Class 1

January 9, 2024

Shorthand and Symbols

$\wedge$: And
$\vee$: Or
$\neg$: Not, negation
$\forall$: For all
$\exists$: There exists
$A \implies B$: A implies B
$A \impliedby B$: A implied by B
$A \iff B$: A if and only if B, A, B are logically equivalent
iff: If and only if
$A \not\Rightarrow B$: A does not imply by B
$A \not\Leftarrow B$: A is not implied by B
$A \Rightarrow\Leftarrow B$: A and B are contradictory
$P!$: Statement P is a contradiction
s.t.: Such that
$\therefore$: Therefore
$\mathbb{N}$: Natural numbers
$\mathbb{Z}$: Integers
$\mathbb{Q}$: Rational numbers
$\mathbb{R}$: Real numbers
$\mathbb{C}$: Complex numbers
$\mathbb{Z}^+$: Positive integers
$\mathbb{R}^+$: Positive real numbers
$\mathbb{R}^n$: n dimensional real space
$\mathbb{R}^{n\times m}$: $n \times m$ matrices with real entries
pf : Proof
$\square$: End of proof
$\blacksquare$: End of proof
Q.E.D. : End of proof
WTS : Want to show
NTS : Need to show
$a|b$: a divides b or b is divisible by a

Proof Methods

The best proofs are as

1. Unambiguous
2. Simple
3. Explanatory
4. Clear

as possible. A correct proof will get full credit, but the best proof will also be elegant.

Direct Proof

Prove the desired claim by a sequence of logical statements.

Example

Prove that if $3x + 1$ is odd and x is an integer, then x must be even.

pf

If $3x + 1$ is odd, then $3x + 1 = 2n + 1$ for some integer n.

$$3x + 1 = 2n + 1$$

$$3x = 2n$$

$$x = \frac{2n}{3} = 2\left(\frac{n}{3}\right)$$

As x is an integer, $\frac{n}{3}$ must be as well, thus x is an even integer. ■

Proof By Contrapositive

Prove the desired claim by proving the contrapositive of the original claim. This works since the contrapositive is logically equivalent to the original claim. Suppose we wish to prove

$$P \implies Q$$

The contrapositive is

$$\neg Q \implies \neg P$$

Example

Prove that if $3x + 1$ is odd and x is an integer, then x must be even.

pf

The contrapositive of this claim is if x is an odd integer, then $3x + 1$ must be even. If x is odd, then $x = 2n + 1$ for some $n \in \mathbb{Z}$.

$$3\left(2n + 1\right) + 1 = 6n + 3 + 1$$

$$= 6n + 4 = 2\left(3n + 2\right)$$

Since $3n + 2 \in \mathbb{Z}$, then $3x + 1$ is even. Thus the contrapositive must also hold. ■
Was the first proof of the second proof more elegant? Which was easier to follow?

Proof By Contradiction

Suppose the claim were false. Show this leads to absurd results.

Example

Prove $\sqrt{2}$ is irrational

pf

Suppose $\sqrt{2}$ were rational. Then there would exist $a, b \in \mathbb{Z}$ st $b \neq 0$ and $\frac{a}{b}$ is fully reduced.

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

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

$$2b^2 = a^2$$

As a, b are integers, this implies a^2 is divisible by 2, as is a. In other words, $a = 2c$ for some $c \in \mathbb{Z}$.

$$2b^2 = (2c)^2$$

$$2b^2 = 4c^2$$

$$b^2 = 2c^2$$

This implies b^2 is also divisible by 2 and therefore b is as well. As a, b are both divisible by 2, this contradicts our earlier assumption that $\frac{a}{b}$ is fully simplified! Thus to avoid contradiction, we must allow $\sqrt{2}$ to be irrational. ■

Proof By Induction

These proofs work best when we have a claim that holds over some countable set (usually the natural numbers or a subset of the natural numbers). Start by taking the lowest number the claim holds for. Prove the claim for this number. This is called the base case. Now, prove that if the claim holds for k, it must also hold for $k+1$. This is the induction step. If both the base case and induction step hold, so must the original claim.

