Proofs

Counterexample

To prove something is true, generally you must do so for all possible values. To prove something is false you only need one example where it doesn't work.

1) For all a, b, it is true that $a^2 + b^2 = (a + b)^2$

Direct Proof:

To prove $P \Rightarrow Q$, we consider an element x for which $P(x)$ is true and show $Q(x)$ is also true.

2) If n is an odd integer then $3n + 7$ is an even integer.

Proof by Contrapositive:

The *contrapositive* of $P \Rightarrow Q$ is the implication $\neg Q \Rightarrow \neg P$. A proof by contrapositive of $P \Rightarrow Q$ is a direct proof of $\neg Q \Rightarrow \neg P$. Another way of putting it: the contrapositive of "if A, then B" is "if not B, then not A."

3) Let n be an integer. If $5n - 7$ is even, then n is odd.

4) Let A and B be sets. If $A \cup B = A$, then $B \subseteq A$

Proof by Contradiction:

To show that $P \Rightarrow Q$ is true by contradiction we show that $\neg(P \Rightarrow Q) \Rightarrow \perp$. Since $\neg(P \Rightarrow Q)$ is logically equivalent to $(P \wedge \neg Q)$, we want to show that $(P \wedge \neg Q) \Rightarrow \perp$ (a contradiction).

5) $\sqrt{2}$ is irrational

Proof by Induction:

Let $S_1, S_2, S_3 \ldots$ be statements such that:

- **i.** **S_1 is true; and**
- **ii.** **Whenever S_k is true, where $k \in \mathbb{N}$, then S_{k+1} is true**

Then all of the statements $S_1, S_2, S_3 \ldots$ are true.

General steps to a proof by induction:

1. **Prove the base case:**
   Substitute base value and show LHS=RHS
2. **Inductive step:**
   a. **Inductive hypothesis: assume true for some $n = k$**
   b. **Show that $n = k + 1$ also holds**

(Substitute I.H. into equation to show LHS=RHS

6) Use induction to show that $\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$ is true for integers $n \geq 1$.

7) Consider the following recurrence relation:

$$T(n) = \begin{cases} 1, & n = 1 \\ T(n-1) + n, & n \geq 2 \end{cases}$$

Show by induction that $T(n) = n(n+1)/2$

<u>Loop Invariant Proof:</u>

To prove a statement S is correct, define S in terms of smaller statements $S_1, S_2, S_3 \ldots S_n$ where:

- **i. S_1 is true before the loop**
- **ii. S_k is true before iteration k, where $1 \leq k \leq n$, and based on this assumption we then must show that S_{k+1} is true after iteration k**
- **iii. Thus, S_n implies S is true by induction**

General steps to a loop invariant proof:

1. **Initialization (base case):**
   Proof the invariant is true before entering the loop for the first time (before the first iteration)
2. **Maintenance (inductive step)**
   a. **Inductive hypothesis: Assume the invariant is true up to an iteration k**
   b. **Show that at the end of the kth iteration, the invariant still holds before beginning the next iteration, $k + 1$**
3. **Termination**
   Show that the loop eventually terminates, and that the invariant holds when it does. (After the last iteration, this verifies we have the desired result!)

7) Prove the invariant "$result = i!$" given the following algorithm:

Algorithm fact(n):
    Input: An integer $n \geq 1$.
    Output: n!
    $i \leftarrow 1$
    $result \leftarrow 1$
    while $i < n$ **do**
        $i \leftarrow i + 1$
        $result \leftarrow result * i$
    end
    return $result$