1. To demonstrate that a statement is true, we sometimes proceed as described in (1) or (2):

   (1) In case the statement is 'very simple', with no apparent 'assumption part' and 'conclusion part', we start by supposing the statement did not hold true.
   Then we logically deduce something 'ridiculously wrong'.
   Hence we declare that the statement under consideration has to hold true in the first place.

   (2) In case the statement is a 'conditional', we start by supposing the assumption in the statement holds true and the conclusion did not hold true.
   Then we logically deduce something 'ridiculously wrong'.
   Hence we declare that the conclusion of the statement has to hold true under the assumption of the statement.

   This method of proof is called **proof-by-contradiction**.

## 2. **Definitions.**

1. *Let* $r \in \mathbb{R}$.

(I) $r$ *is said to be a* **rational number** *if*

$$\text{there exist some } m, n \in \mathbb{Z} \text{ such that } n \neq 0 \text{ and } m = nr.$$

'$n \neq 0$' ensures that it makes sense to rewrite '$m = nr$' as '$r = \frac{m}{n}$'.

(II) $r$ *is said to be an* **irrational number** *if* $r$ *is not a rational number.*

2. *Let* $p \in \mathbb{Z} \setminus \{-1, 0, 1\}$.

$p$ *is called a* **prime number** *if* $p$ *is divisible by no integer other than* $1, -1, p, -p$.

3. **Statement (A).**

*Suppose $a, b$ are rational numbers and $b \neq 0$. Then $a + b\sqrt{2}$ is an irrational number.*

**Proof of Statement (A), with proof-by-contradiction argument?**

- Tacitly assumed results (since school days):

(AT1) *$\sqrt{2}$ is an irrational number.*

(AT2) *Let $r, s$ be rational numbers. $r + s, r - s, rs$ are rational numbers.*
*Moreover, if $s \neq 0$ then $\dfrac{r}{s}$ is a rational number.*

**Statement (A).**

- Tacitly assumed results:

(AT1) $\sqrt{2}$ is an irrational number.

(AT2) Let $r, s$ be rational numbers. $r+s$, $r-s$, $rs$ are rational numbers. Moreover, if $s \neq 0$ then $r/s$ is a rational number.

*Suppose $a, b$ are rational numbers and $b \neq 0$. Then $a + b\sqrt{2}$ is an irrational number.*

**Proof of Statement (A), with proof-by-contradiction argument.**

Suppose $a, b$ are rational numbers and $b \neq 0$.

Further suppose it were true that $a+b\sqrt{2}$ was a rational number.

[We are going to look for something 'ridiculously wrong' out of the combination of what we have supposed and what we have further supposed.]

Write $r = a+b\sqrt{2}$.

Since $a, r$ were rational numbers and $b\sqrt{2} = r-a$,

$b\sqrt{2}$ would be a rational number.

Since $b$ is a non-zero rational number and $\sqrt{2} = \frac{b\sqrt{2}}{b}$,

$\sqrt{2}$ would be a rational number.

But $\sqrt{2}$ is an irrational number. Contradiction arises.

Hence our assumption that $a+b\sqrt{2}$ was a rational number is false.

$a+b\sqrt{2}$ is an irrational number. $\square$

4. **Statement (B).**

*$\sqrt{2}$ is an irrational number.*

**Proof of Statement (B), with proof-by-contradiction argument?**

- Tacitly assumed result (known as **Euclid's Lemma**) for the purpose of this example:

(EL) *Let $h, k \in \mathbb{Z}$, and $p$ be a prime number.*
*Suppose $hk$ is divisible by $p$.*
*Then at least one of $h, k$ is divisible by $p$.*

- Tacitly assumed result (Euclid's Lemma):

(EL) Let $h, k \in \mathbb{Z}$, and $p$ be a prime number. Suppose $hk$ is divisible by $p$. Then at least one of $h, k$ is divisible by $p$.

**Statement (B).**

*$\sqrt{2}$ is an irrational number.*

**Proof of Statement (B), with proof-by-contradiction argument.**

← First attempt, and an incomplete one.

Suppose it were true that $\sqrt{2}$ was a rational number.

[Look for something 'ridiculously wrong' out of what we have supposed.]

Then there would exist some $m, n \in \mathbb{Z}$ such that $n \neq 0$ and $\sqrt{2} = \frac{m}{n}$.

Since $\sqrt{2} = \frac{m}{n}$, we would have $m^2 = 2n^2$. —— (✡)

Since $n^2 \in \mathbb{Z}$, $m^2$ would be divisible by 2.

By Euclid's Lemma, $m$ would be divisible by 2.

Then there would exist some $k \in \mathbb{Z}$ such that $m = 2k$.

Therefore, for the same $m, n, k \in \mathbb{Z}$, we would have $2n^2 = m^2 = (2k)^2 = 4k^2$.

Hence $n^2 = 2k^2$.

[Now look back at (✡).]

Repeating the about argument, we deduce that $n$ would be divisible by 2.

[Ask: what is wrong with all this???]

[Ask: what more can be said about $m, n$ now?] →

[Ask: what about $n$?] →

**Statement (B).**

*$\sqrt{2}$ is an irrational number.*

- Tacitly assumed result (Euclid's Lemma):

(EL) Let $h, k \in \mathbb{Z}$, and $p$ be a prime number. Suppose $hk$ is divisible by $p$. Then at least one of $h$, $k$ is divisible by $p$.

**Proof of Statement (B), with proof-by-contradiction argument.**

Suppose it were true that $\sqrt{2}$ was a rational number.

[Look for something 'ridiculously wrong' out of what we have supposed.]

Then there would exist some $m, n \in \mathbb{Z}$ such that $n \neq 0$ and $\sqrt{2} = \frac{m}{n}$.

Without loss of generality, we assume that $m, n$ have no common factor other than $1, -1$.

Since $\sqrt{2} = \frac{m}{n}$, we would have $m^2 = 2n^2$.

Since $n^2 \in \mathbb{Z}$, $m^2$ would be divisible by 2.

By Euclid's Lemma, $m$ would be divisible by 2.

Then there would exist some $k \in \mathbb{Z}$ such that $m = 2k$.

Therefore, for the same $m, n, k \in \mathbb{Z}$, we would have $2n^2 = m^2 = (2k)^2 = 4k^2$.

Hence $n^2 = 2k^2$.

[Now look back.]

Repeating the above argument, we deduce that $n$ would be divisible by 2.

Now 2 would be a common factor of $m, n$.

But recall that $m, n$ have no common factor other that $1, -1$.

Contradiction arises.

Hence our assumption that $\sqrt{2}$ was a rational number is false.

$\sqrt{2}$ is an irrational number. □

5. **Statement (C).**

*Let $m, n \in \mathbb{Z}$. Suppose $0 < |m| < |n|$. Then $m$ is not divisible by $n$.*

**Proof of Statement (C), with proof-by-contradiction argument.**

Let $m, n \in \mathbb{Z}$. Suppose $0 < |m| < |n|$.

Further suppose it were true that $m$ was divisible by $n$.

Then there would exist some $k \in \mathbb{Z}$ such that $m = kn$. ← How to proceed further? Ask: • What kind of integers are $m, k, n$? • What does $m = kn$ suggest?

Since $|m| > 0$, we have $m \neq 0$.

Since $m = kn$, we have $k \neq 0$. Then $|k| \geq 1$.

Recall that $|n| \geq 0$. Then

$$|m| = |kn| = |k| \cdot |n| \geq 1 \cdot |n| = |n| > |m|.$$

Contradiction arises. The assumption that $m$ was divisible by $n$ is false.

Hence $m$ is not divisible by $n$. □