1

Proof by Contradiction

Assume we want to prove a statement P.
Let C be some statement.

P	C	$C \wedge \sim C$	$\sim P \Rightarrow (C \wedge \sim C)$
T	T	F	T
T	F	F	T
F	T	F	F
F	F	F	F

So $P \equiv \sim P \Rightarrow (C \wedge \sim C)$

Thus, to prove P, we can prove $\sim P \Rightarrow (C \wedge \sim C)$

The structure of a proof by contradiction is:

Assume $\sim P$.
⋮
Therefore $C \wedge \sim C$.

In the case of a $P \Rightarrow Q$ theorem

Assume $P \wedge \sim Q$
⋮
Therefore $C \wedge \sim C$

Recall
$\sim(P \Rightarrow Q) \equiv P \wedge \sim Q$

2

Prop: Let $a \in \mathbb{Z}$. If $2 \mid a^2$, then $2 \mid a$.

proof (Contradiction)

Suppose $2 \mid a^2$ but $2 \nmid a$. Then we have that $a = 2n+1$, which gives

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

Thus a^2 is odd which implies $2 \nmid a^2$, a contradiction.

$\square$

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

$\gcd(a,b)=1$

Proof: Suppose $\sqrt{2} \in \mathbb{Q}$. Then $\sqrt{2} = \frac{a}{b}$ for some $a, b \in \mathbb{Z}$ $(b \neq 0)$. It follows that $2 = \frac{a^2}{b^2}$. Then

$$2b^2 = a^2$$

This implies that $2 \mid a^2$, so by the previous proposition, $2 \mid a$. Thus $a = 2x$ so,

$$2b^2 = a^2 = (2x)^2 = 4x^2$$

This gives

$$b^2 = 2x^2$$

which implies $2 \mid b^2$, so $2 \mid b$. Since $2 \mid a$ and $2 \mid b$, it follows that $\gcd(a,b) \geq 2$, a contradiction. Therefore $\sqrt{2} \notin \mathbb{Q}$

③

<u>Theorem</u>: There are infinitely many prime numbers.

<u>proof</u>: Suppose there are finitely many primes.

Let the prime numbers be $p_1, p_2, \cdots, p_n$. Define $a = p_1 p_2 \cdots p_n + 1$, then since $a > 1$, there is a prime divisor of a. Therefore $p_k \mid a$ for some prime p_k, so $a = c p_k$ for some $c \in \mathbb{Z}$. Thus

$$a = p_1 p_2 \cdots p_{k-1} p_k p_{k+1} \cdots p_n + 1 = c p_k$$

This gives

$$1 = a - p_1 \cdots p_n = c p_k - p_1 \cdots p_{k-1} p_k p_{k+1} \cdots p_n$$

$$= p_k (c - p_1 \cdots p_{k-1} p_{k+1} \cdots p_n)$$

By definition, this means $p_k \mid 1$, a contradiction.

$\square$