INTRODUCTION TO PROOFS (MATH 25)

MIKE GREENE AND TONY VARILLY

ABSTRACT. This handout is intended to be a short supplement for students wishing to gain famailarity with the standard methods of mathematical proofs. While proof techniques here are somewhat elementary, we have attempted to include examples which are mathematically important. Note that you should NOT judge the difficulty or mathematical sophistication of Math 25 based on the level of presentation in this handout; if you find *most* of this handout particularly difficult, you may want to reconsider your choice of math course (but feel free to contact us first).

The fundamental object of pure mathematics is the proof. A *proof* is a short exposition whereby the logical validity of a claim is demonstrated with certainty. Specifically, a proof starts from a collection of fundamental *axioms* as well as specific *hypotheses*. In Math 25, you are welcome to employ basic notions from high school single-variable calculus, theorems proved in class or in the textbook, and theorems you have proven in previous Math 25 problem sets as well in your proofs.

1. Basic Terminology and Notation

Axiom An axiom is a fundamental and unproveable statement of mathematics. For example, one of the most important axioms of arithmetic is that "every natural number, n, has a successor, $n+1$." (The term *postulate* is a synonym.)

Hypothesis A hypothesis is a condition placed on a statement in a claim. For example, the claim that "if n is a prime greater than 2, then n is odd" includes the hypothesis that n is a prime greater than 2.

Implication A statement, A, is said to imply a statement B if "A and not B" is always false. This is written $A \Rightarrow B$.

Negation The negation of a statement A is the statement that A is false. This is written variously as $!A$, $\neg A$, "not A", or $\overline{A}$. We recommend that you avoid the last form because it is easily confused with equivalence.

Converse The converse of a statement of implication, $A \Rightarrow B$ is $B \Rightarrow A$. For example, the statement "all men are mortals" (which is really saying that "x is a man $\Rightarrow$ x is mortal") has the converse "all mortals are men."

2. Standard Techniques

There are a number of standard proof techiques that are worth knowing.

Technique (Proof by Contradiction). *A proof by contradiction begins by assuming a statement equivalent to negation of the claim and then deriving a contradiction with either the hypotheses of the claim or the axioms of mathematics.*

Example (Euclid). *There are infinitely many prime natural numbers.*

Proof. Assume, contrary to the claim, that there are only finitely many prime natural numbers. Specifically, assume there are n of them. Thus we can name them $p_1, p_2, \ldots, p_n$. Next, consider

$$p' := p_1 \cdot p_2 \cdot \ldots \cdot p_n + 1$$

(The symbol ":=" means "we are writing a definition of a term on the left".) Observe that p' has a remainder of 1 when divided by p_i for any $i \leq n$. Thus there are more than n primes. $\Rightarrow\Leftarrow$. □

(The symbol "$\Rightarrow\Leftarrow$" means "and we have derived a contradiction.) In summary, we assumed that the claim was false and derived a contradiction. Thus the negation of the claim is equivalent to a falsehood and thus the claim is true.

Example. $\sqrt{2}$ *is irrational.*

Proof. Suppose, to the contrary, that $\sqrt{2}$ is a rational number and write $\sqrt{2} = m/n$ in lowest terms. Squaring both sides, and multiplying by n^2, we get $2n^2 = m^2$. Thus, m^2 is even, which means m must be even (prove!). Write $m = 2m_1$. Then $2n^2 = 4m_1^2 \Rightarrow n^2 = 2m_1^2$. But this means n^2 is even and so n is even. This is a condraction since we assumed the fraction m/n was in lowest terms. So our hypothesis that $\sqrt{2}$ is rational must be wrong. □

Technique (Proof by Contrapositive). *Proofs by contrapositive rest on the fact that $A \Rightarrow B$ is equivalent to $\neg B \Rightarrow \neg A$.*

Example. n^2 *is odd* $\Rightarrow$ n *is odd.*

Proof. We instead prove the contrapositive, that n is not odd $\Rightarrow$ n^2 is not odd (or more concisely, that even numbers have even squares). We note that an even number, n, be expressed as $2m$ for some m. Thus,

$$n^2 = (2m)^2 = 4m^2$$

which is necessarily even. □

Technique (Mathematical Induction). *This technique is analogous to a string of falling domino tiles. First, you show that the first domino falls; this is known as the* base case. *Then you show that if any given domino falls,the next one topples as well.*

