Direct Proofs

Prove the Pythagorean Theorem.
While a picture is not usually a proof, drawing the problem often helps.

We can construct this square via geometric tools and obtain its area without “cheating”, so let’s calculate it two different ways. In whole, the area is \((a+b)^2 = a^2 + 2ab + b^2\).
Piece by piece, the area is \(4\left(\frac{1}{2}ab\right) + c^2 = c^2 + 2ab\).
Equating these yields the result, \(a^2 + b^2 = c^2\).

Contradiction Proofs

Prove there are infinitely many primes.
Suppose not.
Then there are finitely many primes.
Let them be \(p_1, \ldots, p_n\), and consider \(p_1p_2 \ldots p_n + 1\).
For each \(p_i\), clearly \(p_1p_2 \ldots p_n + 1 \equiv 1 \mod p_i\), so \(p_i \mid p_1p_2 \ldots p_n + 1\). But if no prime divides \(p_1p_2 \ldots p_n + 1\), then \(p_1p_2 \ldots p_n + 1\) must be prime.
This is a contradiction since we assumed only \(p_1, \ldots, p_n\) are prime, so our assumption must have been wrong.
Thus there are infinitely many primes.
Constructive Proofs (Existence Proofs)

Prove \( \exists n \in \mathbb{N} : n \) is equal to the sum of its proper divisors.

The proper divisors of 6 are 1, 2, and 3, which sum to 6. \( \Box \)

Nonconstructive Proofs

Prove that there exists two irrational numbers \( a, b \) such that \( a^b \in \mathbb{Q} \).

First note that \( \sqrt{2} \notin \mathbb{Q} \). Then either \( \sqrt{2} \sqrt{2} \in \mathbb{Q} \) or \( (\sqrt{2} \sqrt{2})^2 = \sqrt{2}^2 = 2 \notin \mathbb{Q} \). So at least one of

\[
\begin{align*}
    a &= \sqrt{2} \\
    b &= \sqrt{2}
\end{align*}
\]

satisfies the statement, though which is not clear. \( \Box \)

Counterexample Proofs

\( \neg \)existence proof

Let's consider every sum of two primes and find something we miss.

\[
\begin{align*}
2 + 2 &= 4 & 3 + 3 &= 6 & 5 + 5 &= 10 \\
2 + 3 &= 5 & 3 + 5 &= 8 & 5 + 7 &= 12 \\
2 + 5 &= 7 & 3 + 7 &= 10 & 7 + 7 &= 14 \\
2 + 7 &= 9 & 3 + 11 &= 14 & 2 + 11 &= 13
\end{align*}
\]

Since all other primes are at least 11 and thus cannot contribute to a sum of 11, 11 is not the sum of two primes. \( \Box \)
Contrapositive Proof / Exhaustion Proof (proof by cases)

Prove that if \( n \equiv 2 \text{ or } 3 \mod 4 \), then \( n \) is not a perfect square.

We will prove the contrapositive.

Let \( n = k^2 \), where \( k \in \mathbb{N} \). There are four cases to consider.

**Case 1:** \( k \equiv 0 \mod 4 \)

Then \( k = 4m \) for some \( m \in \mathbb{N} \).

\[ n = k^2 = (4m)^2 = 16m^2 \equiv 0 \mod 4 \]

**Case 2:** \( k \equiv 1 \mod 4 \)

Then \( k = 4m + 1 \) for some \( m \in \mathbb{N} \).

\[ n = k^2 = (4m+1)^2 = 16m^2 + 8m + 1 \equiv 4(4m^2 + 2m + 1) \equiv 1 \mod 4 \]

**Case 3:** \( k \equiv 2 \mod 4 \)

Then \( k = 4m + 2 \) for some \( m \in \mathbb{N} \).

\[ n = k^2 = (4m+2)^2 = 16m^2 + 16m + 4 \equiv 4(4m^2 + 4m + 1) \equiv 0 \mod 4 \]

**Case 4:** \( k \equiv 3 \mod 4 \)

Then \( k = 4m + 3 \) for some \( m \in \mathbb{N} \).

\[ n = k^2 = (4m+3)^2 = 16m^2 + 24m + 9 \equiv 4(4m^2 + 6m + 2) + 1 \equiv 1 \mod 4 \]

In each case, we have when \( n \) is a perfect square, \( n \not\equiv 2 \text{ or } 3 \mod 4 \), so we're done.
Pigeonhole Proofs

A drawer contains a mix of blue and black socks. What is the minimum number of socks you must withdraw to ensure you have at least two of a single color.

By the pigeonhole principle, 3. We can put at most $n$ things into $n$ different bins so that no bin contains more than one thing. In this case, $n = 3$, things are socks, and bins are colors.

\[ \square \]

Infinite Descent Proof

Prove there is no smallest positive rational number.

