Proof

Michael Cavaliere

Week 4

Class Content

What types of proof are there?

- Direct proof
- Proof by contradiction
- Proof by induction
- Proof by exhaustion
- Counterexample

Question 1

Prove that for $n \in \mathbb{Z}$, if n is even if and only if n^3 is even.

Solution Suppose that n is even, and let $n = 2k$ for some $k \in \mathbb{Z}$. It follows that $n^3 = (2k)^3 = 8k^3$. Since 8 is even, $8k^3$ is even, so n^3 is even.

Conversely, suppose that n is odd, and let $n = 2k + 1$ for some $k \in \mathbb{Z}$. It follows that

$$\begin{aligned} n^3 &= (2k+1)^3 \\ &= (2k+1)(4k^2+4k+1) \\ &= 8k^3 + 12k^2 + 6k + 1 \end{aligned}$$

Since $8k^3 + 12k^2 + 6k$ is even, $8k^3 + 12k^2 + 6k + 1$ is odd, so n^3 is odd.

Hence, n is even if and only if n^3 is even.

Question 2

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

Solution Suppose that $\sqrt[3]{2}$ is rational. This means it can be written in the form

$$\sqrt[3]{2} = \frac{m}{n}$$

for $m, n \in \mathbb{Z}$ with no common factors and $n \neq 0$. Cubing both sides gives

$$2 = \frac{m^3}{n^3} \implies m^3 = 2n^3$$

so m^3 is even. This implies that m is even. Let $m = 2k$ for some $k \in \mathbb{Z}$. This implies that

$$\begin{aligned} m^3 &= (2k)^3 = 8k^3 \\ \implies 8k^3 &= 2n^3 \\ \implies n^3 &= 4k^3 \end{aligned}$$

Since 4 is even, $4k^3$ is even, so n^3 is even. This implies that n is even. Since both m and n are even, 2 is a common factor, which is a contradiction to the assumption that m and n have no common factors. Hence, $\sqrt[3]{2}$ is irrational.

Question 3

Prove that $9^n - 1$ is divisible by 8 for every $n \in \mathbb{N}$.

Solution Let $P(n)$ be the statement above. When $n = 1$, $9^n - 1 = 9 - 1 = 8$, so $9^n - 1$ is divisible by 8, so $P(1)$ is true.

Suppose that $P(k)$ is true, so $9^k - 1$ is divisible by 8, for some $k \in \mathbb{N}$. Then,

$$\begin{aligned} 9^{k+1} - 1 &= 9^{k+1} - 9 + 8 \\ &= 9(9^k - 1) + 8 \end{aligned}$$

Since $9^k - 1$ is divisible by 8, $9(9^k - 1)$ is divisible by 8 and so $9(9^k - 1) + 8$ is divisible by 8. This implies that $9^{k+1} - 1$ is divisible by 8, so $P(k + 1)$ is true. Therefore, by induction, $P(n)$ is true for all $n \in \mathbb{N}$.

Additional Questions

1. For $a, b, c \in \mathbb{Z}$, prove that if a divides b and b divides c, then a divides c.

   Solution Let $a, b, c \in \mathbb{Z}$ and suppose that a divides b and b divides c. By definition, this means that there exists $m, n \in \mathbb{Z}$ such that $b = am$ and $c = bn$. By substituting, this implies that $c = (am)n = a(mn)$. Since $m, n \in \mathbb{Z}$, $mn \in \mathbb{Z}$ and so a divides c.

2. Prove that no square number ends in a 7.

   Solution For any integer $k \in \mathbb{Z}$, $k = 10m + n$ for $m, n \in \mathbb{Z}$ where $0 \leq n < 10$. Since

   $$\begin{aligned} k^2 &= (10m + n)^2 \\ &= 100m^2 + 20mn + n^2 \end{aligned}$$

   the final digit of k^2 is the same as the final digit of n^2. This shows that it suffices to show that no square number between 0 and 9 ends in a 7.

   $$\begin{aligned} 0^2 &= 0 \\ 1^2 &= 1 \\ 2^2 &= 4 \\ 3^2 &= 9 \\ &\vdots \\ 9^2 &= 81 \end{aligned}$$

   Hence, no square number ends in a 7.

3. A sequence is defined recursively by $a_1 = 6$, $a_2 = 27$ and $a_{n+2} = 6a_{n+1} - 9a_n$ for $n \in \mathbb{N}$. Prove that $a_n = 3^n(n+1)$ for all $n \in \mathbb{N}$.

Solution Let $P(n)$ be the statement above. Since $a_1 = 6 = 3^1(1+1)$, $P(1)$ is true. Since $a_2 = 27 = 3^2(2+1)$, $P(2)$ is true.

Suppose that $P(k)$ and $P(k+1)$ are true for $k \in \mathbb{N}$, so $a_k = 3^k(k+1)$ and $a_{k+1} = 3^{k+1}(k+2)$. By definition of a_{k+2},

$$\begin{aligned} a_{k+2} &= 6a_{k+1} - 9a_k \\ &= 6(3^{k+1}(k+2)) - 9(3^k(k+1)) \\ &= 2(3^{k+2})(k+2) - (3^{k+2})(k+1) \\ &= 3^{k+2}(2(k+2) - (k+1)) \\ &= 3^{k+2}(2k+4-k-1) \\ &= 3^{k+2}(k+3) \end{aligned}$$

so $P(k+1)$ is true. Therefore, by induction, $P(n)$ is true for all $n \in \mathbb{N}$.

