Proof methods

Direct

Theorem. Let $a \neq 0$, $b, c \in \mathbb{R}$. Then

$$ax^2 + bx + c = 0 \iff x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$$

Proof.

$$ax^2 + bx + c = 0 \iff x^2 + \frac{b}{a}x + \frac{c}{a} = 0 \quad (\text{since } a \neq 0)$$

$$\iff \left(x + \frac{b}{2a}\right)^2 - \left(\frac{b}{2a}\right)^2 + \frac{c}{a} = 0$$

$$\iff \left(x + \frac{b}{2a}\right)^2 = \left(\frac{b}{2a}\right)^2 - \frac{c}{a}$$

$$\iff x + \frac{b}{2a} = \pm\sqrt{\left(\frac{b}{2a}\right)^2 - \frac{c}{a}}$$

$$\iff x = -\frac{b}{2a} \pm \sqrt{\frac{b^2}{4a^2} - \frac{4ac}{4a^2}}$$

$$\iff x = -\frac{b}{2a} \pm \sqrt{\frac{b^2 - 4ac}{4a^2}}$$

$$\iff x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$$

$\square$

Theorem. Let A and B be sets. Then $A \wedge B \subseteq A \cup B$.

Proof. Suppose $x \in A \cap B$. Then

$$
\begin{aligned}
& x \in A \text{ and } x \in B && (\text{definition of } \cap) \\
\Rightarrow\ & x \in A && (\text{logical and}) \\
\Rightarrow\ & x \in A \text{ or } x \in B && (\text{logical or}) \\
\Rightarrow\ & x \in A \cup B && (\text{definition of } \cup)
\end{aligned}
$$

$\square$

Theorem. If $e, f \in A$ are both identity elements for $\circ$, then $e = f$. (i.e. the identity is unique)

Proof. Since e is an identity,

$$e \circ x = x \quad \text{for any } x \in A.$$

Choose $x = f$, we have

$$e \circ f = f.$$

Similarly, since f is an identity, we have

$$x \circ f = x \quad \text{for any } x \in A.$$

Choose $x = e$, we have

$$e \circ f = e.$$

Since we have $e = e \circ f = f$, we have $e = f$ as required.

$\square$

Theorem. Let A and B be finite sets.
Then $|A \cup B| = |A| + |B| - |A \cap B|$.

Proof.
$|A|$ counts all the elements in A.
$|B|$ counts all the elements in B.
However, we have counted the elements that are in both sets twice.
$|A \cap B|$ counts all the elements that are in both A and B.
Thus $|A \cup B| = |A| + |B| - |A \cap B|$ counts all the elements in A or B only once. $\square$

~~Counterexample~~.

Cases/exhaustion.

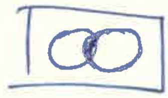
Theorem. $n^2 + 3n + 7$ is odd for all $n \in \mathbb{Z}$.

Proof. We can divide this into two cases:
i) n is even;
ii) n is odd.

i) If n is even, then $n = 2k$ for some $k \in \mathbb{Z}$.
Thus
$$\begin{aligned} n^2 + 3n + 7 &= (2k)^2 + 3(2k) + 7 \\ &= 4k^2 + 6k + 7 \\ &\cancel{= 2(2k^2 + 3k) + 7} \\ &= 2(2k^2 + 3k + 3) + 1, \end{aligned}$$
which is odd.

ii) If n is odd, then $n = 2k+1$ for some $k \in \mathbb{Z}$.

Thus
$$n^2+3n+7 = (2k+1)^2 + 3(2k+1) + 7$$
$$= 4k^2+10k+11$$
$$= 2(2k^2+5k+5)+1,$$
which is odd. $\square$



Counterexample.

Conjecture. For all sets A and B, we have
$$A \cap B \subset A \cup B.$$

Let $A = \{1\}$ and $B = \{1\}$.

Now $A \cap B = \{1\}$, and $A \cup B = \{1\}$.

Since $\{1\} \not\subset \{1\}$, the conjecture is false.

Contradiction.

Theorem. The square root of 2 is irrational.

Proof. Suppose to the contrary that $\sqrt{2} = \frac{m}{n}$, where $m, n \in \mathbb{Z}$ such that $\frac{m}{n}$ is expressed in its simplest terms.

Then we have
$$\sqrt{2} = \frac{m}{n}$$
$$\Rightarrow 2 = \left(\frac{m}{n}\right)^2$$
$$\Rightarrow 2 = \frac{m^2}{n^2}$$
$$\Rightarrow 2n^2 = m^2.$$

Thus m^2 is even, so m must be even.
So $m = 2k$ for some $k \in \mathbb{Z}$. Then

$$2n^2 = (2k)^2 = 4k^2$$
$$\Rightarrow \quad n^2 = 2k^2$$

So n^2 is even, so n must be even.
Say $n = 2j$, $j \in \mathbb{Z}$.
Now $\frac{m}{n} = \frac{2k}{2j} = \frac{k}{j}$ with $k < m$, $j < n$.
But we said $\frac{m}{n}$ was in its simplest terms.
This is a contradiction, so $\sqrt{2} \neq \frac{m}{n}$. $\square$

<u>Theorem</u>. The equation $x^7 + 3x^3 + 5$ has no rational roots.

<u>Proof</u>. Assume to the contrary that $x = \frac{p}{q}$ where $p, q \in \mathbb{Z}$ such that $\frac{p}{q}$ is in its simplest terms.
Then
$$\left(\frac{p}{q}\right)^7 + 3\left(\frac{p}{q}\right)^3 + 5 = 0$$
$$\Leftrightarrow \quad p^7 + 3p^3q^4 + 5q^7 = 0 \qquad (\times q^7)$$

There are four cases:

i) p & q both even. Then $\frac{p}{q}$ is not in simplest terms. Contradiction.

ii) p & q both odd. Then
$$p^7 + 3p^3q^4 + 5q^7 \text{ is odd. Contradiction}$$

iii) p is even, q is odd. Then
$$p(p^6 + 3p^2q^4) + 5q^7 \text{ is odd. Contradiction.}$$

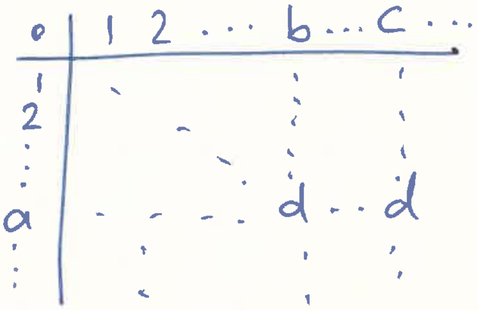
iv) p is odd, q is even. Then

$$p^7 + q(3p^3q^3 + 5q^6) \text{ is odd. Contradiction}$$

In all cases, we have a contradiction. Hence the equation has no rational roots. $\square$

<u>Theorem</u>. Every element in a group appears exactly once in each row of a group table.

<u>Proof</u>. Suppose to the contrary there is an element appearing twice in a row.



Now $a \circ b = d$ and $a \circ c = d$.

Hence $a \circ b = a \circ c$.

We know a^{-1} exists, because we have a group, so let

$$a^{-1} \circ (a \circ b) = a^{-1} \circ (a \circ c)$$

$$\Rightarrow (a^{-1} \circ a) \circ b = (a^{-1} \circ a) \circ c \qquad \text{(associativity)}$$

$$\Rightarrow e \circ b = e \circ c \qquad \text{(inverse)}$$

$$\Rightarrow b = c \qquad \text{(identity)}$$

So b and c are the same column, and d does not appear twice. $\square$

A similar argument works for columns.

This is called the Latin Square property.