Suppose $r \in \mathbb{Q}^+$ is the smallest positive rational number. But $\frac{r}{2} \in \mathbb{Q}^+$, and $\frac{r}{2} < r$.

This is a contradiction, thus no such $r$ exists.

\[ \square \]
Induction is a proof technique used for proving a statement \( P(n) \) is true for every natural number \( n \) when no more direct proof is available. It is somewhat similar to climbing an infinity ladder. You can get on anywhere, and you can climb rungs one, two, four, \( 2^k \), etc at a time. to get to wherever you need to be.

At its most basic, induction follows this formula. Let \( P : \mathbb{N} \rightarrow \mathbb{P} \) be a statement. Then it follows that \( \forall n \in \mathbb{N}, P(n) \) if \( P(0) \) and \( P(n) \Rightarrow P(n+1) \).

To see why this is true, we need a useful fact.

The Well Ordering Principle

Every subset of \( \mathbb{N} \) has a least element.

Now we can show induction works.

Suppose \( P(0) \) and \( P(n) \Rightarrow P(n+1) \).

Now assume \( P(n) \) is not true for all \( n \in \mathbb{N} \), and let \( \mathbb{N} \subseteq \mathbb{N} \) be the set of naturals where \( \lnot P \). Note \( \varnothing \notin \mathbb{N} \).

By the well ordering principle, there is a least \( n+1 \in \mathbb{N} \) such that \( \lnot P(n+1) \). But then \( P(n) \) and \( P(n) \Rightarrow P(n+1) \), so \( n+1 \notin \mathbb{N} \).

Therefore it must be the case that \( \mathbb{N} \neq \varnothing \).
Prove \[ \sum_{i=1}^{n} i = \frac{n(n+1)}{2}. \]

Our \( P(n) \) statement is \( P(n) := \sum_{i=0}^{n} i = \frac{n(n+1)}{2}. \)

We will show \( \forall n \in \mathbb{N}, P(n) \) via induction.

To prove \( P(0) \), observe that \[ \sum_{i=0}^{0} i = 0 = \frac{0(0+1)}{2}. \]

Now assume that \( P(n) \) is true. Let \( n+1 \in \mathbb{N} \). Then

\[ \sum_{i=0}^{n+1} i = \sum_{i=0}^{n} i + (n+1) = \frac{n(n+1)}{2} + n + 1 = \frac{(n+1)(n+2)}{2}. \]

Thus \( P(n+1) \), so \( P(n) \Rightarrow P(n+1) \). \( \square \)

Induction generalizes very easily. So long as you can describe a "ladder" and can get to every rung (or every rung of interest), then you're good.

Prove every tree has one more vertex than edge, i.e. \( |V| = |E| + 1 \).

Define \( P(n) := \) Every Tree with \( n \) vertices satisfies \( |V| = |E| + 1 \).

We will prove \( \forall n \in \mathbb{N}, P(n) \) via induction. (\( 0 \notin \mathbb{N} \) here).

To show \( P(1) \), there is only one tree with 1 vertex. It has no edges, so \( 1 = 0 + 1 \).

Now assume \( P(n) \). Let \( T = (V,E) \) be a tree with \( |V| = n+1 \geq 2 \). Since \( T \) is acyclic and connected, it must have a leaf with a single neighbor. Remove this vertex and its only edge to get \( T' = (V',E') \) with \( |V'| = n \). Then \( T' \) is a tree with \( n \) vertices, and since \( P(n) \), \( |V'| = |E'| + 1 \).

But \( |V'| = |V| - 1 \) and \( |E'| = |E| - 1 \), so \( |V| - 1 = |E| - 1 + 1 \), or \( |V| = |E| + 1 \). \( \square \)
Prove that the distance from the origin at any \((a/b)\in \mathbb{N}^2\) is at most the taxicab distance.

While this is fairly easy to prove otherwise, we will use induction. Define 
\[ P(n,m) := \sqrt{n^2 + m^2} \leq n + m. \]
For \( P(0,0) \), clearly \( \sqrt{0^2 + 0^2} = 0 \leq 0 + 0 = 101 + 101 \). 

To cover all of the “rungs”, we need to be able to get to any \((n,m)\). We’ll do this with two implications.

\[ P(n,m) \Rightarrow P(n+1,m) \]
Assume \( \sqrt{n^2 + m^2} \leq n + m \).

Since distance is a metric,
\[ \sqrt{(n+1)^2 + m^2} \leq \sqrt{n^2 + m^2} + 1 \]
\[ \leq n + m + 1 \]
\[ = (n+1) + m. \]

\[ P(n,m) \Rightarrow P(n,m+1) \]
Follows similarly to the previous case.

