Proofs by Contradiction

In a proof by contradiction, we prove a statement by assuming it is false and deriving a contradiction.

Q: Why are proofs by contradiction effective?

A: The assumption that the statement is false can help by giving us something concrete to work with.

Example:

Theorem: $\sqrt{2}$ is irrational.

Proof: Assume $\sqrt{2} \in \mathbb{Q}$. Then $\exists p, q \in \mathbb{N} \left(\sqrt{2} = \frac{p}{q} \land \gcd(p,q) = 1 \right)$.
Since $\sqrt{2} = \frac{p}{q}$, $p^2 = 2q^2$ so p must be even. Letting $r = \frac{p}{2}$, $r \in \mathbb{N}$ and $p^2 = (2r)^2 = 4r^2 = 2q^2$ so $q^2 = 2r^2$ and thus q must be even. But then $2 \mid p$ and $2 \mid q$, so $\gcd(p,q) \neq 1$. Contradiction.

Proofs by Contradiction

Theorem: There are infinitely many prime numbers.

Proof:

Lemma: $\forall n \in \mathbb{N} \setminus \{1\}\ \exists p \in \mathbb{P}\ (p \mid n)$

Proof: See next page.

Assume that there are finitely many primes $p_1, \dots, p_k$. Consider $n = \left(\prod_{j=1}^{k} p_j\right) + 1$.

Now $\forall j \in [k]$, $n = \left(\prod_{i \in [k] \setminus \{j\}} p_i\right) p_j + 1$ so $p_j \nmid n$. But then n is not divisible by any prime p, which by the lemma is impossible. Contradiction.

Lemma Proof

Lemma: $\forall n \in \mathbb{N} \setminus \{1\} \ \exists p \in \mathbb{P} \ (p \mid n)$

Proof:

Given $n \in \mathbb{N} \setminus \{1\}$, let p be the smallest natural number greater than 1 such that $p \mid n$.

Note: p exists as $n \mid n$.

Claim: $p \in \mathbb{P}$

Proof:

Assume $p \notin \mathbb{P}$. Then $\exists d \in \mathbb{N} \ (d \mid p \wedge 1 < d < p)$.

$d \mid p$ and $p \mid n$ so $d \mid n$. However, this contradicts our choice of p.

Contradiction.