. This is evident in the proof, since we break our sequence of sound logical statements by dividing by zero. This action is undefined in arithmetic, and we will come to see that limiting to a zero denominator is the fundamental idea of calculus.

If one breaks any mathematical rules in constructing an argument, he has introduced a logical flaw and hence has constructed a false argument. It is possible but rare to introduce multiple flaws in an argument that results in a pseudo-proof of a correct theorem; however, such a proof is still flawed although the theorem may not be. It is the prerogative of the reader of a mathematical work to verify all steps in proofs of purported theorems are consistent with established mathematical axioms and definitions, since the tiniest bit of flawed logic can falsify an eleven-hundred page calculus text.