Proofs

First some terminology:

A **theorem** is a mathematical statement that is known to be true.

An **axiom** (**postulate**) is an assumption accepted without proof.

A **proof** is a sequence of statements forming an argument that shows that a theorem is true.

A **lemma** is a short theorem used in the proof of another theorem.

A **corollary** is a theorem that is an immediate consequence of another theorem.

A **conjecture** is a mathematical statement whose truth value is still unknown (usually conjectures are statements that are thought to be true but hard to prove). Once proved (if it is indeed true), it becomes a theorem.

A **fallacy** is an incorrect reasoning.

Goldbach conjecture: Every positive even integer greater than or equal to 4 can be written as the sum of two prime numbers.

$4 = 2+2$
$6 = 3+3$
$8 = 3+5$
$10 = 3+7$
$12 = 5+7$
$14 = 7+7$
$16 = 5+11$
$18 = 7+11$

Some common fallacies:

Fallacy of affirming the conclusion:

$p \to q$

$\underline{q \qquad}$

$\therefore p$

This is an invalid argument. (Make a truth table to see this.)

p	q	$p \to q$
$\boxed{T}$	T	T
T	F	F
$\boxed{F}$	T	T
F	F	T

Fallacy of denying the hypothesis:

$p \to q$
$\underline{\neg p \qquad}$
$\therefore \neg q$

This is an invalid argument. (Make a truth table to see this.)

p	q	$\neg p$	$\neg q$	$p \to q$
T	T	F	F	T
T	F	F	T	F
F	T	T	$\boxed{F}$	T
F	F	T	$\boxed{T}$	T

In Row 3 and Row 4 all premises are true. However, Row 3 has $\neg q$ F, so $\neg q$ does not follow from the premises.

Begging the question (**circular reasoning**):

This is when C is being used to actually prove C.

Type of Proof	Proposition to Prove	Strategy
Direct proof	$p \to q$	assume p show that q follows (using p)
Indirect proof (proof by contraposition)	$\neg q \to \neg p$	assume $\neg q$ show that $\neg p$ follows (using $\neg q$)
Proof by contradiction	prove a statement p	assume $\neg p$ show contradiction follows
Proof by cases	$(p_1 \vee p_2 \vee \ldots \vee p_k) \to q$	prove each of $p_1 \to q$, $p_2 \to q$ … $p_k \to q$
Proof of an equivalence	$p \leftrightarrow q$	prove $p \to q$ <u>and</u> $q \to p$
Vacuous proof	$p \to q$ (where p is F)	prove p is F (if it indeed is) then $p \to q$ is T vacuously
Trivial proof	$p \to q$ (where q is T)	prove q is T (if it indeed is) then $p \to q$ is T trivially

Examples of Proofs and some definitions:

Definition: An integer n is called **odd** if $n = 2k + 1$ for some integer k, and is called **even** if $n = 2m$ for some integer m.

Theorem: If $\overbrace{n \text{ is an odd integer}}^{p}$, then $\overbrace{n^2 \text{ is an odd integer}}^{q}$.

Proof (*direct proof*): Suppose n is an odd integer.
Then, $n = 2k+1$ for some $k \in \mathbb{Z}$.
↳ set of integers
Taking the square of both sides, we get
$$n^2 = (2k+1)^2 = (2k+1)(2k+1) = 4k^2+2k+2k+1 = 4k^2+4k+1.$$
$$= 2\underbrace{(2k^2+2k)}_{m \in \mathbb{Z}}+1$$
$$= 2m+1$$
So, n^2 can be expressed $\underset{(m \in \mathbb{Z})}{2m+1}$. Therefore, n^2 is odd.

Theorem: If $\underbrace{3n + 2 \text{ is an odd integer}}_{p}$, then $\underbrace{n \text{ is an odd integer}}_{q}$.

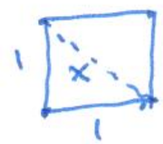
Proof (*proof by contraposition*):
(suppose $\neg q$) Suppose n is not an odd integer. So we suppose that n is an even integer.
Then $n = 2m$ for some $m \in \mathbb{Z}$.
↳ "an element of".
$$n = 2m \overset{/\cdot 3}{\Rightarrow} 3n = 6m$$
Then $3n = 6m \underset{/+2}{\Rightarrow} 3n+2 = 6m+2$.
So, $3n+2 = 6m+2 = 2 \cdot \underbrace{(3m+1)}_{r \in \mathbb{Z}}$.

So $3n+2 = 2 \cdot r$, and hence by definition $3n+2$ is an even integer $(\neg p)$, which completes the proof!

Definition: Let m and n be ~~positive~~ integers. If $n = km$ for some positive integer k, then we say that

n is a **multiple** of m;
m is a **divisor** of n (m **divides** n).
We write $\mathbf{m|n}$ (read: "m divides n").

