Math Fundamentals II

- Direct Proof
- Proof by Contradiction
- Proof by Contraposition
- Proof by Induction

Direct Proof: to prove something of the form $p \rightarrow q$...

- Assume *p* is true…
- ...and show that *q* must also be true.

Example. Prove that if $\underbrace{n \text{ is an odd integer}}_{p}$, then $\underbrace{n^2 \text{ is also an odd integer}}_{q}$.

Prove: $p \to q$

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

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

$$= 2j + 1, \quad j = 2k^2 + 2k, \; j \in \mathbb{Z}.$$

Proof by Contraposition: to prove something of the form $p \rightarrow q$...

$p \rightarrow q$

$\equiv \neg q \rightarrow \neg p$

- Assume $\neg q$ is true...
- ...and show that $\neg p$ must also be true.

Example. Prove that if n^2 is an odd integer, then n is also an odd integer.

p

q

Let $n = 2k,\ k \in \mathbb{Z}$.

$n^2 = (2k)^2 = 4k^2 = 2(2k^2) = 2j;\ j = 2k^2,$

$j \in \mathbb{Z}$.

Proof by Contradiction: to prove something of the form *p*...

- Assume that *p* is false...
- ...and show that it leads to a contradiction.

Proof by Contradiction:
to prove something of the form $p \rightarrow q$...

- Assume that *p* is true and *q* is false...
- ...and show that it leads to a contradiction.

Example. Prove that $2^{1/2}$ is irrational.

$P \to F$

Assume $\sqrt{2}$ is rational. Then $\sqrt{2} = \frac{p}{q}$, $p, q \in \mathbb{Z}$, $q \neq 0$, p and q are coprime (no factors in common).

$$(\sqrt{2})^2 = \left(\frac{p}{q}\right)^2$$

$$2 = \frac{p^2}{q^2}$$

$$2q^2 = p^2$$

p^2 is even

p is even

$p = 2k$, $k \in \mathbb{Z}$

$$2 = \frac{(2k)^2}{q^2}$$

$$\frac{2q^2}{2} = \frac{4k^2}{2}$$

$$q^2 = 2k^2$$

q^2 is even

q is even

$$\frac{\cancel{2}k}{\cancel{2}j}$$

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

p and q are not coprime.

Example. What is wrong with this "proof" that 1 = 2?

Step	**Reason**
1. $a = b$	Premise
2. $a^2 = a \times b$	Multiply both sides of (1) by a
3. $a^2 - b^2 = a \times b - b^2$	Subtract b^2 from both sides of (2)
4. $(a - b)(a + b) = b(a - b)$	Algebra on (3)
5. $a + b = b$	Divide both sides by $a - b$ → dividing by 0
6. $2b = b$	Replace a by b in (5) because $a = b$
7. $2 = 1$	Divide both sides of (6) by b

Proof by Induction: to prove that something is true for all natural numbers (or a subset of natural numbers)...

$P(1) \rightarrow P(2) \rightarrow P(3)$

$P(k) \rightarrow P(k+1)$

$F \rightarrow F$

- Goal: Prove that P(n) is true for all $n \geq n_0$.
- Basis Step: Show that P(n) is true for n_0 (and possible more if necessary).
- Inductive Step:
  - Prove P(k) → P(k+1) for weak induction (or P(k-1) → P(k))
  - Prove P(n_0≤j≤k) → P(k+1) for strong induction

Parts of an Inductive Proof.

for all $n \geq 0$

① Basis Step → Show $P(k)$ for any base cases.

② Inductive Step: Show $P(k) \rightarrow P(k+1)$ (weak)

(a) State the IH.

OR $P(n_0 \leq j \leq k-1) \rightarrow P(k)$ (strong)

Assume this as the inductive hypothesis.

(b) Rewrite $P(k+1)$ in terms of something smaller.

(c) Apply the IH.

(d) Do math to finish the proof.

(end with $P(k)$ / $P(k+1)$)

Example.

Prove: $\sum_{j=1}^{n} \log j = \log(n!)$ for all $n \geq 1$.

<u>Basis Step</u>. $\sum_{j=1}^{1} \log j = \log 1 = 0 = \log(1!)$ ✓

<u>Inductive Step</u>. (weak induction)

Assume as the IH that $\sum_{j=1}^{k} \log j = \log(k!)$ for some $k \geq 1$.

