Proofs

Now we'll talk about how to rigorously prove statements. previously we've justified things but now we will begin to actually prove things.

Terminology: Theorem - statement which can be shown to be true.

propositions - less important theorems.

proof - collection of statements which work from hypothesis to conclusion to justify theorem as true.

axiom - statements assumed to be true w/o proof. Usually these statements create your environment & are inherently unprovable

e.g. numbers exist, $0 < 1$, etc.

lemma - small result used to prove a larger result.

corrollary - theorem that can be proved as a result of another theorem.

E.g. Thm: Any number +1 is a number

$\square$

Corrollary: 3 is a number

Proofs are not given for corollaries, they follow from another theorem.

Conjecture: statement that is proposed as being true, in need of a proof.

Note; most math proofs are not worded like logical statements. often variables are used before being defined, if they're defined at all.

e.g. $x \cdot 0 = 0$, for every real number x.

Note: Occasionally we'll need to prove statements of the form $\forall x\,(P(x) \to Q(x))$ these proofs have the form $P(c) \to Q(c)$ where c is an arbitrary element from the domain.

Note arbitrary does not mean choose a random value, but instead means choose a variable c to be any element.

Note: when you read proofs (outside of this class) you will commonly find the words "clearly" & "obvious". These words mean the author expects the reader to fill in any breaks. You should avoid using those words in this class.

Methods:

Direct proofs - proving statements of the form $p \to q$ with a direct proof involve starting with assuming p to be true & then moving to subsequent steps eventually arriving at q being true.

Recall $p \to q$ has truth table

p	q	$p \to q$
T	T	T
T	F	F
F	T	T
F	F	T

We only need to demonstrate top row holds, Notice, we aren't saying anything about p & q exactly, just if p is true then q is.

e.g. Consider the proposition

If $2=1$ then $1+1=3$

pf Assuming $2=1$ then $1+1=1+2=3$ $\square$

Fact If n is even then there is an integer k s.t. $n=2k$.

If n is odd then $\exists$ k s.t. $n=2k+1$.

Ex: Give a direct proof of: For all integers m, n if m is odd & n is even then $m+n$ is odd.

pf: Note: this statement is $\forall m,n\ (P(m,n) \rightarrow Q(m,n))$. To prove this we just take a variable m, n satisfying the given conditions.

Assume m is an odd integer & n is an even integer.

Then $m=2k+1$ for some integer k. Similarly $n=2j$ (note not same k) for some integer j. Then

$$
\begin{aligned}
m+n &= 2k+1+2j \\
&= 2k+2j+1 \\
&= 2(k+j)+1 \\
&= 2p+1
\end{aligned}
$$

p an integer since k & j were. Thus $m+n$ is an odd integer. $\square$

$\square$ - is used to show the end of a proof, similar to writing Q.E.D but less pretentious. Often attributed to Halmos (famous mathematician)

Fact: A rational number is one that can be written as a fraction of integers,

e.g. $\frac{2}{3}$, $\frac{2}{1}$, $\frac{7}{1}$, $\frac{14}{13}$ etc.

π is not rational. it is irrational.

Example: prove if x & y are rational numbers then so is $x+y$.

pf: Assume x & y are rational numbers so $x = \frac{p}{q}$, $y = \frac{a}{b}$

for x, y, a, b integers.

Then $$x + y = \frac{p}{q} + \frac{a}{b}$$

$$= \frac{pb}{qb} + \frac{aq}{bq}$$

$$= \frac{pb + aq}{qb}$$

qb is an integer & so is $pb + aq$ so $x+y$ is rational. $\square$.

proof by contrapositive: Some statements are very difficult to prove directly. Possibly because the assumption seems unrelated to the conclusion, but more likely the hypothesis is hard to work with. to address this we use proof by contrapositive. Recall the contrapositive of $p \to q$ is $\neg q \to \neg p$. $\neg q \to \neg p$ is equivalent to $p \to q$

(meaning?)

Ex: prove if x^2 is irrational (not rational) then x is irrational

Pf: First try direct: - - - where to even start ?

However working with rational numbers is easy we prove the contrapositive

If x is rational then x^2 is rational.

Since x is rational $x = \frac{p}{q}$ for integers p, q. $q \neq 0$.