Example

Prove the formula for the triangle numbers

$$T_n = \sum_{i=1}^{n} i = \frac{n(n+1)}{2}$$

pf

First start with the base case when $n = 1$.

$$\sum_{i=1}^{1} i = 1 = \frac{2}{2} = \frac{1(1+1)}{2}$$

Now that the base case holds, we will perform the induction step. Suppose the formula for T_n holds whenever $1 \leq n \leq k$. This implies

$$T_k = \sum_{i=1}^{k} i = \frac{k(k+1)}{2}$$

If we add $k+1$ to both sides, we get

$$\sum_{i=1}^{k} i + (k+1) = \frac{k(k+1)}{2} + (k+1)$$

$$\sum_{i=1}^{k+1} i = \frac{k(k+1)}{2} + (k+1) = (k+1)\left(\frac{k}{2} + 1\right) = (k+1)\left(\frac{k}{2} + \frac{2}{2}\right)$$

$$\sum_{i=1}^{k+1} i = \frac{(k+1)(k+2)}{2}$$

As we expected. As both the base case and induction step holds, we have proven our claim by induction. ■

Practice Problems

Try these problems on your own for practice. What proof methods did you use?

1. Show $\sum_{i=1}^{n} i^2 = \frac{n(n+1)(2n+1)}{6}$ for $n \in \mathbb{Z}^+$.
2. Show $n^3 - n$ is divisible by 6 for $n \in \mathbb{Z}^+$.
3. Show $3n + 5$ is even if and only if n is odd.
4. Show there are infinitely many prime numbers.
5. Show $\sqrt{p}$ is irrational for any prime number p.
6. Show x is divisible by 9 if and only if the sum of its digits is divisible by 9.
7. If p,q are rational, show $p + q$ and $p - q$ are rational. Further show if $q \neq 0$, then $\frac{p}{q}$ is rational.

Practice Solutions

Here are some possible solutions. Other proofs also exist.

1)

A proof by induction is helpful here. For the base case, consider $n = 1$.

$$\sum_{i=1}^{1} i^2 = 1 = \frac{1 * 2 * 3}{6} = \frac{1\,(1+1)\,(2*1+1)}{6}$$

For the induction step, suppose $\sum_{i=1}^{n} i^2 = \frac{n(n+1)(2n+1)}{6}$. Then

$$\sum_{i=1}^{n+1} i^2 = \sum_{i=1}^{n} i^2 + (n+1)^2 = \frac{n\,(n+1)\,(2n+1)}{6} + (n+1)^2$$

$$= \frac{n\,(n+1)\,(2n+1)}{6} + \frac{6\,(n+1)^2}{6} = \frac{(n+1)}{6}\,(n\,(2n+1) + 6\,(n+1))$$

$$= \frac{(n+1)}{6}\left(2n^2 + n + 6n + 6\right) = \frac{(n+1)}{6}\left(2n^2 + 7n + 6\right)$$

$$= \frac{(n+1)}{6}\,(2n+3)\,(n+2) = \frac{(n+1)\,(n+2)\,(2\,(n+1)+1)}{6}$$

■

2)

There are a few ways to do this. Which proof is a better proof? First, I will show a direct proof:

$$n^3 - n = n\left(n^2 - 1\right) = n\,(n+1)\,(n-1)$$

we know $2|n$ or $2|n+1$ $\forall n \in \mathbb{N}$. Thus $2|n^3 - n$. We also know $3|n$, $3|n+1$, or $3|n-1$ $\forall n \in \mathbb{N}$. Thus $3|n^3 - n$. As $2|n^3 - n$ and $3|n^3 - n$, then $\mathrm{LCM}\,(2,3) = 6$ also divides $n^3 - n$, thus $6|n^3 - n$. ■

Now, let's do the proof by induction. Base case: $n = 1$:

$$1^3 - 1 = 0$$

and $6|0$ as $0 = 6 * 0$. Induction step: Suppose $6|n^3 - n$. Consider

$$(n+1)^3 - (n+1) = n^3 + 3n^2 + 3n + 1 - n - 1 = n^3 + 3n^2 + 3n - n$$

$$= \left(n^3 - n\right) + 3n\,(n+1)$$

As $2|n$ or $2|n+1$, then $2|n\,(n+1)$. Thus $2|3n\,(n+1)$. As $3|3n\,(n+1)$ as well, then $6|3n\,(n+1)$. By the induction hypothesis, $6|\left(n^3 - n\right)$. So $6|\left(n^3 - n\right) + 3n\,(n+1)$ and therefore

$6|\,(n+1)^3 - (n+1)$ as desired. ■

3)

