Proofs

This is meant to be an informal document detailing a few common proof techniques in multiple subjects. This means that the formatting may not even be the same; this is me jotting down my thoughts on some proofs, and probably some other related stuff.

Proofs are not just informal observations, although their inception usually relies on them. Well, I've run out of stuff to say, so enjoy the handout! The solutions are here.

Induction

Induction is a two-step process:

1) Prove that $P(n),$ where $P(n)$ denotes the identity or theorem you are trying to prove, is true for a particular value of $n.$ This is generally known as the base case, and it is usually proven for small values of $n,$ such as $n = 1.$
2) Prove that $P(n+1)$ is true *if* (not if and only if, just if) $P(n)$ is true.

Let's look at a few examples:

1. Prove that $\sum_{x=1}^{n} x = \frac{n(n+1)}{2}.$

Solution: Let us have $n = 1$ be our base case. Clearly, $1 = \frac{1(1+1)}{2}.$ Then we may prove that $(1 + 2 + ... + n + n + 1) = \frac{(n+1)(n+2)}{2}$ by subtracting $(1 + 2 + ... + n)$ and $\frac{n(n+1)}{2}$ from the left and right side of this equation. (We can assume that $(1 + 2 + ... + n) = \frac{n(n+1)}{2}$ because we assume $P(n)$ is true.) Doing this gives us $n + 1 = \frac{2(n+1)}{2}$ which is clearly true. We have proved this identity using induction.

However, something more interesting may be how we derived this formula. (This is usually known as the motivation.) We note that by the commutative property, $1 + 2 + ... + n = n + (n - 1) + ... + 1.$ Add this to itself, matching values, to get $(n + 1) + (n + 1) + ... + (n + 1)$ (there are n terms). The value of the sum is $n(n + 1),$ which is double the value of our initial summation (it consists of two copies of our summation). Therefore, we can divide by 2 to get $\frac{n(n+1)}{2}.$ It is important to remember that ***this is in no way a proof by induction, and this is the motivation for it*** -- in fact, it is so important that I decided to bold, underline, and italicize it! This does not make the motivation any less valid as a proof, however, it is not a proof by induction.

2. Prove that $2^{2x} + 3 \cdot 2^{x} + 2$ is divisible by 3 for all positive integer values of $x.$

Solution: Have our base case be $x = 1.$ Clearly, $2^2 + 3 \cdot 2^1 + 2$ is divisible by $3.$ We want to prove that this is true for $x + 1.$ Note that if $3|2^{2(x+1)} + 3 \cdot 2^{x+1} + 2$ then $3|2^{2(x+1)} + 3 \cdot 2^{x+1} + 2 - (2^{2x} + 3 \cdot 2^x + 2)$ which is equivalent to $3|3(2^{2x}) + 3(2^x)$ which is obviously true. By induction, we are done.

3. Prove that $x^{k+2} + x^{k+1} + x^k + x^2 + x + 1$ is always divisible by $x + 1$ for all positive integer values of $k.$

Solution: If we factor our expression out, we get $(x^k + 1)(x^2 + x + 1) \equiv x^k + 1 \ mod \ (x + 1).$ Note that if $k = 1$ then we have $x + 1$ is divisible by $x + 1,$ and if $k = 2$ then we have $x^2 + 1 = (x + 1)(x - 1)$ which is divisible by $x + 1$ too. Note then that IF $x^k + 1$ is divisible by $x + 1,$ then $x^{k+2} + 1 \equiv -x^{k+1} + 1 \equiv x^k + 1.$ All positive integers k such that $k \equiv 0 \ (mod \ 2)$ or $k \equiv 1 \ (mod \ 2)$ (these are all the positive integers) satisfy the condition. Therefore, we are done.

Here are a few problems to do yourself:

1. Prove that $\sum_{x=1}^{n} x^2 = \frac{n(n+1)(2n+1)}{6}.$

2. Prove that $5^{2n-1} + 7^{2n-1}$ is always divisible by 6 for all positive $n.$

You may be asking at this point, *"Why may I assume in the second step that $P(n)$ is true? Why must I prove a base case?"* Let's take a look at what our proof by induction does, using a "two-column proof" that goes on forever.

Claim	Reasoning
$P(n)$ is true for $n = 1.$	We have adhered to property $1,$ plugged in the value for $n = 1,$ and verified that it works.
$P(n)$ is true for $n = 2.$	We have proved that $P(n + 1)$ is true if $P(n)$ is true. Plugging in $n = 1$ gives us $P(2)$ is true.
$P(n)$ is true for $n = 3.$	We have proved that $P(n + 1)$ is true if $P(n)$ is true. Plugging in $n = 2$ gives us $P(3)$ is true.