Then $\sum_{j=1}^{k+1} \log j = \log((k+1)!)$ because:

$$\sum_{j=1}^{k+1} \log j = \sum_{j=1}^{k} \log j + \log(k+1) = \log(k!) + \log(k+1) \text{ by the IH}$$

$$\log(k!) + \log(k+1) = \log(k!(k+1)) = \log[(k+1)!]$$

Example. Prove $2^n < n!$ for all $n \geq 4$.

Basis Step.

$2^4 = 16 < 4! = 24$ ✓

Inductive Step. (weak induction)

Assume as the IH that $2^k < k!$ for some $k \geq 4$.

Then $2^{k+1} < (k+1)!$ because:

$2^{k+1} = 2 \cdot 2^k < 2 \cdot k!$ by the IH and

$2 \cdot k! < (k+1)k! = (k+1)!$

Example. Prove that every integer that is greater than or equal to 12 is the sum of a multiple of 4 and a multiple of 5.

Basis Step.

$12 = 4(3) + 5(0)$ ✓

$13 = 4(2) + 5(1)$ ✓

$14 = 4(1) + 5(2)$ ✓

$15 = 4(0) + 5(3)$ ✓

Inductive Step. (strong induction)

Assume as the IH that $j = 4a + 5b$, $a, b \in \mathbb{Z}$ for $12 \le j \le k-1$ for some $k \ge 16$. Then $k = 4n + 5m$, $n, m \in \mathbb{Z}$ because:

$k = k - 4 + 4 = 4a + 5b + 4$ by the IH $(a, b \in \mathbb{Z})$

$= 4(a+1) + 5b$ (Let $n = a+1$ and $m = b$).

Example. Is this a valid proof? NO

Given. T(N) = T(floor(N/3)) + 1 and T(1) = T(2) = 1
Conjecture. T(N) is O(logN)

Proof.
We will show that T(N) ≤ 2logN for all N ≥ 1. → This needs to be adjusted b/c T(1) does not work.

Basis Step.
T(1) = 1 ≤ 2(log1) = 2 ← not true
also, T(2) is also required.

Inductive Step.
Assume as the IH that T(k-1) ≤ 2log(k-1) for some k ≥ 1. ← should be strong induction
We will show that T(k) ≤ 2logk.

T(k) = T(floor(k/3)) + 1
≤ 2log(floor(k/3)) + 1 by the IH
≤ 2log(k/3) + 1
= 2logk - 2log3 + 1
≤ 2logk

Example. Let T(N) = T(N-1) + 1 and T(1) = 1. Prove that T(N) ≤ 2N for all N ≥ 1.

Basis Step:

$T(1) = 1 \leq 2(1)$ ✓

Inductive Step:

Assume as the IH that $T(k) \leq 2k$ for some $k \geq 1$.

Then $T(k+1) \leq k+1$ because:

$$
\begin{aligned}
T(k+1) &= T(k) + 1 \\
&\leq k + 1 \quad \text{by the IH}
\end{aligned}
$$

Example. Let T(N) = T(floor(N/2)) + N and T(1) = 1. Prove that T(N) ≤ 2N for all N ≥ 1.

Basis Step.

$T(1) = 1 \leq 2(1)$ ✓

Inductive Step.

Assume as the IH that $T(j) \leq 2j$ for $1 \leq j \leq k-1$ for some $k > 1$.

Then $T(k) \leq 2k$ because:

$$
\begin{aligned}
T(k) &= T(\lfloor k/2 \rfloor) + k \\
&\leq 2\lfloor k/2 \rfloor + k \quad \text{by the IH} \\
&\leq 2(k/2) + k \\
&= k + k = 2k
\end{aligned}
$$

Example. Let T(N) = T(floor(N/3)) + 1 and T(1) = T(2) = 1.
Prove that T(N) ≤ logN + 1 for all N ≥ 1.

Basis Step:

$T(1) = 1 \leq \log 1 + 1 = 1$ ✓

$T(2) = 1 \leq \log 2 + 1 = 2$ ✓

Inductive Step:

Assume as the IH that $T(j) \leq \log j + 1$ for $1 \leq j \leq k-1$ for some $k > 2$. Then $T(k) \leq \log k + 1$ because:

$$\begin{aligned} T(k) &= T(\lfloor k/3 \rfloor) + 1 \\ &\leq \log \lfloor k/3 \rfloor + 1 + 1 \quad \text{by the IH} \\ &\leq \log(k/3) + 1 + 1 \\ &= \log k - \log 3 + 1 + 1 \\ &= \log k + 1 - \log 3 + 1 \leq \log k + 1 \end{aligned}$$ ✓