Communication for maths

On the presentation of proof by induction

What is a proof, and what is it for?

- A proof is
  - designed to confirm the truth of a mathematical statement;
  - a set of mathematical steps which, by logical inference and algebraic manipulation, leads to the conclusion that the mathematical statement is true.

What is a proof, and what is it for?

- A proof is
  - a series of statements, …
  - … each of which follows logically from axioms and/or (by the rules of logic and algebra) from what has gone before. …
  - … It starts with things we know to be (or accept as) true, …
  - … and it ends with the thing we are trying to prove.

What is a proof, and what is it for?

- *Example*

Theorem

If n and m are odd integers, then $n + m$ is even.

Proof: Let n and m be odd integers. Then

$$n = 2j + 1 \qquad \text{and} \qquad m = 2k + 1$$

for some integers j and k.

What is a proof, and what is it for?

Then

$$n + m = (2j + 1) + (2k + 1)$$
$$= 2j + 2k + 2$$
$$= 2(j + k + 1). \qquad (*)$$

Since $j + k + 1$ is integer, and (*) is by definition even, $n + m$ is even.

Q.E.D.

What is a proof, and what is it for?

- *Another example*

Proofs do not have to be just full of symbols. Some proofs are very wordy. The following is taken form a mathematics journal:

Theorem 2.7 (General Remainder Theorem over a commutative coefficient ring): *Let R be a commutative ring; let $f, m \in R[x]$ with $m = a_h x^h + a_{h-1} x^{h-1} + \cdots + a_1 x + a_0$ and $h > 0$; and let a_h be a unit of R.*

(1) *If $f = 0$ or $\deg(f) < h$, then the remainder of f modulo m in $R[x]$ is f;*
(2) *If $\deg(f) \geq h$, then the remainder of f modulo m in $R[x]$ can be found by substituting the polynomial $s = a_h^{-1}(-a_{h-1}x^{h-1} - \cdots - a_1 x - a_0)$ for x^h in f, and iterating this substitution in the polynomial thus obtained until its degree becomes less than h.*

What is a proof, and what is it for?

Proof: We have $f = 0m + f$; then if $f = 0$ or $deg(f) < h$, for the uniqueness provided by Theorem 2.6, the remainder is f.

Let us now analyze the case $n = deg(f) \geq h$. Since a_h is a unit of R, then there exists $a_h^{-1} \in R$, and, therefore, the polynomial $s \in R[x]$. In addition, $x^h \equiv_m s$ because $x^h - s = a_h^{-1}m$. Therefore, by Remark 1, the polynomial f_1 obtained by replacing x^h with s in f is m-congruent to f; thus, there exists $a \in R[x]$ such that $f = am + f_1$. Hence, if $deg(f_1) < h$, for the uniqueness provided in Theorem 2.6, f_1 is the remainder of f modulo r, and the theorem is proved. Otherwise, we can observe that $deg(f_1) < deg(f)$ because x^h has been replaced with a polynomial s of degree less than h; then, repeating this replacement in f_1, we obtain a polynomial f_2 that is m-congruent to f_1 and having $deg(f_2) < deg(f_1)$. Iterating at most $k = n - h + 1$ times the previous replacement, we obtain a sequence of polynomials $f_1, f_2, \ldots, f_k \in R[x]$ with $f \equiv_m f_1 \equiv_m \cdots \equiv_m f_k$ and $deg(f_k) \leq n - k = h - 1$. For the uniqueness provided by Theorem 2.6, f_k is the remainder of f modulo m in $R[x]$. ■

From F. Laudano (2018): A generalization of the remainder theorem and factor theorem, *International Journal of Mathematical Education in Science and Technology*

Requirements for presenting proof by induction on this maths course

- *Three key words*
  1. **"Claim"**: State the expression you wish to prove. You can also label it as a statement. The usual symbol for this is $P(n)$. For example

a) Claim : $\sum_{i=1}^{n} 2i = n^2 + n \quad , \quad n \in \mathbb{N}$

b) Claim : Let $P(n)$ be the Statement

$4^n - 1$ is divisible by 3 for $n \in \mathbb{N}$

Requirements for presenting proof by induction on this maths course

- *Three key words*
  2. **"Proof"**: Present your proof, using algebra, logic and only that which is already known or assumed.

