Methods of Proof

In math and computer science, it is not just enough to *find* the correct answer, we need to *prove* we have the correct answer.
What do we mean by proof? The root word "probare" is Latin, it means "to test".

For Mathematicians, "proof" means something much more rigorous, and a proof has two essential features:

1. It must be finitely long so you can give it to someone else
2. It must be possible for someone else to check the proof for correctness without needing brilliant flashes of insight

Thus, to prove something you first need a formal system of axioms and inference rules, and a "proof" of some statement A is some sequence of inference rules from the axioms to the statement A.
Example:
Axioms:
A1 "Tim is teaching 2321"
A2 "If Tim is teaching 2321 then 2321 is fun"

Inference Rules:
$$\frac{X, X \Rightarrow Y}{Y}$$

Proof that 2321 is fun
By A1, "Tim is teaching 2321"
By A2, "If Tim is teaching 2321 then 2321 is fun"
Therefore, by the inference rule *modus ponens*, "2321 is fun"

For most math and computer science, this level of formalism/tedium is not needed, and proofs are instead informal things where the axioms and inference rules are not stated. As you read an informal proof, you can infer what axioms and inference rules are being used and decide in the moment if you accept or object to it.

One of our goals for this class is to get you comfortable with proofs, so you can handle reading and writing the more complex proofs you will see in CSE 2331, Math 3345, and other classes.
There are 3 main methods of proof we will rely on: **Direct Proof**, **Proof by Induction**, and **Proof by Contradiction**.

Direct Proof

A direct proof should follow these style and format guidelines:

State the statement you want to prove.

Proof.
Each line should be a statement or declaration.
Each statement should be true.
The truth of each statement should be clear from a definition, axiom, lemma, theorem, the previous line, or some combination.
Provide a short and precise explanation/justification when needed.
Conclusion should mirror the statement we are proving.

□

Example 1 of a direct proof:

The square of an odd number is odd.

Proof.
Let n be an odd integer.
Then there exists $k \in \mathbb{Z}$ such that $n = 2k + 1$.
Therefore,

$$\begin{aligned} n^2 &= (2k+1)^2 \\ &= (2k+1)(2k+1) \\ &= 4k^2 + 4k + 1 \\ &= 2(2k^2 + 2k) + 1 \end{aligned}$$

Since $k \in \mathbb{Z}$, we have that $2k^2 + 2k \in \mathbb{Z}$.
So $2(2k^2 + 2k) + 1$ is odd.
So n^2 is odd.
Therefore, the square of an odd integer is also odd. □

Example 2 of a direct proof:

Let $a, b, c \in \mathbb{N}$. If $a > c$ and $b > c$ then $\max\{a, b\} - c > 0$.

Proof.
Let $a, b, c \in \mathbb{N}$ such that $a > c$ and $b > c$.
We will consider two cases:
Case 1: $\max\{a, b\} = a$.
Since $a > c$, we have $a - c > 0$.
So $\max\{a, b\} - c = a - c > 0$.
Case 2: $\max\{a, b\} = b$.
Since $b > c$, we have $b - c > 0$.
So $\max\{a, b\} - c = b - c > 0$.
Therefore, by cases 1 & 2, we have that $\max\{a, b\} - c > 0$. □

Proof By Induction

Proof by induction is a very popular and powerful technique, especially when you want to prove a statement like $\forall n \in \mathbb{N}, f(n)$ where $f(n)$ is some function.

People often initially find proof by induction confusing, if you don't pay close attention while reading an induction prove it can look like nothing was proven at all, and it is easy to make a mistake while writing an induction proof.

But once you understand them, induction proofs are simple and elegant.

A proof by induction should follow these style and format guidelines:

State the statement you want to prove, typically a statement like $\forall n \in \mathbb{N}, f(n)$.

Proof by Induction.
Base Case:
Compute $f(n)$ directly for the base case, the smallest value of n, typically $n = 0$ or $n = 1$.
Induction Step:
Assume the statement is true for an arbitrary value n.
Prove the statement is true for $n + 1$.
In other words, we prove here that $f(n) \Rightarrow f(n + 1)$.
Conclusion:
State what you have proven. □

Why does this work? I like to use the analogy of a ladder.

For you to climb a ladder, all you need to know are two things:
(1) How to get on the ladder
(2) How to get from one rung of the ladder to the next
Once you know these two things, you can climb a ladder that is 10 rungs, 100 rungs, 10^{10} rungs, it doesn't matter.

