Methods of Proof

Ross Mathematics Program 2016

Every summer, new first-year students experience the frustrations that inevitably accompany their inability to justify their beliefs. To help systematize their approaches to theorem-proving, we have prepared this monograph on methods of proof. While intended for the beginner, advanced students and teachers will find much of value here.

All of these methods are based on the ...

BS Postulate: Anything you can get away with is a valid approach.

It is evident that this is consistent with the Zermelo-Frankel Postulates, with or without the Axiom of Choice. For an example, see the previous sentence.

A few time-savers:

T-S1. For a problem that takes more than two lines to state, simply put down: "Already done on Set #14," and forget about it.

T-S2. Salvages: Prove that the problem statement is false, or, better yet, salvage it to $0 + 0 = 0$. (True in $\mathbf{Z}$, true in $\mathbf{Z}_m$, true in $\mathbf{Z}[i]$.)

T-S3. If you face significant difficulties with a problem, simply define it to be true as an axiom. If it turns out to be inconsistent, keep in mind even Zermelo had controversial results when defining axioms.

T-S4. **(Theorem of Obviosity)** Anything obvious need not be proven, cannot be proven, and when you get right down to it, is probably false.

T-S5. **(Theorem of Inobviosity)** Anything not obvious is probably true. For example, since the previous sentence isn't obvious, it's probably true.

Elementary Methods of Proof

Proof by Omitted Base Case.
To prove: all positive integers are greater than 9000.
Proof: Let $S = \{n \in \mathbf{Z}^+ : n \leq 9000\}$. Assume for the sake of contradiction that S is nonempty, so by the Well-Ordering Principle it has a least element ℓ. But if $\ell \leq 9000$, then since $\ell - 1 < \ell$, we must have $\ell - 1 \leq 9000$ as well. So $\ell - 1 \in S$, and ℓ is not the least element. This is the desired contradiction.

Proof by Lecture Theory.
To prove: Generalized Riemann Hypothesis.
Proof: We know that $1 = 1$. The important consequence (assuming Artin reciprocity) is the following:

$$\zeta(\cdots\cdots\cdots\cdots$$

$$\vdots$$

$$\vdots$$

Thus by the work above, which sadly as in lectures often gets erased, GRH is a trivial consequence. In fact, it is an exercise left to the reader to generalize the result even further.

Proof by Contradiction.
Let $a, b \in \mathbf{Z}, b \neq 0$. Suppose there exist no $q, r \in \mathbf{Z}$ such that $a = bq + r$ and $0 \leq r < |b|$. But when $a = 7$ and $b = 3$, $7 = 3 \cdot 2 + 1$, and $0 \leq 1 < |3|$, contrary to its non-existence. Thus $\forall\ a, b \in \mathbf{Z}$, $b \neq 0$, $\exists\ q, r \in \mathbf{Z}$ such that $a = bq + r$ and $0 \leq r < |b|$.

Proof by Let.
Let $x = [a_1, ..., a_n]$. Let $x = \frac{P_n}{Q_n}$. Then by transitivity of equality, $[a_1, ..., a_n] = \frac{P_n}{Q_n}$.

Proof by the Well-Ordering Principle.
To prove: All positive integers are fairly small.
Proof: Let $S = \{n \in \mathbf{Z}^+ : n \text{ isn't fairly small}\}$. Suppose $S \neq \varnothing$. Since $S \subseteq \mathbf{Z}^+$, WOP implies that S has a least element n_0. But n_0 must be fairly small if it is less than every other element of S. $\Rightarrow\Leftarrow$. Therefore $S = \varnothing$. Hence all positive integers are fairly small. (Related results: Every positive integer can be uniquely described in at most fifteen English words. All positive integers are clearly smaller than a million. All positive integers are medium-sized. All positive integers are over-rated.)

Proof by Example. (Proof by Pseudo-Induction, Proof by Calculator, Proof by Lack of a Counter-Example, Proof by "..." , etc.)
Let p be prime. $2^2 - 1$ is prime, $2^3 - 1$ is prime, $2^5 - 1$ is prime, and $2^7 - 1$ is prime. Continuing in this manner, $2^p - 1$ is prime.

Proof by Assumption.
Suppose $ax + by = 1$ has a solution in $\mathbf{Z}$. Then $ax = 1 - by$, so $a|(1 - by)$. Therefore $\exists\ k \in \mathbf{Z}$ such that $ak = 1 - by$. Similarly, $\exists\ j \in \mathbf{Z}$ such that $bj = 1 - ax$. Adding, $ak + bj = (1 - by) + (1 - ax) = 2 - (ax + by) = 2 - 1$. But $2 - 1 = 1$, so $ax + by = 1$ has an integer solution, namely $x = k$ and $y = j$.

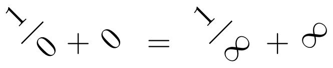
Proof by Differentiation.
Let $x = 1$. Differentiate both sides to yield $1 = 0$. As before, this proves the result.

Proof by Solving Another Problem.
To prove: Every even integer greater than 4 is the sum of two odd primes.
Proof: $1 + 1 = 2$. Thus every even prime is the sum of two odd integers.

