# Dr Oliver Mathematics
# Proof by Contradiction

In this note, we will examine proof by contradiction.

To prove that a statement, $P$, is true, we begin by assuming that $P$ is false and show that it leads to a contradiction.

**Example 1**
$\sqrt{2}$ is irrational.

**Solution** Suppose $\sqrt{2}$ *is* rational. Then

$$\sqrt{2} = \frac{a}{b}$$

for some $a \in \mathbb{N}$ and $b \in \mathbb{N}$ in simplest form. Now,

$$\begin{aligned}\sqrt{2} = \frac{a}{b} &\Rightarrow a = \sqrt{2}b \\ &\Rightarrow a^2 = 2b^2.\end{aligned}$$

Now, $2b^2$ is even so $a^2$ is even.
And, if $a^2$ is even, then $a$ is even.
Next, $a = 2c$ for some integer $c$.
Now,

$$\begin{aligned}a^2 = 2b^2 &\Rightarrow (2c)^2 = 2b^2 \\ &\Rightarrow 4c^2 = 2b^2 \\ &\Rightarrow 2c^2 = b^2.\end{aligned}$$

Now, $2c^2$ is even so $b^2$ is even.
And, if $b^2$ is even, then $b$ is even – contradiction.

Therefore, $\sqrt{2}$ is irrational. ■

**Example 2**
There are infinitely many prime numbers.

**Solution** Let us assume there *is* a greatest prime number.
Let $p_1$, $p_2$, $p_3$, …, $p_n$ be the list of prime numbers.
Now, consider

$$N = p_1 p_2 p_3 \ldots p_n + 1.$$

Is this a prime?
$p_1$? No, because we are left with remainder 1.

$p_2$? No, because we are left with remainder 1.
⋮
$p_n$? No, because we are left with remainder 1.
So, if you divide $N$ by one of the primes on our list, you get a remainder of 1. So $N$ is not divisible by any of the primes $p_1$, $p_2$, $p_3$, ..., $p_n$.

However, by the Fundamental Theorem of Arithmetic, $N$ must have a prime factor (which might be either itself or some smaller number). This contradicts our assumption that $p_1$, $p_2$, $p_3$, ..., $p_n$ was a list of all the prime numbers.

Therefore, there are infinitely many prime numbers. ■

**Example 3**
There is no greatest even integer.

**Solution** Suppose there *is* a greatest even integer, $N$. For every even integer $n$, $N \geqslant n$. Now, consider

$$M = N + 2.$$

Then, $M$ is an even integer because it is a sum of even integers. Also, $M > N$ since $M = N + 2$. Therefore, $M$ is an integer that is greater than the greatest integer – contradiction.

Therefore, there is no greatest even integer. ■

Here are some examples for you to try.

1. $\sqrt{3}$ is irrational.

**Solution**

Suppose $\sqrt{3}$ is rational. Then

$$\sqrt{3} = \frac{a}{b}$$

for some $a \in \mathbb{N}$ and $b \in \mathbb{N}$ in simplest form. Now,

$$\begin{aligned} \sqrt{3} = \frac{a}{b} &\Rightarrow a = \sqrt{3}b \\ &\Rightarrow a^2 = 3b^2. \end{aligned}$$

Case: if $b$ is even

$$
\begin{aligned}
b \text{ even} &\Rightarrow b^2 \text{ even} \\
&\Rightarrow 3b^2 \text{ even} \\
&\Rightarrow a^2 \text{ even} \\
&\Rightarrow a \text{ even},
\end{aligned}
$$

in which case $\dfrac{a}{b}$ is not in simplest form.

Case: if $b$ is odd

$$
\begin{aligned}
b \text{ odd} &\Rightarrow b^2 \text{ odd} \\
&\Rightarrow 3b^2 \text{ odd} \\
&\Rightarrow a^2 \text{ odd} \\
&\Rightarrow a \text{ odd}.
\end{aligned}
$$

Now,

$$a = 2m + 1 \text{ and } b = 2n + 1.$$

Then,

$$
\begin{aligned}
a^2 = 3b^2 &\Rightarrow (2m+1)^2 = 3(2n+1)^2 \\
&\Rightarrow 4m^2 + 4m + 1 = 3(4n^2 + 4n + 1) \\
&\Rightarrow 4m^2 + 4m + 1 = 12n^2 + 12n + 3 \\
&\Rightarrow 4m^2 + 4m = 12n^2 + 12n + 2 \\
&\Rightarrow 2m^2 + 2m = 6n^2 + 6n + 1 \\
&\Rightarrow 2m(m+1) = 6n(n+1) + 1.
\end{aligned}
$$

Since $2m(m+1)$ is an integer, the left hand side is even. Since $6n(n+1)+1$ is an integer, the right hand side is odd and we have found a contradiction.

Therefore, $\sqrt{3}$ is irrational.

2. $\sqrt{5}$ is irrational.