Thus by induction, \( \forall n, m \in \mathbb{N}, P(n,m) \).

Prove that any \( n \in \mathbb{N} \) at least 8 is the sum of 3’s and 5’s.

We will first prove \( P(8) \), \( P(9) \), and \( P(10) \).
\[ 8 = 3 + 5 \quad 9 = 3 + 3 + 3 \quad 10 = 5 + 5 \]

Now assume \( n \in \mathbb{N} \) at least 8 is the sum of 3’s and 5’s. 

Then \( n = 3a + 5b \) for some \( a, b \in \mathbb{N} \).

Now for \( n + 3 \), we have \( n + 3 = 3a + 5b + 3 = 3(a+1) + 5b \).
Sometimes we need more power. Induction shows that everything between the base case and \( n \) in the inductive step must be true, so we can assume that. In other words, if \( P(n) \) is a statement, \( P(0) \), and \( \forall k \leq n, P(k) \Rightarrow P(n+1) \), then \( \forall n \in \mathbb{N}, P(n) \). We call this **strong induction**.

Our previous proof, we could have instead done the following with the same base case. Assume \( \forall 8 \leq k \leq n, k = 3a_k + 5b_k \) for some \( a_k, b_k \in \mathbb{N} \).

For \( n+1 \ (n \geq 10) \),

\[
  n+1 = (n-2) + 3 = 3a_{n-2} + 5b_{n-2} + 3 = 3(a_{n-2} + 1) + 5b_{n-2}.
\]

\[ \square \]

Other interesting induction choices include:

- \( P(0), \ P(n) \Rightarrow P(2n) \land P(2n+1) \).

- \( \forall k \in \mathbb{N}, P(2^k) \land P(n) \Rightarrow P(n-1) \).

- \( P(0) \land P(n) \Rightarrow P(2n) \land P(n-1) \).

- \( P([0,1]) \land P([n,n+1]) \Rightarrow P([n+1,n+2]) \).
There is a variant of induction we use to make life easier on us. If we have a recursively defined structure, we can induct on the number of recursions. (As an aside, we can also do this on recursive algorithms.) This is called structural induction.

A graph $G = (V, E)$ of vertices $V$ and edges $E$ connecting vertices can be recursively defined as follows:

- $G = (\emptyset, \emptyset)$
- $G = (V \cup \{u\}, E)$, where $E$ contains no edges incident on $u$ and $u \not\in V$.
- $G = (V, E \cup \{e\})$, where $e \not\in E$.

Prove that for any graph $G = (V, E)$, $2 \left\lfloor \sum_{u \in V} \text{deg}(u) \right\rfloor$ (i.e., the sum of the degrees of odd degree vertices is even)

We will prove this via structural induction. For the base case when $G = (\emptyset, \emptyset)$, $|\emptyset| = 1 = 10 + 1 = 101 + 1$.

Now assume that any graph constructed via $n$ applications of the recursive definition satisfies the hypothesis.

Let $G = (V, E)$ be a graph constructed via $n+1$ applications of the recursive definition.

If $E = \emptyset$, then remove any vertex $u$ from $V$ to get $V'$. By assumption, $(V', E)$ satisfies the hypothesis. Since $u$ has no edges incident upon it, it follows that $G$ does as well.

If $E \neq \emptyset$, then remove an edge $(u, v)$ from $E$ to get $E'$. Then $(V, E')$ satisfies $2 \left\lfloor \sum_{u \in V} \text{deg}(u) \right\rfloor$. We only need now to consider what $(u, v)$ does to $u$ and $v$ to get from $(V, E')$ to $G$.
The edge \((u,v)\) adds 1 degree to \(u\) and \(v\).

There are four cases.

1. \(2 \cdot \text{deg}(u) \land 2 \cdot \text{deg}(v)\)

   Adding \((u,v)\) to the graph makes \(\text{deg}(u)\) odd and \(\text{deg}(v)\) odd, so the sum \(\sum_{a \in V} \text{deg}(a)\) increases by an even amount.

2. \(2 \cdot \text{deg}(u) \land 2 \cdot \text{deg}(v)\)

   Adding \((u,v)\) to the graph swaps the parity of \(u\) and \(v\), hence the sum \(\sum_{a \in V} \text{deg}(a)\) remains even.

3. \(2 \cdot \text{deg}(u) \land 2 \cdot \text{deg}(v)\)

   Similarly to the previous case.

4. \(2 \cdot \text{deg}(u) \land 2 \cdot \text{deg}(v)\)

   Similarly to the first case, but the sum decreases by an even amount.

\[ \square \]