Repeating this process infinitely gives us $P(x)$ is true for all natural numbers $x.$ This last step is usually known as the inductive process, the inductive step, or just induction. You'd imagine that doing this for every induction problem would be tedious, so we usually state that we are done by induction, the inductive step, or something similar.

Contradiction

Another method for proving a result is contradiction.
Here is how contradiction works:

Objective - We are trying to prove X.
Assume X is false.
Show that if X is false, a contradiction occurs.
Note that this contradiction means X is not false, implying X is true.

In this section, we will be using some classical problems as examples, and generalizations will be left as exercises to the reader. Perhaps the most famous example of a problem that utilizes proof by contradiction is the following:
"Prove that there are infinitely many primes."

Here is the solution:
Assume there are finitely many primes. Have them be $p_1, p_2 ... p_n.$ Note that $p_1, p_2 ... p_n - 1$ is not divisible by $p_1, p_2 ... p_n$ which implies that $p_1, p_2 ... p_n - 1$ is divisible by some other prime (possibly $p_1, p_2 ... p_n - 1$) as $p_1, p_2 ... p_n - 1$ must have a prime factorization. This leads to a contradiction as we assume there are no other primes, but we see there must be other primes. By contradiction, there are not finitely many primes. Therefore, there are infinitely many primes.

Here are a few more examples:

1. Prove $\sqrt{2}$ is irrational.

Solution: Assume $\sqrt{2}$ is rational and can be expressed in simplest form as $\frac{n}{m}.$ Then $\frac{n^2}{m^2} = 2,$ implying that $n^2 = 2m^2.$ Since $2m^2$ has a factor of $2,$ n^2 must as well. Since n is integer, n must have a factor of $2.$ Have $n = 2k$ for some other integer $k.$ Substituting, we see that $4k^2 = 2m^2,$ which implies $2k^2 = m^2.$ By the same argument above, m has a factor of two. Since both n and m have a factor of two, $\frac{m}{n}$ is not in

simplest form, leading to a contradiction. By contradiction, $\sqrt{2}$ is not rational, which means it must be irrational.

2. Prove there are infinitely many primes of the form $3n+2.$

Solution: Assume there are finitely many primes of this form. Have $p_1, p_2 ... p_n$ be our finitely many odd primes of form $3n+2.$ Then note that $3p_1p_2...p_n+2$ is not divisible by any of the primes $p_1, p_2 ... p_n,$ and that it is not divisible by $3.$ Note then that some odd prime must divide $3p_1p_2...p_n+2,$ as $3p_1p_2...p_n+2>1$ and is odd. We cannot have all of these primes be of the form $3k+1,$ because multiplying numbers with a remainder of 1 yields a remainder of $1,$ and we desire a remainder of $2.$ Thus, $3k+2|3p_1p_2...p_n+2$ for some $k.$ This leads to a contradiction, as we assumed there were no other primes in the form of $3k+2.$ By contradiction, there are not finitely many primes of the form $3n+2,$ implying that there are infinitely many primes of the form $3n+2.$

Here are some problems for you to solve:

1a. Prove $\sqrt{3}$ is irrational.

1b. Prove $\sqrt[3]{4}$ is irrational.

1c. Prove $\sqrt{k}$ is either irrational or integer for positive integer values of $k.$

1d. Prove $\sqrt[n]{k}$ is either irrational or integer for positive integer values of $k.$

2a. Prove there are infinite primes of the form $4n+3.$

2b. Prove there are infinite primes of the form $6n+5.$

Algebra: More Than One Proof

There is usually more than one way to get to an answer, even for a computational problem. The same is true of proofs. Using the examples, we will showcase a few trivial problems with a ton of ways to solve them. The most famous example of a problem with a variety of different methods, some vastly more complicated than others, is the Pythagorean Theorem. When we refer to different methods, we do not include convoluted methods or other artificial ways to inflate the count (e.g. reversing

a step of the proof for no real reason). There are many genuine methods to solve these problems.

Let's look at a few examples:

1. Prove that if $ab = ac = bc$ for non-zero values of a, b, c then $a = b = c.$

Solution A: Note that $ab = \frac{abc}{c}$, $ac = \frac{abc}{b}$, and $bc = \frac{abc}{a}$. Substituting yields $\frac{abc}{c} = \frac{abc}{b} = \frac{abc}{a}$. Dividing the entire equation by abc yields $\frac{1}{a} = \frac{1}{b} = \frac{1}{c},$ and taking the reciprocal yields $a = b = c,$ which is what we desired.

Solution B: Since $ab = ac,$ we can divide by a to get $b = c.$ A similar argument can be made for $ac = bc,$ and dividing by c yields $a = b.$ The transitive property yields $a = b = c,$ which is what we desired.