**Solution**

Suppose $\sqrt{5}$ is rational. Then

$$\sqrt{5} = \frac{a}{b}$$

for some $a \in \mathbb{N}$ and $b \in \mathbb{N}$ in simplest form. Now,

$$\begin{aligned}\sqrt{5} = \frac{a}{b} &\Rightarrow a = \sqrt{5}b \\ &\Rightarrow a^2 = 5b^2.\end{aligned}$$

Case: if $b$ is even

$$\begin{aligned} b \text{ even} &\Rightarrow b^2 \text{ even} \\ &\Rightarrow 3b^2 \text{ even} \\ &\Rightarrow a^2 \text{ even} \\ &\Rightarrow a \text{ even,} \end{aligned}$$

in which case $\frac{a}{b}$ is not in simplest form.

Case: if $b$ is odd

$$\begin{aligned} b \text{ odd} &\Rightarrow b^2 \text{ odd} \\ &\Rightarrow 3b^2 \text{ odd} \\ &\Rightarrow a^2 \text{ odd} \\ &\Rightarrow a \text{ odd.} \end{aligned}$$

Now,

$$a = 2m + 1 \text{ and } b = 2n + 1.$$

Then,

$$\begin{aligned} a^2 = 5b^2 &\Rightarrow (2m+1)^2 = 3(2n+1)^2 \\ &\Rightarrow 4m^2 + 4m + 1 = 5(4n^2 + 4n + 1) \\ &\Rightarrow 4m^2 + 4m + 1 = 20n^2 + 20n + 5 \\ &\Rightarrow 4m^2 + 4m = 20n^2 + 20n + 4 \\ &\Rightarrow m^2 + m = 5n^2 + 5n + 1 \\ &\Rightarrow m(m+1) = 5n(n+1) + 1. \end{aligned}$$

Since $m(m+1)$ is an integer, the left hand side is even. Since $5n(n+1)+1$ is an integer, the right hand side is odd and we have found a contradiction.

Therefore, $\sqrt{5}$ is irrational.

3. $\sqrt{6}$ is irrational.

**Solution**

Suppose $\sqrt{6}$ is rational. Then

$$\sqrt{6} = \frac{a}{b}$$

for some $a \in \mathbb{N}$ and $b \in \mathbb{N}$ in simplest form. Now,

$$\begin{aligned}\sqrt{6} = \frac{a}{b} &\Rightarrow a = \sqrt{6}b \\ &\Rightarrow a^2 = 6b^2.\end{aligned}$$

This last statement means the right-hand side is even, because it is a product of integers and one of those integers (at least) is even. So $a^2$ must be even. But any odd number times itself is odd, so if $a^2$ is even, then $a$ is even. If $a$ is even, then $a = 2c$ for some natural number $c$. Then,

$$\begin{aligned}a^2 = 6b^2 &\Rightarrow (2c)^2 = 6b^2 \\ &\Rightarrow 4c^2 = 6b^2 \\ &\Rightarrow 2c^2 = 3b^2.\end{aligned}$$

Now we see that $3b^2$ is even. For $3b^2$ to be even, $b^2$ must be even since 3 is odd and an odd times an even number is even. And by the same argument above, if $b^2$ is even then $b$ is even. So both $p$ and $q$ are even which means both are divisible by 2. But that means in which case $\frac{a}{b}$ is not in simplest form – contradiction.

So $\sqrt{6}$ is irrational.

4. $\sqrt[3]{2}$ is irrational.

**Solution**

Suppose $\sqrt[3]{2}$ is rational. Then

$$\sqrt[3]{2} = \frac{a}{b}$$

for some $a \in \mathbb{N}$ and $b \in \mathbb{N}$ in simplest form. Now,

$$\begin{aligned}\sqrt[3]{2} = \frac{a}{b} &\Rightarrow a = \sqrt[3]{2}b \\ &\Rightarrow a^3 = 2b^3.\end{aligned}$$

Now, $a^3$ is even which implies $a$ is even. Let $a = 2c$ where $c$ is a positive integer.

Then,

$$
\begin{aligned}
a^3 = 2b^3 &\Rightarrow (2c)^3 = 2b^3 \\
&\Rightarrow 8c^3 = 2b^3 \\
&\Rightarrow 4c^3 = b^3.
\end{aligned}
$$

Now, $b^3$ is even which implies $b$ is even – contradiction.

So $\sqrt[3]{2}$ is irrational.

5. Prove that $\log_5 10$ is irrational.

**Solution**

Suppose $\log_5 10$ is rational. Then

$$\log_5 10 = \frac{a}{b}$$

for some $a \in \mathbb{N}$ and $b \in \mathbb{N}$ in simplest form. Now,

$$
\begin{aligned}
\log_5 10 = \frac{a}{b} &\Rightarrow 10 = 5^{\frac{a}{b}} \\
&\Rightarrow 10^b = 5^a.
\end{aligned}
$$

So, we have $10^b$ which is a 1 followed by $b$ zeroes and $5^a$ which ends in a 5 – contradiction.

So $\log_5 10$ is irrational.