$m|n$ $\boxed{\ne \frac{m}{n} \text{ Not the same thing}}$



$x = \sqrt{1^2+1^2}$
$x = \sqrt{2}$

Definition: A real number r is called **rational** if $r = \dfrac{p}{q}$ for some integers p and q with $q \neq 0$. A real number that is not rational is called **irrational**. 0.75 is rational $0.75 = \frac{3}{4}$
π is irrational

Theorem: $\underbrace{\sqrt{2} \text{ is irrational.}}_{P}$

Proof (*proof by contradiction*): Suppose that $\sqrt{2}$ is not irrational; so we suppose that $\sqrt{2}$ is rational. So, by the definition of rational numbers $\sqrt{2} = \frac{p}{q}$ $(q \neq 0)$. (Let $\frac{p}{q}$ be the most simplified fraction among all that are equal to $\sqrt{2}$.) $\sqrt{2} = \frac{p}{q}$. Taking the square of both sides, we get $2 = \frac{p^2}{q^2}$.

$2 = \frac{p^2}{q^2} \Rightarrow 2 \cdot q^2 = p^2$ Since $p^2 = 2 \cdot \underbrace{q^2}_{m \in \mathbb{Z}}$, p^2 is even.

Then p must be even. So $p = 2r$ for some $r \in \mathbb{Z}$.

Then from $p^2 = 2 \cdot q^2$, we get $(2r)^2 = 2 \cdot q^2$
$\Rightarrow 4r^2 = 2 \cdot q^2 \Rightarrow 2r^2 = q^2$

so q^2 is even. Then q is even, and so $q = 2s$ for $s \in \mathbb{Z}$.

We obtain $p = 2r$ and $q = 2s$, so $\frac{p}{q} = \frac{2r}{2s}$, which contradicts our supposition that $\frac{p}{q}$ is in the most simplified form. This completes the proof.
We conclude that $\sqrt{2}$ is irrational.

$n = 2k+1 \quad k \in \mathbb{Z}$

Case 1: k is odd, so $k = 2r+1$ for some $r \in \mathbb{Z}$.

Then $n = 2\cdot(2r+1)+1 = 4r+3$

case 2: k is even, so $k = 2t$ for some $t \in \mathbb{Z}$.

Then, $n = 2\cdot(2t)+1 = 4t+1$

Theorem: The square of any odd integer has the form $8m+1$ for some integer m.

Proof (*proof by cases*): Let n be an odd integer.
So, $n = 2k+1$ for some $k \in \mathbb{Z}$.
We consider 2 cases depending on the parity of k:

Case 1: (if k is odd) $n = 4r+3$ for some $r \in \mathbb{Z}$.

Then $n^2 = (4r+3)^2 = (4r+3)(4r+3)$

$= 16r^2+12r+12r+9$

$= 16r^2+24r+9 = 16r^2+24r+8+1 = 8(\underbrace{2r^2+3r+1}_{m \in \mathbb{Z}})+1.$

Case 2: (if k is even) $n = 4t+1$ for some $t \in \mathbb{Z}$.

Then $n^2 = (4t+1)^2 = (4t+1)(4t+1) = 16t^2+4t+4t+1$

$= 16t^2+8t+1 = 8(\underbrace{2t^2+t}_{m \in \mathbb{Z}})+1.$

We showed that in both cases n^2 can be written as $8m+1$ for some $m \in \mathbb{Z}$, which finishes the proof.

an attempt with a direct proof approach: Let n be an odd integer.

Then, $n = 2k+1$ for $k \in \mathbb{Z}$.

Then, $n^2 = (2k+1)^2 = 4k^2+4k+1$

We want to show that

$n^2 = 8m+1$ for some $m \in \mathbb{Z}$.

We don't know how.

So, maybe we try another approach.

Theorem: Let m and n be positive integers. Then $\overbrace{m = n}^{p}$ if and only if $\underbrace{m|n \text{ and } n|m}_{q}$.

Proof (*proof of equivalence*): To prove $p \iff q$, we need to prove i) $p \Rightarrow q$ and ii) $q \Rightarrow p$.

i) ($p \Rightarrow q$): Suppose $m = n$ ($m, n \in \mathbb{Z}^+$).

Since $m = n$, we have $m \cdot 1 = n$. So $m|n$.

Similarly $m = n$, we have $m = n \cdot 1$. So $n|m$.

This completes the proof of i).

ii) ($q \Rightarrow p$): Suppose that $m|n$ and $n|m$ where $n, m \in \mathbb{Z}^+$. Since $m|n$, we have $n = k_1 m$ ($k_1 \in \mathbb{Z}^+$). (I)

Since $n|m$, we have $m = k_2 n$ ($k_2 \in \mathbb{Z}^+$) (II)

substitute

Then $m = k_2 k_1 m$, (where $k_2, k_1 \in \mathbb{Z}^+$)

$\Rightarrow k_2 \cdot k_1 = 1$

So $k_2 = 1$, $k_1 = 1$.

Then, from (I) we get $n = 1 \cdot m$.

So, $n = m$.

This finishes the proof of ii).

By parts i) & ii), we have completed the proof.

Theorem: If $0 > 1$, then 3 is an even number.

Proof (*vacuous proof*):

Theorem: If $0 < 1$, then $\sqrt{4}$ is a rational number.

Proof (*trivial proof*):