  More on this in a moment.

  An appropriate example of this is:

<u>Proof</u> : Base case : .....

Requirements for presenting proof by induction on this maths course

- *Three key words*

  3. **"End of Proof"**: This formally states that you have finished the proof and that (hopefully) you have shown your statement to be true.

  To show the end of a proof you can do one of the following:

  - Write "End of proof";
  - Write "QED". This is Latin for "quad erat demonstrandum", and means "What was to be demonstrated";
  - Use the symbol "■" at the end of the last line of your proof.

Requirements for presenting proof by induction on this maths course

- *Three key words*
  3. An example of an appropriate end-of-proof statement is:

.... $P(n)$ is true $\forall\, n \in \mathbb{N}$ $\blacksquare$

Requirements for presenting proof by induction on this maths course

- *Presenting your proof*

  Five important points to note when presenting you proof:

  - Base case: Make sure to show the test of LHS and RHS separately (why?).

Requirements for presenting proof by induction on this maths course

- *Presenting your proof*

  Five important points to note when presenting you proof:

  - For $\sum_{i=1}^{n} 2i = n(n+1)$ we present

Base case: $n = 1$

$LHS = 2(1) = 2$

$RHS = 1(1+1) = 2$

$\therefore LHS = RHS, \therefore \ldots$

Requirements for presenting proof by induction on this maths course

- *Presenting your proof*

  Five important points to note when presenting you proof:

  – State the inductive assumption. An appropriate example of this is:

Assume $P(k)$, i.e. $\sum_{i=1}^{k} 2i = k^2 + k$, $1 \le k \le n$

Requirements for presenting proof by induction on this maths course

- *Presenting your proof*

  Five important points to note when presenting you proof:

  – State when the inductive assumption has been used. An appropriate example of this is:

By assumption $\sum_{i=1}^{k} 2i = k^2 + k$

$\therefore \sum_{i=1}^{k} 2i + 2(k+1) = k^2 + k + 2(k+1)$

Requirements for presenting proof by induction on this maths course

- *Presenting your proof*

  Five important points to note when presenting you proof:

  – State that the inductive step has been shown. An appropriate example of this is:

Hence $P(k) \Rightarrow P(k+1)$

Requirements for presenting proof by induction on this maths course

- <u>*Presenting your proof*</u>

  Five important points to note when presenting you proof:

  – Formally state the conclusion of the proof. An appropriate example of this is:

$$\therefore \quad P(n) \text{ is true } \forall n \in \mathbb{N}$$

Example and exercise

- **Example 1:** Consider example 1 handed out. This represents a correct presentation of proof by induction.

- **Exercise 1:** Consider exercise 1. Go through the proof presented and identify those element missing from the presentation of this proof.

Important comments

1. Assuming that all your algebra is correct, the steps that you show is as important as the correctness of the proof itself:

   – Too few steps means the reader has to do all the work (in which case you are not communicating or presenting maths, instead you are setting an exercise);

Important comments

1. Assuming that all your algebra is correct, the steps that you show is as important as the correctness of the proof itself:
   - Too many steps usually means that you are presenting steps which are trivial.
     Don’t confuse “trivial” with “obvious”. What is a trivial step to you may still need to be shown.

Important comments

2. A proof need not contain only symbolic maths. It is ok, and actually preferable, to write brief phrases where appropriate.

   One such example is when you state that you are using the inductive assumption $P(k)$. You actually write this, at the appropriate point in the proof, *as part of* your proof.

Important comments

3. How you physically write/present the proof on paper is equally as important as the correctness of the proof itself.

   In other words, follow the guidelines about physical presentation and formatting you have seen so far in this course, as well as the guidelines to come.

Important comments

4. “QED” is only used at the end of a proof, nowhere else.

   So, do not write “QED” unless the maths you are presenting is a proof.

   “QED” does not come at the end of an example, exercise, or anywhere else.

Presentation

Reminder

- The above slides refer to only a few of the aspects of mathematical presentation.
- Refer to previous slides for all other aspects of mathematical presentation in order to give a full and proper solution to a problem.