1. Contradiction

proof by contradiction

Assume conclusion is false. Derive something that is absurd/impossible. This implies our original assumption is wrong, so the conclusion is true.

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

Proof: Suppose by way of contradiction (BWOC) that $\sqrt{2}$ is rational. So there exists $a, b \in \mathbb{Z}$, $b \neq 0$ such that $\sqrt{2} = \frac{a}{b}$. We choose a, b so that $\frac{a}{b}$ is fully reduced. Square both sides to get $2 = \frac{a^2}{b^2}$, so $a^2 = 2b^2$. Since $b^2 \in \mathbb{Z}$, a^2 is even. Then a is even. So there exists $k \in \mathbb{Z}$ such that $a = 2k$. So $(2k)^2 = 2b^2$, and $b^2 = 2k^2$. Since $k^2 \in \mathbb{Z}$, b^2 is even, then b is even. Since 2 divides both a and b, $\frac{a}{b}$ is not fully reduced, contradiction, so $\sqrt{2}$ is irrational.

Definition: For an integer $n \geq 2$, n is a prime if the only posible divisors are 1 and n. Otherwise n is composite, so there exist $a, b \in \mathbb{N}$, $a, b \geq 2$, such that $n = ab$.

primes: 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, ...

Proposition: Every integer $n \geq 2$ contains a prime divisor.

Proof: Suppose BWOC that there are integers ≥ 2 that do not have prime divisors. Among all such integers, let n be the smallest one (We can do this due to the well-ordering principle).

We see that n is not a prime, for otherwise $n|n$ and n is a prime divisor of itself, contradiction.

So n is composite, and there exists $a, b \in \mathbb{Z}$, $a, b \geq 2$ such that $n = ab$.

Since $a, b \geq 2$, $a < n$, By the minimality of our choice of n, a has a prime divisor p. Since $p|a$ and $a|n$, by transitivity, $p|n$. So p is a prime divisor of n, contradiction.

Euclid's Theorem: there are infinitely many primes.

Proof: suppose BWOC there are finitely many primes.

Let $p_1, p_2, \ldots, p_k$ be all the primes.

Define: $N = p_1 p_2 \cdots p_k + 1$. By the previous preposition, N has a prime divisor.

Suppose this prime is p_i.

Then $p_i \mid N$, so $p_i \mid (p_1 p_2 \ldots p_k + 1)$. Also, $p_i \mid p_1 p_2 \ldots k$

By div. of int. comb, $p_i \mid [(p_1 \ldots p_k + 1) - p_1 \ldots p_k]$,

so $p_i \mid 1$

Since all primes are at least 2, $p_i \nmid 1$.

Contradiction.