Teaching an Introductory Proofs Class

August 6, 2014

James Bisgard
Central Washington University

bisgardj@cwu.edu and www.cwu.edu/~bisgardj
At CWU, Math 260 “Sets and Logic” is our introduction to proof class

- 10 week (CWU is on a quarter system) course that meets Monday through Friday

- Usually between 20 and 30 students

- Pre-requisites: either two quarters of calculus, OR one quarter of calculus and one quarter of programming

- Audience: “Standard” math majors, prospective high school teachers, Computer Science majors, some math minors

- No one single mathematical subject, but more emphasis on sets and basic number theory
My thinking about this course has been formed by the two texts I’ve used. My first two times, I used *How To Prove It* by Daniel Velleman, 2nd edition, Cambridge University Press, 2006.

This emphasizes that understanding the logical structure of a statement can help construct a proof. Unfortunately, I wasn’t able to get as far into the book as I would have liked, and so I switched to *Logic, Sets, & Proof: An Introduction* by James Harper, one of my colleagues at CWU.

There is less discussion of the structure of proofs, but students start writing their own proofs faster. In addition, I find it straightforward to add emphasis about structure.
I’ve taught several subsequent junior level math courses where students have to write proofs. From my experience in those courses, one of my goals in our introductory proof course is:

**Minimize the number of conversations that begin with “I don’t know where to start” in future classes!**

In subsequent classes, I want to discuss the content of those classes, not how to start the proof of a conditional, or the basic set up for showing two sets are equal. A sample homework problem:

*Consider the theorem: Suppose $a, b, \text{ and } c$ are integers and $a | b$ and $a | c$. Then, for any integers $k_1, k_2$, $a | (k_1 \cdot b + k_2 \cdot c)$.***

1. **Give a format for a proof of this theorem.**
2. **Prove this theorem.**
Since $x \mid y$ is an existence statement, and a direct proof of an existence statement has the form of [give a candidate for the thing] [show the thing does the right stuff] (where we use square brackets around the portions that will need detail), a possible format is:

Let $a, b, c \in \mathbb{Z}$, and suppose $a \mid b$ and $a \mid c$.

Let $k_1, k_2$ be arbitrary integers.

[Find a candidate $m \in \mathbb{Z}$ ]

[Show that $m$ does what it’s supposed to: $ma = k_1 b + k_2 c$]
A possible proof is then:

Let \( a, b, c \in \mathbb{Z} \), and suppose \( a|b \) and \( a|c \). Let \( k_1, k_2 \) be arbitrary integers. Since \( a|b \) and \( a|c \), there are integers ♥ and ♣ so that ♥ \cdot a = b and ♣ \cdot a = c. Let \( m := k_1 \cdot ♥ + k_2 \cdot ♣ \). We then have

\[
ma = k_1 \cdot ♥ \cdot a + k_2 \cdot ♣ \cdot a = k_1 \cdot b + k_2 \cdot c,
\]

and so there is an integer \( m \) so that \( ma = k_1 \cdot b + k_2 \cdot c \), i.e. \( a|(k_1 \cdot b + k_2 \cdot c) \).

When we go over solutions, we always match the parts of the outline with the corresponding parts of the proof.
Some more thoughts:

1. Detail is important! Switching the order on quantifiers can completely change the meaning of a statement. Or simply misplacing a few parentheses can cause all sorts of trouble:

\[
\forall n \in \mathbb{N} \; P(n) \equiv P(1) \land \left( \forall n \in \mathbb{N} \; (P(n) \rightarrow P(n + 1)) \right) \\
\not\equiv P(1) \land \left( (\forall n \in \mathbb{N} \; P(n)) \rightarrow P(n + 1) \right)
\]

2. Language is important: “any” and “some” make very different statements!

3. Emphasize that proofs aren’t like calculus - proofs are not solved!

4. Encourage your students - proofs are not like calculus!