MATH1050 Examples of proofs-by-contradiction

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**.

   Here we give some examples of the application of this method. The focus is on the format of the argument. We postpone the discussion on the mechanism behind this method of argument until we know more about mathematical logic.

2. **Definitions**.

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

      (I) *r is said to be a* **rational number** *if there exist some* $m, n \in \mathbb{Z}$ *such that* $n \neq 0$ *and* $m = nr$.

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

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

   - Tacitly assumed result for the purpose of this example:

   (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 $\frac{r}{s}$ is a rational number.*

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

   Suppose a, b are rational numbers and $b \neq 0$.
   Suppose it were true that $a + b\sqrt{2}$ was a rational number. 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 $\sqrt{2} = \dfrac{b\sqrt{2}}{b}$, $\sqrt{2}$ would be a rational number.
   But $\sqrt{2}$ is an irrational number.
   This is a contradiction.
   Hence our assumption that $a + b\sqrt{2}$ was a rational number is false.
   $a + b\sqrt{2}$ is an irrational number.

   Remark. Below is an argument in which the tacit assumption (A2) is not used:

   Suppose a, b are rational numbers and $b \neq 0$.
   Suppose it were true that $a + b\sqrt{2}$ was a rational number.
   Then (by definition of rational numbers,) there would exist some m, n such that $n \neq 0$ and $m = n(a + b\sqrt{2})$.
   Since a, b are rational numbers, there exist some s, t, u, v such that $t \neq 0$, $v \neq 0$ and $s = ta$, $u = vb$.
   Now $\dfrac{m}{n} = a + b\sqrt{2} = \dfrac{s}{t} + \dfrac{u}{v}\sqrt{2}$.
   Since $b \neq 0$, $u \neq 0$. Since $n \neq 0$ and $t \neq 0$, we have $unt \neq 0$.
   Note that $\sqrt{2} = \dfrac{v}{u}\left(\dfrac{m}{n} - \dfrac{s}{t}\right) = \dfrac{vmt - vns}{unt}$. Also that $vmt, vns, vmt - vns, unt \in \mathbb{Z}$.
   Then (by definition of rational numbers,) $\sqrt{2}$ 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.

4. **Statement (B)**.

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

- 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.*

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

Suppose it were true that $\sqrt{2}$ was a rational number.
Then there would exist $m, n \in \mathbb{Z}$ 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 $1, -1$; (otherwise, cancel all common factors of m, n as numerators, denominators in the fraction $\frac{m}{n}$ to obtain $\frac{m'}{n'}$ and then re-label m', n' as m, n respectively).
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.
According to 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, we would have $2n^2 = (2k)^2 = 4k^2$.
Hence $n^2 = 2k^2$.
Repeating the above argument, we deduce that n would be divisible by 2.
Now 2 would be a common factor of m and n.
But recall that m, n have no common factor other than $1, -1$.
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 $0 < |m| < |n|$.
Suppose it were true that m was divisible by n.
Then there would exist some $k \in \mathbb{Z}$ such that $m = kn$.
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 $|m| = |kn| = |k||n| \geq 1 \cdot |n| = |n| > |m|$.
Contradiction arises.
Hence m is not divisible by n.

6. **Appendix. An illustration of proof-by-contradiction from elementary linear algebra.**

Refer to your (first) *linear algebra* course for the respective definitions of the notions of *linear combinations*, *linear dependence*, *linear independence*.

Statement (D).

Let $\mathbf{u}_1, \mathbf{u}_2, \mathbf{u}_3, \mathbf{v}$ be vectors in $\mathbb{R}^n$. Suppose $\mathbf{u}_1, \mathbf{u}_2, \mathbf{u}_3$ are linearly independent over $\mathbb{R}$. Then $\mathbf{v}$ is a linear combination of $\mathbf{u}_1, \mathbf{u}_2, \mathbf{u}_3$ over $\mathbb{R}$, or $\mathbf{u}_1, \mathbf{u}_2, \mathbf{u}_3, \mathbf{v}$ are linearly independent over $\mathbb{R}$.

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

Let $\mathbf{u}_1, \mathbf{u}_2, \mathbf{u}_3, \mathbf{v}$ be vectors in $\mathbb{R}^n$. Suppose $\mathbf{u}_1, \mathbf{u}_2, \mathbf{u}_3$ are linearly independent over $\mathbb{R}$.
Further suppose $\mathbf{v}$ is not a linear combination of $\mathbf{u}_1, \mathbf{u}_2, \mathbf{u}_3$ over $\mathbb{R}$, and $\mathbf{u}_1, \mathbf{u}_2, \mathbf{u}_3, \mathbf{v}$ are linearly dependent over $\mathbb{R}$.
Since $\mathbf{u}_1, \mathbf{u}_2, \mathbf{u}_3, \mathbf{v}$ are linearly dependent over $\mathbb{R}$, there existed some $\alpha_1, \alpha_2, \alpha_3, \beta \in \mathbb{R}$ such that $\alpha_1\mathbf{u}_1 + \alpha_2\mathbf{u}_2 + \alpha_3\mathbf{u}_3 + \beta\mathbf{v} = \mathbf{0}$ and $\alpha_1, \alpha_2, \alpha_3, \beta$ were not all zero.
We claim that it would then happen that $\beta = 0$. Justification:

> Suppose $\beta \neq 0$. Then it would be true that $\mathbf{v} = -\frac{\alpha_1}{\beta}\mathbf{u}_1 - \frac{\alpha_2}{\beta}\mathbf{u}_2 - \frac{\alpha_3}{\beta}\mathbf{u}_3$. Therefore it would be true that $\mathbf{v}$ was a linear combination of $\mathbf{u}_1, \mathbf{u}_2, \mathbf{u}_3$. Contradiction would arise.

Then $\beta = 0$ indeed.
Since $\beta = 0$ and $\alpha_1, \alpha_2, \alpha_3, \beta$ were not all zero, it would be true that $\alpha_1, \alpha_2, \alpha_3$ were not all zero.
Recall that $\mathbf{0} = \alpha_1\mathbf{u}_1 + \alpha_2\mathbf{u}_2 + \alpha_3\mathbf{u}_3 + \beta\mathbf{v} = \alpha_1\mathbf{u}_1 + \alpha_2\mathbf{u}_2 + \alpha_3\mathbf{u}_3$.
Then $\mathbf{u}_1, \mathbf{u}_2, \mathbf{u}_3$ would be linearly dependent over $\mathbb{R}$.
Recall that by assumption, $\mathbf{u}_1, \mathbf{u}_2, \mathbf{u}_3$ are linearly independent over $\mathbb{R}$.
Contradiction arises.
Hence $\mathbf{v}$ is a linear combination of $\mathbf{u}_1, \mathbf{u}_2, \mathbf{u}_3$ over $\mathbb{R}$, or $\mathbf{u}_1, \mathbf{u}_2, \mathbf{u}_3, \mathbf{v}$ are linearly independent over $\mathbb{R}$.

Remarks. The proof-by-contradiction method is preferred in this argument because of the fact that the definition for the notion of linear independence is not easy to use in a direct argument for the statement. Note that within this argument, the proof-by-contradiction argument is applied twice.