Proof by Contradiction (or Indirect Proof)

Given a statement is either true or false. In order to prove a statement is true, one method is to assume the opposite of the statement, then deduce a contradiction to the opposite statement from known or given facts. This means the opposite statement must be false. Therefore the original statement is true. Here are a few examples. (Below we will write $\sim p$ to denote the opposite of a statement p.)

Examples of Proof by Contradiction

(1) Prove that $\sqrt{2}$ is an irrational number.

Solution. Assume $\sim(\sqrt{2}$ is irrational). Then $\sqrt{2}$ is rational. So there exist $m, n \in \mathbb{N}$ such that $\sqrt{2} = m/n$ and after cancelling common factors, $\underline{m, n \text{ will have no common factor greater than } 1.}$

Squaring both sides and multiplying by n^2, we have $2n^2 = m^2$. Then m^2 is even, hence m is even. Then there exists $k \in \mathbb{N}$ such that $m = 2k$. So $2n^2 = (2k)^2 = 4k^2$. Then $n^2 = 2k^2$. Again, we see n^2 is even. Then n is also even. As m, n are both even, they have a common factor 2, contradiction (to the underlined statement). Therefore, $\sqrt{2}$ is irrational.

---

(2) Let $a \in \mathbb{R}$ such that the equation $x^3 + \sqrt{2}x^2 - \sqrt{3}x + a = 0$ have three real roots. Prove that the equation has an irrational root.

Solution. Assume $\sim$(the equation has an irrational root). Then the equation has no irrational root. Hence all three roots r_1, r_2, r_3 are rational. In that case,

$$x^3 + \sqrt{2}x^2 - \sqrt{3}x + a = (x - r_1)(x - r_2)(x - r_3) = x^3 - (r_1 + r_2 + r_3)x^2 + (r_1 r_2 + r_2 r_3 + r_3 r_1)x - r_1 r_2 r_3.$$

Then $\sqrt{2} = r_1 + r_2 + r_3 \in \mathbb{Q}$, contradiction.

---

(3) Let $a, b \in \mathbb{Q}$ and $a < b$. Prove that $\exists c \in \mathbb{R} \setminus \mathbb{Q}$ such that $a \le c \le b$.

Solution. Assume $\sim(\exists c \in \mathbb{R} \setminus \mathbb{Q}$ such that $a \le c \le b)$. Then $\underline{\forall c \in \mathbb{R} \setminus \mathbb{Q}, \text{ either } c < a \text{ or } c > b.}$ We are given that $a, b \in \mathbb{Q}$ and $a < b$, which imply $d = (b - a)/2 > 0$ and $d \in \mathbb{Q}$.

Since $1 < \sqrt{2} < 2$, we have $d < d\sqrt{2} < 2d$. Adding a to all parts, we get

$$(a + b)/2 = a + d < a + d\sqrt{2} < a + 2d = b.$$

Since $a < b$, we get $a + a < a + b$ and so $a < (a + b)/2$. Then $a < a + d\sqrt{2} < b$. From the underlined statement, we see $r = a + d\sqrt{2} \in \mathbb{Q}$. Then $\sqrt{2} = (r - a)/d$. Since $r, a, d \in \mathbb{Q}$, we get $(r - a)/d \in \mathbb{Q}$, contradiction (to $\sqrt{2}$ is irrational).

---

(4) Let A, B, C be sets. Prove that $A \setminus (B \cup C) \subseteq (A \setminus B) \cap (A \setminus C)$.

Solution. Assume $A \setminus (B \cup C) \subseteq (A \setminus B) \cap (A \setminus C)$ is false. Then there exists x such that (i) $x \in A \setminus (B \cup C)$ and (ii) $x \notin (A \setminus B) \cap (A \setminus C)$. Now condition (i) means $x \in A$ and

$$x \notin B \cup C \ \Big(= \sim (x \in B \cup C) \ = \sim ((x \in B) \text{ or } (x \in C)) \ = \ (x \notin B) \text{ and } (x \notin C)\Big).$$

Then $x \in A \setminus B$ and $x \in A \setminus C$. So $x \in (A \setminus B) \cap (A \setminus C)$, contradiction (to condition (ii)).

---

(5) Let $P(n)$ be a true or false statement. Given $P(1)$ is true. Suppose

(*) $\forall\ n \in \mathbb{N}$, if $P(n)$ is true, then $P(n+1)$ is true.

Prove that $\forall\ n \in \mathbb{N}$, $P(n)$ is true.

Solution. Assume $\sim(\forall\ n \in \mathbb{N}$, $P(n)$ is true). Then $\exists\ n \in \mathbb{N}$ such that $P(n)$ is false.

Examine $P(1), P(2), \ldots, P(n)$ in that order. Since $P(n)$ is false, there is a *smallest* positive integer m (at most equal to n) such that $\underline{P(m) \text{ is false.}}$ Since $P(1)$ is true, $m \geq 2$. Then $m-1 \geq 1$. Since $P(m)$ is false with m smallest. So $P(m-1)$ is true. By (*), $P(m) = P((m-1)+1)$ is true, contadiction (to underlined statement). Therefore, $\forall\ n \in \mathbb{N}$, $P(n)$ is true.

Exercises For the exercises below, do proof by contradiction.

(1) Let $x \in \mathbb{R}$ and $x^3 + 4x - 4 = 0$. Prove that x is irrational. (*Hint*: Assume $x = m/n$ in reduced term. Show m, n are even.)

(2) A prime number is an integer greater than 1 such that its only positive divisors are 1 and itself. (For example, 2, 3, 5 are prime numbers.) Prove that there are infinitely many prime numbers. (*Hint*: Assume only finitely many of these prime number exists, say in increasing order, they are $p_1 = 2,\ p_2 = 3,\ p_2 = 5,\ \ldots,\ p_n$. Show $M = p_1 p_2 \cdots p_n + 1$ is also a prime number.) How many prime numbers p are there such that $p+1$ is divisible by 4?

(3) Prove that it is impossible to order the complex numbers $\mathbb{C}$ so that the following properties all hold:

(a) for every $x, y \in \mathbb{C}$, exactly one of the following $x > y$, $x = y$, $y > x$ is true

(b) if $x, y \in \mathbb{C}$ and $x > y$, then for every $z \in \mathbb{C}$, $x + z > y + z$

(c) if $x, y \in \mathbb{C}$, $x > 0$ and $y > 0$, then $xy > 0$.

(*Hint*: Assume it is possible. Start with $i \neq 0$. There are two cases, namely $i > 0$ or $0 > i$. In each case, try to show $1 > 0$ and $0 > 1$ will follow. So both cases will lead to contradiction.)