2. Prove that $a^2 + b^2 \geq 2ab$ for all positive values of $a, b.$

Solution A: Subtracting $2ab$ from both sides yields $a^2 - 2ab + b^2 \geq 0.$ Factoring gives us $(a - b)^2 \geq 0.$ Note that a square of any real number is non-negative, so we are done.

Solution B: By AM-GM $\frac{a+b}{2} \geq \sqrt{ab}.$ Squaring and multiplying both sides by 4 yields $(a + b)^2 \geq 4ab.$ Expanding then yields $a^2 + 2ab + b^2 \geq 4ab,$ which implies $a^2 + b^2 \geq 2ab,$ and we are done.

3. Prove that $\frac{n(n+1)}{2} \leq \frac{n(n+1)(2n+1)}{6}$ for all positive integers $n.$

Solution A: Note that $\frac{n(n+1)}{2} = \sum_{x=1}^{n} x = 1 + 2 + 3 + ... + n$ and $\frac{n(n+1)(2n+1)}{6} = \sum_{x=1}^{n} x^2 = 1^2 + 2^2 + 3^2 + ... + n^2.$ Matching up each term in the triangular sum with its counterpart, we see that for any of these n terms, that $k \leq k^2.$ (This should be self-explanatory.) So $1 + 2 + 3 + ... + n < 1^2 + 2^2 + 3^2 + ... + n^2$ and as such $\frac{n(n+1)}{2} \leq \frac{n(n+1)(2n+1)}{6}.$

Solution B: Expanding gives us $\frac{3n^2+3n}{6} \leq \frac{2n^3+3n^2+n}{6},$ or $\frac{2n^3-2n}{6} \geq 0.$ This implies $2n^3 \geq 2n,$ which is obviously true for positive integer values of $n.$

Here are some exercises to do:

1. If $ab = bc = cd$ for non-zero $a, b, c, d,$ find which values a, b, c, d must be equal.

2. Use Exercise 1 to prove that given a set of positive reals $(a_1, a_2 ... a_n),$ that if $\frac{\sum_{x=1}^{n-1} a_x a_{x+1}}{n-1} = \sqrt[n-1]{\prod_{x=1}^{n} a_x \prod_{x=2}^{n-1} a_x},$ then $a_1 = a_3 = ... = a_{2\lceil \frac{n}{2} \rceil - 1}$ and $a_2 = a_4 = ... = a_{2\lfloor \frac{n}{2} \rfloor}.$

3. Prove that for all positive $\{a, b, c, d\}$ that $\frac{a}{c} + \frac{c}{a} \leq \frac{(ad+bc)(ab+cd)}{abcd} - 2.$

Why does it matter if we have more than one way to prove something? Isn't one result enough? Technically, yes, but there are a few reasons why people find seemingly over complicated ways to prove simple theorems (take Pythagorean again, for example). First and foremost, this is done, in a sense, just because it can be. The love of mathematics fuels the discovery of new methods to solve already solved problems, in hopes of finding a different way to think about the problem. Secondly, some methods may work for more specific or more general versions of the problem. Take a look at the two Solutions for Example 1 and compare them to what you can find for Exercise 1. Clearly, one of the methods does not yield anything meaningful while the only one only requires a small amount of generalization.

Circles, Triangles, and Cyclic Quadrilaterals

We will show some properties of circles, triangles, and cyclic quadrilaterals. These will be used to solve some problems and examples.

In a cyclic quadrilateral ABCD, $m\measuredangle ABD + m\measuredangle ACD = m\measuredangle BDC + m\measuredangle BAC = 180^\circ.$

Take a triangle ABC, whose medians are AD, BE, and CF. The centroid M (the point where all three medians intersect) splits the medians such that $\overline{AM} = 2\overline{DM}.$

Given an isosceles triangle ABC such that $\overline{AB} = \overline{AC},$ the angle bisector, median, and altitude of point A to side BC are all the same line. This further implies that the centroid, orthocenter, and incenter of an equilateral triangle are all the same point. This can easily be proven by proving that all three of these lines create two congruent triangles using congruence criterion.

Given isosceles triangle ABC such that $\overline{AB} = \overline{AC},$ the perpendicular bisector of BC intersects A.

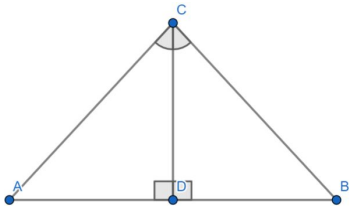
If two triangles have equal area and have two congruent angles, they are congruent.

If two chords of a circle intersect at one point on the circumference of that circle, then the angle it creates has half the measure of the arc it subtends.