6. There exist no integers $a$ and $b$ for which $18a + 6b = 1$.

**Solution**

There *exist* (one or more) integers $a \in \mathbb{Z}$ and $b \in \mathbb{Z}$ for which $18a + 6b = 1$. Then

$$18a + 6b = 1 \Rightarrow 6a + b = \tfrac{1}{6}.$$

$6a$ is an integer, $b$ is an integer, and so $6a + b$ is an integer. But $\frac{1}{6}$ is not an integer – contradiction.

So there exist no integers $a$ and $b$ for which $18a + 6b = 1$.

7. If $|x| < \epsilon$ for every real number $\epsilon > 0$, then $x = 0$.

**Solution**

Suppose that $|x| < \epsilon$ for every positive number $\epsilon$ but $x \neq 0$.

Since $x \neq 0$, necessarily $\frac{1}{2}|x| > 0$, so in particular $|x| < \epsilon$ for the positive number $\epsilon = \frac{1}{2}|x| > 0$. This means

$$|x| < \tfrac{1}{2}|x|.$$

But, $x \neq 0$ by assumption, so we can divide both sides by $|x|$ to conclude that $1 < \frac{1}{2}$ – contradiction.

Thus, if $|x| < \epsilon$ for every real number $\epsilon > 0$, then $x = 0$.

8. $\sqrt{2} + \sqrt{6} < \sqrt{15}$.

**Solution**

Suppose that $\sqrt{2} + \sqrt{6} \geqslant \sqrt{15}$. Then

$$\begin{aligned}
\sqrt{2} + \sqrt{6} \geqslant \sqrt{15} &\Rightarrow (\sqrt{2} + \sqrt{6})^2 \geqslant 15 \\
&\Rightarrow (\sqrt{2})^2 + 2(\sqrt{2})(\sqrt{6}) + (\sqrt{6})^2 \geqslant 15 \\
&\Rightarrow 2 + 4\sqrt{3} + 6 \geqslant 15 \\
&\Rightarrow 4\sqrt{3} \geqslant 7 \\
&\Rightarrow (4\sqrt{3})^2 \geqslant 7^2 \\
&\Rightarrow 48 \geqslant 49 \text{ – contradiction.}
\end{aligned}$$

So $\sqrt{2} + \sqrt{6} < \sqrt{15}$.

9. If $n$ is an integer and $n^3 + 5$ is odd, then $n$ is even.

**Solution**

$n \in \mathbb{Z}$ and suppose that $n^3 + 5$ is odd but that $n$ is odd.
So $n = 2k + 1$ for some integer $k$.

Then

$$\begin{aligned} n^3+5 &= (2k+1)^3+5 \\ &= (8k^3+12k^2+6k+1)+5 \\ &= 8k^3+12k^2+6k+6 \\ &= 2(k^3+6k^2+3k+3). \end{aligned}$$

But $n = 2 \times$ an integer and so $n$ is even – contradiction.

So, if $n$ is an integer and $n^3+5$ is odd, then $n$ is even.

10. For all integers $n$, if $n^2$ is odd, then $n$ is odd.

**Solution**

Suppose that $n^2$ is odd, then $n$ is even. By definition of even, we have $n = 2k$ for some integer $k$. So, by substitution, we have

$$\begin{aligned} n^2 &= (2k)^2 \\ &= 2(2k^2). \end{aligned}$$

Now, $2k^2$ is an integer because the products of integers are integers. So $n^2$ is even which mean that $n$ is even contradiction.

Hence, if $n^2$ is odd, then $n$ is odd.

11. The sum of any rational number and any irrational number is irrational.

**Solution**

Suppose that the sum of the rational number $x$ and the irrational number $y$ is rational. So

$$x = \frac{a}{b} \text{ and } x+y = \frac{c}{d}$$

for some integers $a$, $b$, $c$, and $d$ with $b \neq 0$ and $d \neq 0$. Now,

$$\begin{aligned} x+y = \frac{c}{d} &\Rightarrow \frac{a}{b}+y = \frac{c}{d} \\ &\Rightarrow y = \frac{c}{d} - \frac{a}{b} \\ &\Rightarrow y = \frac{bc-ad}{bd}. \end{aligned}$$

But $(bc - ad)$ are integers because $a$, $b$, $c$, and $d$ are all integers and products and differences of integers are integers, and $bd \neq 0$ by zero product property. Therefore, by definition of rational, $y$ is rational – contradiction.

So the sum of any rational number and any irrational number is irrational.

12. There do not exist two prime numbers $p$ and $q$ for which $p - q = 97$.

**Solution**

Suppose for the sake of contradiction that this is true. Let $p$ and $q$ be prime numbers for which $p - q = 97$. Now, they have opposite parity (even/odd) so $q = 2$.

What is $p$? Well,

$$p = 97 + 2 = 99 = 9 \times 11 \text{ – contradiction.}$$

So there do not exist two prime numbers $p$ and $q$ for which $p - q = 97$.