Proof by Tautology.
To prove: $1 = 3$.
Proof: Assume $1 = 3$. Then $3 = 1$. Adding the two equations gives $4 = 4$. But this is true since "=" is an equivalence relation and hence is reflexive. Since we have deduced a tautology from our original statement, it must be true.

Proof by Theorem that Almost Applies.
To prove: the set $\mathbb{R}$ of real numbers cannot be put into bijection with the set $\mathbb{R} \setminus \{0\}$ of nonzero reals.
Proof: From set theory, the cardinality of $\mathbb{R}$ is $2^{\aleph_0}$, and the cardinality of $\mathbb{R} \setminus \{0\}$ is $2^{\aleph_0} - 1$. Suppose these are equal. Rearranging gives $2^{\aleph_0} + 1 = 2^{\aleph_0} + 1^{\aleph_0} = 2^{\aleph_0}$, which is impossible by Fermat's Last Theorem.

Proof by Rotation.
Since $\dfrac{1}{0} = \infty$ and $\dfrac{1}{\infty} = 0$, we have $\dfrac{1}{0} + 0 = \dfrac{1}{\infty} + \infty$. Successive rotations yield:



$$\begin{aligned} -10 + 0 &= -18 + 8 \\ -10 &= -10. \end{aligned}$$

□

Advanced Techniques (Used by the Professionals).

Some useful technical phrases are: "the proof is an exercise left to the interested reader." The proof is: "immediate," "an obvious corollary," "already done," "follows from (10.1)." Alternatively it can be useful to say: "No simple proofs are known," "proof is a straightforward calculation," "proof is beyond the scope of this book," "proof may be found in Grothendieck's *Élements de Géométrie Algébrique (EGA)*, p. 4551," "proof follows by a standard application of motivic cohomology," "proof is a simple application of the Atiyah-Singer index theorem for elliptic operators," etc.

General types of advanced proofs:

- Proof by sweeping generalization
- Proof by opaqueness
- Proof by vague preceding discussion
- Proof by non-existent lemma
- Proof by diagram of simplest possible case
- Proof by inability to find a counterexample
- Proof by intimidation
- Proof by awesome notation
- Proof by erasure
- Proof by forceful manner
- Proof by premature "QED"

Here are illuminating examples from Greenberg & Harper, *Algebraic Topology: A First Course*, p. 292:

> **Lemma.** Let $K : (V, V - x) \to (V \times V, V \times V - \Delta)$ be the inclusion.
> Then $M \cdot N = \sum_i [{\zeta_M}^{x_i} \times {\zeta_N}^{x_i}, H(K)\mu]$, where μ is the Thom class and ${\zeta_M}^{x_i} \times {\zeta_N}^{x_i}$ is regarded as an element of $H_N(V, V - x)$.
>
> *Proof:* By (30.2), $[{\zeta_V}^{x_i}, H^N(K)\mu] = 1$.
>
> **Proposition:** The cup product $S'(X)$ is bilinear, associative, and has as identity element the 0-cochain 1 defined by $[x, 1] = 1$ for every point x in X.
>
> *Proof:* Easy. (Note: previously 1 was denoted $\partial^{\#}$ (19.2).).

Invoking a large theorem to help a small proof.[1]

> **Proposition.** If $n \geq 3$, then the n^{th} root of 2 is irrational.
>
> *Proof:* Suppose $\sqrt[n]{2} = p/q$ where p, q are positive integers. Then $2q^n = p^n$ which can be rewritten as $q^n + q^n = p^n$. This is impossible by Fermat's Last Theorem. QED

[1] Grader's comment on this method: "Don't pound in a thumbtack with a sledgehammer. Use your head!"

Exercises

For each problem, apply one of the techniques discussed above, even if you know of another solution method.
(Starred problems are more difficult, since they are not stated in "Prove that . . . " format.)

P1. Prove the theorems of Obviosity and Inobviosity. (Hint: see (3.6.1.2.7).)

P2. Prove that $a^n + b^n = c^n$ has no solutions $a, b, c, n \in \mathbf{Z}^+$.

P3. Prove that there are no odd perfect numbers. (Use P2).

P4. Prove that there are no positive integers between two consecutive positive integers.

P5.* Find a formula for the n^{th} positive integer.

P6. Prove that $\mathbb{Z}ed \neq \mathbb{Z}$.

P7. Prove that Pell's Equation is a pain.

P8. Prove that any two finite fields are practically the same.

P9. Prove that any sufficiently large abelian group must be commutative.

P10.* How big must a field be to hold a group of rings? A ring of groups?

P11.* $p \equiv 1 \pmod 3 \implies x^2 + x + 1$ has a root in $\mathbf{Z}_p$.
Use this fact to prove the Diophantine property for $\mathbf{Z}$.

P12. Prove that there are no perfect squares.
[Hint. Show that $\sigma(n^2) \neq 2n^2$. Deduce that n^2 cannot be perfect.]

P13.* What question is its own answer?

P14.$^\bigstar$ This sentence no verb. Other sentences have contain two verbs. Explain.

P15. Prove that this sentence does not refer to itself.

P16. Prove a statement of your own choice that is obviously false.

Essay question. Explain your position on the following question. Is it not true that you couldn't fail to disagree with Ross's methods any less than you did before?