We will use a combination of direct proof and proof by contrapositive. First, let's show $3n + 5$ is even if n is odd. Suppose n is odd. Then

$$n = 2k + 1$$

for some $k \in \mathbb{Z}$. Thus

$$3n + 5 = 3\,(2k + 1) + 5 = 6k + 3 + 5 = 6k + 8 = 2\,(3k + 4)$$

as $3k + 4 \in \mathbb{Z}$, then $3n + 5$ is even. To show n must be odd if $3n + 5$ is even, we will show the contrapositive holds. The contrapositive states if n is even, $2n + 5$ is odd. Suppose n is even. Then

$$n = 2k$$

for some $k \in \mathbb{Z}$.Thus

$$3n + 5 = 3\,(2k) + 5 = 6k + 4 + 1 = 2\,(3k + 2) + 1$$

as $3k + 2 \in \mathbb{Z}$, then $3n + 5$ is odd. As we have proven the contrapositive, we know that the original statement also holds. ■

4)

Here, a proof by contradiction helps. Suppose there are finitely many primes. We will number them $p_1, p_2, \ldots, p_n$. Then

$$p_i | \prod_{k=1}^{n} p_k$$

in other words, each prime number divides the product of all of the primes. As a prime number must be larger than 1, then

$$p_i \not| \prod_{k=1}^{n} (p_k) + 1$$

As there are no primes in our list that divide $\prod_{k=1}^{n} (p_k) + 1$, then $\prod_{k=1}^{n} (p_k) + 1$ contains no prime factors! This is a contradiction as every integer greater than one contains a unique prime factorization. Thus to avoid contradiction there must be infinitely many prime numbers.

5)

We will do a proof by contradiction using the same reasoning as the $\sqrt{2}$ irrationality proof.

Suppose $\sqrt{p}$ were rational. Then there would exist $a, b \in \mathbb{Z}$ st $b \neq 0$ and $\frac{a}{b}$ is fully reduced.

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

$$p = \frac{a^2}{b^2}$$

$$pb^2 = a^2$$

As a, b are integers, this implies a^2 is divisible by p, as is a. In other words, $a = pc$ for some $c \in \mathbb{Z}$.

$$pb^2 = (pc)^2$$

$$pb^2 = p^2c^2$$

$$b^2 = pc^2$$

This implies b^2 is also divisible by p and therefore b is as well. As a, b are both divisible by p, this contradicts our earlier assumption that $\frac{a}{b}$ is fully simplified! Thus to avoid contradiction, we must allow $\sqrt{2}$ to be irrational. ■

6)

Suppose the x is an n digit number of the form $x = a_n a_{n-1} \dots a_0$ where each $a_i \in \{0, 1, 2, \dots, 9\}$, and each a_i represents a digit of x. Then we can write x as

$$x = \sum_{i=0}^{n} a_i \left(10\right)^i$$

For convenience, we will also define the sum of the digits as

$$s = \sum_{i=0}^{n} a_i$$

Then

$$x - s = \sum_{i=0}^{n} a_i \left(10\right)^i - \sum_{i=0}^{n} a_i = \sum_{i=0}^{n} a_i \left(\left(10\right)^i - 1\right)$$

As $\left(10\right)^i - 1 = 999 \dots 999$, then $9 | \left(10\right)^i - 1$ for each $i \geq 0$. As such, $9 | a_i \left(\left(10\right)^i - 1\right)$ for each i and thus $9 | x - s$. This implies that $\frac{x}{9}$ and $\frac{s}{9}$ have the same remainder. If $9|x$, then the remainder is 0, so $9|s$. And similarly, if $9|s$, then the remainder is 0, so $9|x$. $\blacksquare$

7)

Suppose $p = \frac{a}{b}$, $q = \frac{c}{d}$ for $a, b, c, d \in \mathbb{Z}$ and with $b, d \neq 0$. Then

$$p + q = \frac{a}{b} + \frac{c}{d} = \frac{ad}{bd} + \frac{bc}{bd} = \frac{ab + bc}{bd}$$

as $ab + bc, bd \in \mathbb{Z}$ and $bd \neq 0$, then $p + q \in \mathbb{Q}$. Similarly,

$$p - q = \frac{a}{b} - \frac{c}{d} = \frac{ad}{bd} - \frac{bc}{bd} = \frac{ab - bc}{bd}$$

as $ab - bc, bd \in \mathbb{Z}$ and $bd \neq 0$, then $p - q \in \mathbb{Q}$. If we add the restriction that $q \neq 0$, then $c \neq 0$. Thus

$$\frac{p}{q} = \frac{\left(\frac{a}{b}\right)}{\left(\frac{c}{d}\right)} = \frac{a}{b} * \frac{d}{c} = \frac{ad}{bc}$$

as $ad, bc \in \mathbb{Z}$ and $bc \neq 0$, then $\frac{p}{q} \in \mathbb{Q}$. $\blacksquare$