Example. *Let n a positive integer. Then $n^5 - n$ is divisible by 5.*

Proof. We "induct" on n. If $n = 1$, then $1^5 - 1 = 0$, and zero is divisible by 5. (The first domino has fallen.) Suppose the theorem holds for some positive integer n, that is $n^5 - n$ is divisible by 5. We want to show that $(n+1)^5 - (n+1)$ is divisible by 5. We have

$$(n+1)^5 - (n+1) = n^5 + 5n^4 + 10n^3 + 10n^2 + 5n + 1 - (n+1) \tag{1}$$

$$= (n^5 - n) + 5(n^4 + 2n^3 + 2n^2 + n). \tag{2}$$

We know by *induction hypothesis* that $n^5 - n$ is divible by 5. Clearly, the remaining expression in (2) is also divisible by 5. Hence $(n+1)^5 - (n+1)$ is divisible by 5. This completes our proof by induction □

This example can be generalized. We have $n^p - n$ is divible by p where p is a prime number. This is known as *Fermat's Little Theorem.*

Proof of Fermat's Little Theorem. We'll prove the theorem by induction, in a very similar way to the case $p = 5$ done above. Notice first that $1^p - 1 = 0$ for any p and 0 is divisible by p. This gives us our base case. Assume the theorem is true for some n, that is, $n^p - n$ is divisible by p. We want to show that $(n+1)^p - (n+1)$ is divisible by p. This time, we have

$$(n+1)^5 - (n+1) = n^p + \binom{p}{1}n^{p-1} + \binom{p}{2}n^{p-2} + \cdots + \binom{p}{p-1}n + 1 - (n+1) \tag{3}$$

$$= (n^p - n) + (\binom{p}{1}n^{p-1} + \binom{p}{2}n^{p-2} + \cdots + \binom{p}{p-1}n), \tag{4}$$

where $\binom{p}{k} = \dfrac{p(p-1)\cdots(p-k+1)}{k(k-1)\cdots 1}$. We say "$p$ choose k" for $\binom{p}{k}$. We know by induction hypothesis that $n^p - n$ is divisible by p. For $k > 1$ $\binom{p}{k}$ is divisible by p. This is because all the factor in the denominators of are fraction are smaller than p; since p is prime, it follows p is not cancelled. So the second part of (4) is divisible by p, and so $(n+1)^p - (n+1)$ is divisible by p. This concludes the proof. □

Technique (Strong Mathematical induction). *This is a slight variant on mathematical induction. Again, first you prove a statement for some small suitable number (your base case). Now you assume the statement holds* for all k *between your base case and* n *and prove the statement for* $n + 1$.

Our example for strong induction will come from graph theory. Intuitively speaking, a *simple graph* is a collection of vertices on the plane and edges joining some of these vertices such that no edge joins a vertex to itself and there are no multiple edges between vertices (not to be confused with the graph of a function!). We let e denote the number of edges of a graph, and v the number of vertices. A *tree* is a simple graph that contains no 'circuits'. Intuitively speaking, graph is connected if you cannot think of it as two separate pieces without altering the graph.

Example. *Let Γ be a connected tree with e edges and v vertices. Then $e = v - 1$.*

Proof. As advertised, we'll use strong induction. We'll "induct" on the number of edges e. If $e = 1$, then graph must consist of two vertices joined by an edge. There can't only be one vertex because then the edge would join the vertex to itself; also, there can't be more than two vertices because then the graph would be disconnected. So $e = v - 1$ in this case. Now suppose that *all* trees with fewer than e edges satisfy the desired formula. Consider any tree with e edges. Pick any edge and remove it. You will disconnect the tree into two components, each of which is a tree, and has at most $e - 1$ edges. Suppose these two trees have e_1 and e_2 edges, v_1 and v_2 vertices respectively. By inductive hypothesis, $e_1 = v_1 - 1$ and $e_2 = v_2 - 1$. Add these equations and we get $e_1 + e_2 = v_1 + v_2 - 2$. But $e = e_1 + e_2 + 1$ and $v = v_1 + v_2$ by construction. Thus $e = v - 1$ for this bigger tree too. This concludes the proof by induction. □

Mathematics Department, Harvard University
E-mail address: mgreene@fas.harvard.edu, varilly@fas.harvard.edu