Introduction to Mathematical Proofs

If I am going to help you with math, I will have to use LaTeX. I'll start with something simple: describing two kinds of mathematical proof.

First, what exactly is a proof? A proof is an argument that shows, using only deductive logic, that a certain proposition is true. For instance, here is a very simple proof of the statement "every natural number n is either even or odd", where an even number is any natural number n that is divisible by two, and an odd number n is any natural number that leaves a remainder of 1 when divided by two.

We know, by the properties of the division algorithm, that when a natural number n is divided by another non-zero natural number d the result is a quotient q and a remainder r, where $n = dq + r$, and $0 \leq r < d$. The result follows immediately, because the only possible remainders upon division by 2 are 0 (even numbers) and 1 (odd numbers). Here endeth the proof.

<=======>

Now mathematical proofs can take many forms. A very common and ancient type of proof is the proof by contradiction, or *reductio ad absurdum*. We begin by assuming that a certain statement is true. We proceed, using only deductive logic, to prove that this implies a contradiction. Therefore the assumption is false, and its negation must be true.

Here are a couple of famous proofs by contradiction. The first one is Euclid's proof that there is no largest prime number. Suppose that there are only finitely many prime numbers, $p_1, p_2, p_3, \ldots p_n$. Clearly, we can form the number $P = p_1 * p_2 * p_3 * \ldots * p_n + 1$. P cannot be divisible by any of the primes p_i, because it leaves the remainder 1 upon division by any of the p_i. So either P is prime or, if it is composite, it is divisible by some prime $p' > p_n$. Either way, the original list of "all" the prime numbers is incomplete.

Here I'd like to take a little detour to introduce some mathematical notation that may be unfamiliar to you. In the preceding proof we used an extended product $p_1 * p_2 * p_3 * \ldots * p_n$. Extended products come up fairly often in higher mathematics; mathematicians have invented a shorthand notation for them using the Greek letter Π:

$$\prod_{i=1}^{n} p_i = p_1 * p_2 * p_3 * \ldots * p_n$$

Using the extended product notation, we can easily define the factorial function ($n!$), which comes up a lot in calculus.

$$n! = \prod_{i=1}^{n} i = 1 * 2 * 3 * \ldots * n$$

OK, so here's another proof by contradiction, also known to the ancient Greeks: the square root of 2 is not a rational number, that is, it cannot be expressed as a fraction $\frac{m}{n}$.

For the sake of argument, suppose that $\sqrt{2} = \frac{m}{n}$ where the fraction $\frac{m}{n}$ has been expressed in lowest terms (that is, m and n do not share a common prime factor). Then we have

$$\sqrt{2} = \frac{m}{n} \tag{1}$$

$$2 = \frac{m^2}{n^2} \tag{2}$$

$$2n^2 = m^2 \tag{3}$$

Since the left-hand side of (3) is even, m is an even number, because the square of an odd number is always odd. So we can substitute $m = 2k$ in equation (3) above:

$$2n^2 = (2k)^2 \tag{4}$$

$$2n^2 = 4k^2 \tag{5}$$

$$n^2 = 2k^2 \tag{6}$$

But now from equation (6) we see that n must also be an even number, contradicting our assumption that m and n do not have a common prime factor.

<=======>

OK, now that we understand how the proof by contradiction works, let's think about another common form of proof: the proof by mathematical induction. This form of proof depends on the fact that we can form each natural number as the sum of ones – $1 = 1 + 0; \quad 2 = 1 + 1; \quad 3 = 2 + 1; \quad \ldots$

The *principle of mathematical induction* states that if an assertion is true when $n = 1$, and if the fact that the assertion is true when $n = k$ implies that the assertion is also true when $n = k + 1$, the assertion is true for every natural number n.

Let's use mathematical induction to prove a formula that generates the triangular numbers. The nth triangular number is the sum of the first n positive integers. So we have $T_1 = 1; \quad T_2 = 1 + 2 = 3; \quad T_3 = 1 + 2 + 3 = 6; \quad \ldots$ I assert that $T_n = \frac{n(n+1)}{2}$. The proof is by mathematical induction.

First we observe that the formula is correct for T_1: $T_1 = 1 = \frac{(1*(1+1))}{2} = \frac{(1*2)}{2}$.

So the formula is correct when $n = 1$. Now comes the induction step. Suppose that

$$T_n = \frac{n(n+1)}{2} \tag{7}$$

It follows that

$$\begin{aligned} T_{n+1} &= T_n + (n+1) && (8) \\ &= \frac{n(n+1)}{2} + (n+1) && (9) \\ &= \frac{n^2+n}{2} + \frac{2(n+1)}{2} && (10) \\ &= \frac{n^2+3n+2}{2} && (11) \\ &= \frac{(n+1)(n+2)}{2} && (12) \\ &= \frac{(n+1)((n+1)+1)}{2} && (13) \end{aligned}$$

and the induction is complete.

OK, one more notational convention and then we're done for now. There is another kind of mathematical shorthand, using the Greek letter sigma (Σ) to signify a sum. Pi is for product; sigma is for sum. We write $\Sigma_{i=1}^{n} s_i$ to denote the quantity $s_1 + s_2 + s_3 + \ldots + s_n$.

So now we can write a shorthand expression for the nth triangular number:

$$T_n = \sum_{i=1}^{n} i$$

A lot of higher mathematics involves sums with infinitely many terms. To define such sums rigorously we must first define the concept of a limit. I'll talk about limits next time. For now, here's a famous infinite sum to think about.

$$\sum_{k=1}^{\infty} \left(\frac{1}{2}\right)^k = \quad ?$$