Note that two base cases are needed and two inductive hypotheses are needed, because a_{k+2} is reliant on both a_k and a_{k+1}. This is a variation on induction, but hopefully you can see why it works!

4. Prove by contradiction that if $x \in \mathbb{Q}$ and $y \in \mathbb{R} \setminus \mathbb{Q}$, then $x + y \in \mathbb{R} \setminus \mathbb{Q}$.

Solution Let $x \in \mathbb{Q}$ and $y \in \mathbb{R} \setminus \mathbb{Q}$. Suppose that $x + y \notin \mathbb{R} \setminus \mathbb{Q}$, so $x + y \in \mathbb{Q}$. By definition, $x = \frac{m}{n}$ and $x + y = \frac{p}{q}$ for $m, n, p, q \in \mathbb{Z}$ with $n, q \neq 0$. Then,

$$y = (x+y) - x = \frac{p}{q} - \frac{m}{n} = \frac{pn}{qn} - \frac{mq}{nq} = \frac{pn - mq}{nq}$$

Since $m, n, p, q \in \mathbb{Z}$, $pn - mq \in \mathbb{Z}$ and $nq \in \mathbb{Z}$. Since $n, q \neq 0$, $nq \neq 0$. Hence, $y \in \mathbb{Q}$, which is a contradiction, so $x + y \notin \mathbb{Q}$ and so $x + y \in \mathbb{R} \setminus \mathbb{Q}$.

5. Is it true that if $x \in \mathbb{Q}$ and $y \in \mathbb{Q}$, then $x + y \in \mathbb{Q}$? Provide a proof or a counterexample.

Solution The statement is true. Let $x, y \in \mathbb{Q}$, so $x = \frac{m}{n}$ and $y = \frac{p}{q}$ for $m, n, p, q \in \mathbb{Z}$ with $n, q \neq 0$. Then,

$$x + y = \frac{m}{n} + \frac{p}{q} = \frac{mq}{nq} + \frac{pn}{qn} = \frac{mq + pn}{nq}$$

Since $m, n, p, q \in \mathbb{Z}$, $mq + pn \in \mathbb{Z}$ and $nq \in \mathbb{Z}$. Since $n, q \neq 0$, $nq \neq 0$. Hence, $x + y \in \mathbb{Q}$.

6. Is it true that if $x \in \mathbb{R} \setminus \mathbb{Q}$ and $y \in \mathbb{R} \setminus \mathbb{Q}$, then $x + y \in \mathbb{R} \setminus \mathbb{Q}$? Provide a proof or a counterexample.

Solution The statement is false. Let $x = \sqrt{2}$ and $y = -\sqrt{2}$, so $x, y \in \mathbb{R} \setminus \mathbb{Q}$. Then, $x + y = 0$ so $x + y \in \mathbb{Q}$.

7. All cows are the same colour.

Proof. Let $P(n)$ be the statement that any n cows are all the same colour for $n \in \mathbb{N}$. Since one cow is always the same colour as itself, $P(1)$ is true.

Suppose that $P(k)$ is true for some $k \in \mathbb{N}$, so any k cows are all the same colour. Let C be a set of $k+1$ cows. If one cow c_1 is removed from C, then $C \setminus \{c_1\}$ is a set of k cows, so by the inductive hypothesis all cows in $C \setminus \{c_1\}$ are the same colour. Similarly, if a different cow c_2 is removed from C, then $C \setminus \{c_2\}$ is a set of k cows, so by the inductive hypothesis all cows in $C \setminus \{c_2\}$ are the same colour.

Since $C \setminus \{c_1, c_2\} \subseteq C \setminus \{c_1\}$ and $C \setminus \{c_1, c_2\} \subseteq C \setminus \{c_2\}$, the cows in $C \setminus \{c_1, c_2\}$ are the same colour as the cows in $C \setminus \{c_1\}$ and the cows in $C \setminus \{c_2\}$. This implies that the cows in $C \setminus \{c_1\}$ and $C \setminus \{c_2\}$ are all the same colour.

Since $C = (C \setminus \{c_1\}) \cup (C \setminus \{c_2\})$, this implies that all cows in C are the same colour, so $P(k+1)$ is true.

Hence, by induction, all cows are the same colour. $\square$

This result clearly is not true, so what is the mistake in the proof?

Solution The proof of the inductive step assumes that $|C| \geq 3$, because it assumes that c_1 and c_2 can be removed from C and $C \setminus \{c_1, c_2\}$ is not empty. This means that it cannot be used to go from the base case $P(1)$ to $P(2)$.

Thinking about the argument above in the case that $k = 1$, if we assume $P(1)$ is true then let $C = \{c_1, c_2\}$ be a set of $k+1$ cows. It is clear that all cows in $C \setminus \{c_1\}$ are the same colour and all cows in $C \setminus \{c_2\}$ are the same colour. However, $C \setminus \{c_1, c_2\} = \varnothing$ and so the argument above cannot be used to show that the cows in $C \setminus \{c_1\}$ and $C \setminus \{c_2\}$ are the same colour.

The moral of this example is that it is very important to make sure that the argument in your inductive step works for all $k \in \mathbb{N}$.