The base case is like getting on to the ladder, and the induction step is like climbing from one rung to the next.

My base case tells me it is true for $n = 0$, so my induction step tells me it is true for $n = 1$ (using modus ponens).

Since I know it is true for $n = 1$, my induction step tells me it is true for $n = 2$ (modus ponens again).

Since I know it is true for $n = 2$, my induction step tells me it is true for $n = 3$ (modus ponens again).

Since I know it is true for $n = 3$, my induction step tells me it is true for $n = 4$ (modus ponens again).
...

Example 1 of an induction proof (weak induction):
For all $n \geq 1$,

$$\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$$

Proof by Induction.
Base Case:
Let $n = 1$, then we have

$$\begin{aligned}
\sum_{i=1}^{n} i &= \sum_{i=1}^{1} i \\
&= 1 \\
&= \frac{1}{1} \\
&= \frac{2}{2} \\
&= \frac{1(1+1)}{2} \\
&= \frac{n(n+1)}{2}
\end{aligned}$$

Induction Step:

Let n be an arbitrary value, assume that

$$\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$$

Then

$$\sum_{i=1}^{n+1} i = 1 + 2 + 3 + ... + n + (n+1) = \sum_{i=1}^{n} i + (n+1)$$

Applying the assumption, we have

$$\begin{aligned}
\sum_{i=1}^{n+1} i &= \frac{n(n+1)}{2} + (n+1) \\
&= \frac{n(n+1)}{2} + \frac{2(n+1)}{2} \\
&= \frac{n(n+1) + 2(n+1)}{2} \\
&= \frac{n^2 + n + 2n + 2}{2} \\
&= \frac{n^2 + 3n + 2}{2} \\
&= \frac{(n+1)(n+2)}{2}
\end{aligned}$$

Conclusion:
Therefore, for all $n \geq 1$ we have that $\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$. □

Example 2 of an induction proof (strong induction):

This is a tougher proof, so I include here some commentary in red. Those parts are not a part of the proof, just extra explanation.

The reason this is strong induction and the one before was weak induction is because of the difference in the assumption we make in the induction step.

Theorem 0.1. *Let $G = (V, E)$ be an undirected graph. We say a graph is connected if every pair of vertices is connected by a path.*
If G is connected then $|E| \geq |V| - 1$.

Proof by Induction.
Base Case:
Let $G = (V, E)$ be a graph with $|V| = 0$.
In such a graph $|E| = 0 \geq -1 = 0 - 1 = |V| - 1$.

Induction Step:
Let n be an arbitrary integer ≥ 0.
Assume that all connected graphs $G = (V, E)$ with $|V| \leq n$ vertices have that $|E| \geq |V| - 1$.

Our goal in the induction step is to prove that all connected graphs with $n+1$ vertices have at least n edges.

Let $G' = (V', E')$ be a connected graph with $|V'| = n + 1$.

Case 1: $|V'| = 1$.

Then since we do not allow self loops $|E'| = 0 \geq |V'| - 1$.

Case 2: $|V'| \geq 2$.

Since G' is connected and $|V'| \geq 2$, each vertex must have degree at least 1.

Let u be an arbitrary vertex selected from V'.

Let $G'' = (V'', E'')$, where

$$V'' = V' \setminus \{u\}$$

and

$$E'' = \{\{x, y\} \in E' : x \neq u \wedge y \neq u\}.$$

What we have done here is created a new graph G'' from G' by "deleting" the vertex u.

Let $C_1, C_2, \ldots, C_k$ be the connected components of G'', and $C_i = (V_i, E_i)$ for all $i \in \{1, 2, \ldots, k\}$.
When we deleted the vertex u, we may or may not have split the graph into several parts. We will call these parts $C_1, C_2, \ldots, C_k$, and treat them like graphs.

For all $i \in \{1, 2, \ldots, k\}$, $|V_i| \leq n$.
This is clear, since G'' has n vertices the connected components cannot have more than n vertices.

$C_1, C_2, \ldots, C_k$ are connected graphs, each on at most n vertices, so we can apply the assumption we made at the start.
Therefore, for each $i \in \{1, 2, \ldots, k\}$, we have that $|E_i| \geq |V_i| - 1$.
We will use the observation that $|E_i| \geq |V_i| - 1$ later. The next few lines are unrelated.

G' is a connected graph, and so there is a path connecting all pairs of vertices.

In particular, for all $v \in V'$, there is a path connecting u and v.

