Trying a direct proof

$\forall a(\mathtt{Even}(a^2) \rightarrow \mathtt{Even}(a))$ "if a^2 is even, then a is even."

Proof By Contradiction

If a^2 is even then a is even.

Claim: $\sqrt{2}$ is irrational (i.e. not rational).

Proof:

Suppose for the sake of contradiction that $\sqrt{2}$ is rational.

By definition of rational, there are integers s, t such that $t \neq 0$ and $\sqrt{2} = s/t$. Without loss of generality, let s/t be in lowest terms (i.e., with no common factors greater than 1).

$\sqrt{2} = \frac{s}{t}$

$2 = \frac{s^2}{t^2}$

$2t^2 = s^2$ so s^2 is even. By the fact above, s is even, i.e. s$= 2k$ for some integer k. Squaring both sides $s^2 = 4k^2$

Substituting into our original equation, we have: $2t^2 = 4k^2$, i.e. $t^2 = 2k^2$.

So t^2 is even (by definition of even). Applying the fact above again, t is even.

But if both s and t are even, they have a common factor of 2. But we said the fraction was in lowest terms.

That's a contradiction! We conclude $\sqrt{2}$ is irrational.

What's the difference?

What's the difference between proof by contrapositive and proof by contradiction?

Show $p \to q$	Proof by contradiction	Proof by contrapositive
Starting Point	$\neg(p \to q) \equiv (p \land \neg q)$	$\neg q$
Target	Something false	$\neg p$

Show p	Proof by contradiction	Proof by contrapositive
Starting Point	$\neg p$	---
Target	Something false	---

Another Proof By Contradiction

Claim: There are infinitely many primes.

Proof:

Suppose for the sake of contradiction, that there are only finitely many primes. Call them $p_1, p_2, \dots, p_k$.

Consider the number $q = p_1 \cdot p_2 \cdot \dots \cdot p_k + 1$

Case 1: q is prime

Case 2: q is composite

But [] is a contradiction! So there must be infinitely many primes.