So $x^2 = \left(\frac{p}{q}\right)^2 = \frac{p}{q} \cdot \frac{p}{q} = \frac{p^2}{q^2}$ p^2, q^2 integers $q^2 \neq 0$

So x^2 is rational.

Thus if x^2 is irrational x is too. $\square$

Example: prove the statement: If x & y are integers & xy is odd then both x & y are too.

Pf: Direct is awkward, xy odd $\Rightarrow$ $xy = 2k+1$ some k

So $x = \frac{2k+1}{y}$ is that even or odd?

Easier to work backwards. We prove the contrapositive, if at least one of x & y are even then xy is even.

AWLOG (this means I'm gonna choose something specific, but not break generality, usually b/c of symmetry) x is even

Then $x = 2k$, $xy = 2ky = 2p$ p an integer

$\Rightarrow$ xy even.

$\square$

Note: Some propositions are <u>Vacuously true</u> recall $p \to q$ is true always when p is false. If we know it is then $p \to q$ is <u>Vacuously true</u>.

Some theorems ~~as stated~~ are Incorrect, there we must remember our negation rules.

<u>Ex</u>: Prove or disprove: For all real numbers x, y if x is rational & y is irrational then xy is irrational.

<u>Pf</u>: Seems valid, except for one case: $x = 0$ then $xy = 0$. This disproves our statement, the statement said $\forall x, y$ & we found a counter-example.

$\square$

To disprove an existential statement we need to show $\forall$. (more later).

<u>proof by Contradiction</u>: Heads up, this ones difficult to wrap your head around. It turns out $p \to q$ and $(p \wedge \neg q) \to (r \wedge \neg r)$ are logically equivalent. One says if p is true then q is. The other says, if p is true & q is false (making $p \wedge \neg q$ true) then $r \wedge \neg r$ is also true. But, we <u>know</u> $r \wedge \neg r$ is never true! Thus $p \wedge \neg q$ must be false $\Rightarrow$ If p is true then so is q

<u>Example</u>: If $x+y \geq 2$ then either $x \geq 1$ or $y \geq 1$

<u>pf</u>: Starting with $x+y \geq 2$ doesn't give any info on x or y.

So, lets use Contradiction: Suppose $x \geq 1$ or $y \geq 1$ is false

$\Rightarrow \neg(x \geq 1 \vee y \geq 1) \Rightarrow x < 1 \wedge y < 1$

Then $x+y < 1+1 < 2$. This is a contradiction,

We assumed $x+y \geq 2$ & showed $x+y < 2$.

Thus $x+y \geq 2 \Rightarrow$ either $x \geq 1$ or $y \geq 1$.

D.

<u>Note</u>: You assume the hypothesis & the negation of the Conclusion

The contradiction you get is often unknown ahead of time.

<u>Example</u>: prove $\sqrt{2}$ is irrational.

<u>pf</u>: There is no If _ then _ in this statement. We can think of this as If <u>standard math facts</u> then $\sqrt{2}$ is irrational!

Still gives us nowhere to go. Lets go for Contradiction!

Suppose $\sqrt{2}$ is rational then $\sqrt{2} = \frac{a}{b}$ for a, b integers $b \neq 0$. We can AWLOG $\frac{a}{b}$ is reduced (no common factors i.e. $\frac{2}{3}$, not $\frac{4}{6}$). Then $2 = \frac{a^2}{b^2}$ (Square both sides)

$\Rightarrow 2b^2 = a^2$. b^2 is an integer $\Rightarrow a^2$ is even. It is a fact that if a^2 is even then so is a (prove this yourself!)

Thus $a = 2c$ for some integer c. Thus $2b^2 = 4c^2$ dividing by 2:

$b^2 = 2c^2$ Thus b^2 is even $\Rightarrow$ b is even $\rightarrow\leftarrow$

We assumed $\frac{a}{b}$ is in lowest form no common factors, but a, b both multiples of 2. Thus $\sqrt{2}$ must be irrational.

$\square$.

Note: the contradiction here sort of came out of no where.

Note: Today is just day 1 of proofs we'll have more examples tomorrow.

Note: The examples from today should not be treated as obvious. Proving things is a lot of work. Very rarely do you start with just writing down the correct solution.

There is normally a lot of scratch work.

Especially with contradiction proofs. Todays examples is the equivalent of me saying "program this project, & here is the clean solution".

Next time: Examples & Induction.