Therefore, for all $i \in \{1, 2, \ldots, k\}$, for all $v_i \in V_i$, there is a path in G' from u to v_i.

So u must have at least one edge corresponding to each connected component.

So $\deg(u) \geq k$.
The last five lines are just a formal way of observing that, since G' broke into k connected components when we deleted u, there must be at least k edges

that were deleted because they were connected to u.

Therefore,

$$\begin{aligned}
|E'| &= |E''| + \deg(u) && \text{(By the construction of } G'') \\
&= \sum_{i=1}^{k} |E_i| + \deg(u) && \text{(Edges not deleted are in a conn. comp.)} \\
&\geq \sum_{i=1}^{k} |E_i| + k && \text{(Established earlier)} \\
&\geq \sum_{i=1}^{k} (|V_i| - 1) + k && \text{(Established earlier)} \\
&= \sum_{i=1}^{k} |V_i| - \sum_{i=1}^{k} 1 + k \\
&= \sum_{i=1}^{k} |V_i| \\
&= n
\end{aligned}$$

So we have that $|E'| \geq n = |V'| - 1$.
Conclusion:
For any connected graph $G = (V, E)$, we have that $|E| \geq |V| - 1$. □

Proof By Contradiction

Proof by contradiction is possibly the most popular proof technique.

It works by using the observation that $A \vee \neg A$ is a tautology; if I can prove $\neg A$ is false then I have proven A is true.

A proof by contradiction will assume the negation of the statement we actually want to prove, adding it to our set of axioms.

Then use that to prove something obviously false (a contradiction, like $1 = 2$). Since we (generally) believe that the axioms and inference rules of mathematics are correct, the contradiction must be coming from the axiom we added.

A proof by contradiction should follow these style and format guidelines:

State the statement you want to prove.

Proof by Contradiction.
Assume ¬(statement you want to prove).
Find something "obviously false" that would be true as a consequence of that assumption.
$\rightarrow\leftarrow$
State the negation of your assumption. □

Proof by Contradiction Example 1:
$\sqrt{2}$ is irrational.

Proof by Contradiction.
Assume $\sqrt{2}$ is rational.
So there exists $p, q \in \mathbb{N}$ such that $\sqrt{2} = \frac{p}{q}$ and $\gcd(p, q) = 1$.
So we have that $2 = \frac{p^2}{q^2}$, and so $2q^2 = p^2$.
Therefore, p must be even, i.e. there exists $a \in \mathbb{N}$ such that $p = 2a$.
So $2q^2 = (2a)^2 = 4a^2$.
So $q^2 = 2a^2$, and therefore q must be even.
Since p and q are both even, $\gcd(p, q) = 2$.
Therefore, $1 = gcd(p, q) = 2$.
$1 = 2$.
$\rightarrow\leftarrow$
So our assumption must be false, and therefore $\sqrt{2}$ is irrational. $\square$

Proof by Contradiction Example 2:
The set of prime numbers is infinite.

Proof by Contradiction.
Assume the set of prime numbers is finite.
Let $P = \{p_1, p_2, \ldots, p_k\}$ be the set of prime numbers.
Let $n = p_1 \cdot p_2 \cdot \ldots \cdot p_k + 1$.
Clearly $n > p_i$ for all $i \in \{1, 2, \ldots, k\}$, so $n \notin P$.
So n is a composite number.
Since n is composite, there exists $q \in P$ and $a \in \mathbb{N}$ such that $n = q \cdot a$ and $a \neq 1$.
So $q \cdot a = n = p_1 \cdot p_2 \cdot \ldots \cdot p_k + 1$.
So $a = \frac{p_1 \cdot p_2 \cdot \ldots \cdot p_k + 1}{q}$.
But $q \in P$, so $q = p_i$.
So

$$a = \frac{p_1 \cdot p_2 \cdot \ldots \cdot p_k + 1}{q} = \frac{p_1 \cdot p_2 \cdot \ldots \cdot p_k + 1}{p_i} = p_1 \cdot \ldots \cdot p_{i-1} \cdot p_{i+1} \cdot \ldots \cdot p_k + \frac{1}{p_i}$$

$p_1 \cdot \ldots \cdot p_{i-1} \cdot p_{i+1} \cdot \ldots \cdot p_k \in \mathbb{N}$ but since 1 is not a prime we have $0 < \frac{1}{p_1} < 1$.
So $a \notin \mathbb{N}$.
$\rightarrow\leftarrow$
So our assumption must be false, and therefore the set of prime numbers is infinite. $\square$