Here are some examples:

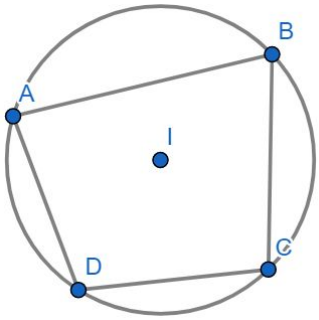
1. Prove that given triangle ABC, if cevian CD is an angle bisector and an altitude, then $\overline{AC} = \overline{BC}.$

Solution: Since CD is an angle bisector, $m\measuredangle ACD = m\measuredangle BCD,$ and since CD is an altitude, $m\measuredangle ADC = m\measuredangle BDC.$ By the ASA congruence criterion, $ADC \cong BDC,$ implying that $\overline{AC} = \overline{BC},$ which is what we desired.



2. Prove that in cyclic quadrilateral $ABCD,$ $m\measuredangle A + m\measuredangle C = m\measuredangle B + m\measuredangle D = 180^\circ.$

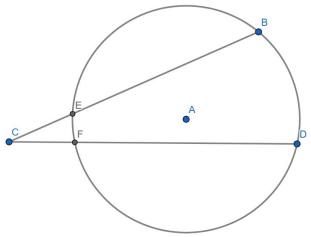
Solution: Have the measure of minor arc AB be denoted as $m(AB)$ and the measure of major arc AB be denoted as $M(AB).$ It should be obvious that $m(AB) + M(AB) = 360^\circ.$ Note that because the angle two chords that intersect at the circumference of a circle has half of the degree measure of the angle it subtends, that $m\measuredangle A + m\measuredangle C = \frac{1}{2}[m(BD) + M(BD)] = \frac{1}{2}(360) = 180.$ A similar argument may be applied for $m\measuredangle B + m\measuredangle D,$ which would complete our proof. (This part is left as an exercise for the reader. This is a fairly important concept in geometry -- this is the most recognizable feature of a cyclic quadrilateral.)



3. Prove that in cyclic quadrilateral $ABCD,$ that $m\measuredangle DAC = m\measuredangle DBC,$ $m\measuredangle CAD = m\measuredangle CBD,$ $m\measuredangle ABD = m\measuredangle ACD,$ and $m\measuredangle BAC = m\measuredangle BDC.$

Solution: Note that $\angle DAC$ and $\angle DBC$ subtend the same arc, so they have the same degree measure. This can be applied to the other three conditions, which is left as an exercise for the reader.

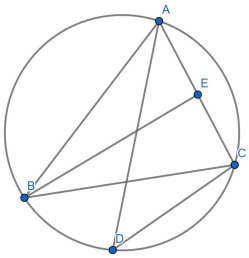
4. Prove that $m\measuredangle C = \frac{1}{2}m(BD) - \frac{1}{2}m(EF),$ where $m(AB)$ denotes the measure of minor arc $AB.$



Solution: Note $m\measuredangle CBF = \frac{1}{2}m(EF)$ and $m\measuredangle BFD = \frac{1}{2}m(BD).$ Then note that $m\measuredangle CFB + m\measuredangle BCF + m\measuredangle CBF = 180^\circ.$ Since $m\measuredangle CFB = 180 - m\measuredangle BFD,$ this becomes $\frac{1}{2}m(EF) + 180 - \frac{1}{2}m(BD) + m\measuredangle BCF = 180.$ Rearranging gives us $m\measuredangle BCF = \frac{1}{2}m(BD) + \frac{1}{2}m(EF),$ and we are done.

Here are some problems to do:

1. Given that A, B, C, and D are all on the circumference of the same circle, that BE is the angle bisector of BAC, that $m\measuredangle AEB = m\measuredangle CEB,$ and that $m\measuredangle ADC = 50^\circ,$ find $m\measuredangle BAC.$



2. Given points A, B, C, D, E such that BE is the angle bisector of ABC, $m\measuredangle AEB = m\measuredangle CEB,\ m\measuredangle BAC + m\measuredangle BDC = m\measuredangle ABD + m\measuredangle ACD,$ and $m\measuredangle ADC = 48^\circ,$ find $m\measuredangle BCA.$

3. Consider equilateral triangle $ABC.$ Have A' be the midpoint of $BC,$ B' be the midpoint of $BC,$ C' be the midpoint of $AC,$ and have the center of ABC be denoted as $I.$ Prove that any equilateral triangle DEF with center I and intersects the circumcircle of ABC six times satisfies the following: The chords formed by the sections of lines $DE,$ $DF,$ and EF that are contained within the circumcircle of ABC are bisected by lines $IA',$ $IB',$ and $IC',$ in no particular order.

4. Given that $m\measuredangle BAC = m\measuredangle BGC = 40^\circ,$ $m\measuredangle ABG = 80^\circ,$ $m\measuredangle GEC = 2m\measuredangle DBE,$ and $m\measuredangle DBE = m\measuredangle GEB,$ find $m\measuredangle ADB.$