Direct proof strategy: define a specific $y \in S$ and prove $P(y)$ holds.

Ex: ① Prop'n There exists an even integer $n \in \mathbb{N}$ that can be written as the sum of two primes in two distinct ways.

Pf: Consider $n = 10$. Then n is even and moreover $10 = 5+5 = 7+3$. Since $3, 5, 7$ are prime, the claim is proved. (Note: $24 = 19+5 = 17+7$ works too...)

Indirect proof strategy: Assume $\neg(\exists x \in S)\, P(x)$ (equiv: $(\forall x \in S) \neg P(x)$) and derive a contradiction.

Ex: ② Fix $n \in \mathbb{N}$ and $a_1, \dots, a_n \in \mathbb{R}$. Then there is a $k \in \{1, 2, \dots, n\}$ s.t. a_k is at least as large as the average (mean) of $a_1, \dots, a_n$

secretly a $\forall \exists$ claim, we focus on $\exists$ part

i.e.:

$$(\exists k \in [n]) \left(a_k \geq \frac{1}{n}(a_1 + a_2 + \cdots + a_k) \right)$$

$$\frac{1}{n} \sum_{i=1}^{n} a_i$$

Pf:- Sps not, toward a contradiction.
- that is, sps that

$$(\forall k \in [n])\left(a_k < \frac{1}{n}(a_1 + \cdots + a_n)\right)$$

- for simplicity, let $s = a_1 + a_2 + \cdots + a_n$
- So our assumption is: $(\forall k \in [n])(a_k < \frac{s}{n})$
- but then:

$$\begin{aligned} s &= a_1 + a_2 + \cdots + a_n && \text{(defn of } s\text{)} \\ &< \underbrace{\frac{s}{n} + \frac{s}{n} + \cdots + \frac{s}{n}}_{n \text{ times}} && \text{(by our assumption)} \\ &= n \cdot \frac{s}{n} = s \end{aligned}$$

This shows $s < s$, a contradiction.
Hence our assumption was <u>false</u>, and so the prop'n is <u>true</u>.

<u>Universal Claims</u>

<u>General form:</u> $(\forall x \in S)P(x)$

<u>Direct</u> <u>strategy</u>: - Let $x \in S$ be arbitrary but fixed. Prove $P(x)$.

<u>Ex</u>: ① <u>Prop'n</u> $(\forall x, y \in \mathbb{R})\left(xy \leq \left(\frac{x+y}{2}\right)^2\right)$

<u>Pf</u>: - Fix $x, y \in \mathbb{R}$.

- then: $(x-y)^2 \geq 0$ (squares always ≥ 0)
- i.e. $x^2 - 2xy + y^2 \geq 0$

$\Rightarrow x^2 + y^2 \geq 2xy$

$\Rightarrow x^2 + 2xy + y^2 \geq 4xy$ (+2xy to both sides)

i.e. $(x+y)^2 \geq 4xy$

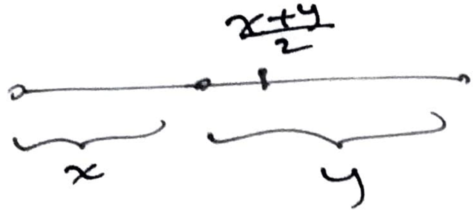
$\Rightarrow \frac{(x+y)^2}{4} \geq xy$

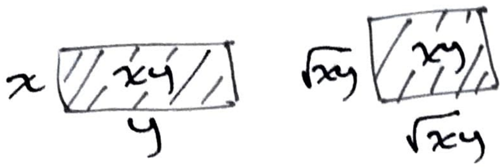
$\Rightarrow \left(\frac{x+y}{2}\right)^2 \geq xy$, as desired.

Since $x, y \in \mathbb{R}$ were arbitrary the claim is proved. ✓

<u>Aside</u>: prop'n is one version of the "AM-GM" inequality.

- <u>arithmetic</u> <u>mean</u> (AM) of x, y is $\frac{x+y}{2}$
- <u>geometric</u> <u>mean</u> (GM) of x, y is $\sqrt{xy}$





prop'n says (for $x,y \geq 0$) that

$$\sqrt{xy} \leq \frac{x+y}{2} \quad \text{i.e. } GM \leq AM.$$

Indirect strategy: Assume $\neg(\forall x \in S)P(x)$ (equiv: $(\exists x \in S)\neg P(x)$) and derive a contradiction.

Ex: ② $\sqrt{2}$ is irrational, that is:

$$(\forall a,b \in \mathbb{Z})\left(\frac{a}{b} \neq \sqrt{2}\right)$$

Pf: – Sps not, that is, sps $\exists a,b \in \mathbb{Z}$ s.t. $\frac{a}{b} = \sqrt{2}$

– we may assume a,b share no common factors, since if they did we could 'cancel' these factors to get $a', b' \in \mathbb{Z}$ without common factors s.t. $\frac{a'}{b'} = \sqrt{2}$.

Now: – since $\frac{a}{b} = \sqrt{2}$

we have $a = \sqrt{2}\, b$

$\Rightarrow a^2 = 2b^2$

hence a^2 is even. It follows that a is even (why?)

– hence $\exists k \in \mathbb{Z}$ s.t. $a = 2k$

– then $a^2 = 4k^2$

– giving $2b^2 = 4k^2$

– hence $b^2 = 2k^2$

– we now see that b^2, and hence b, is also even.

– so **both** a, b are even: hence they share a factor of 2

– a contradiction as a, b share no common factors!

– the prop'n follows.

Conditional Claims

General form: $P \Rightarrow Q$

Three strats: ① Direct: Assume P holds, prove Q

② Contrapositive: Prove $\neg Q \Rightarrow \neg P$, i.e. assume $\neg Q$ and prove $\neg P$

③ Indirect Assume $\neg(P \Rightarrow Q)$ (equiv: $P \wedge \neg Q$) and derive contradiction

② and ③ often similar in practice

Ex ① (Direct) Let $O = \{\ldots -5, -3, -1, 1, 3, 5, \ldots\}$ denote the set of all odd integers.

Prop'n $(\forall n \in \mathbb{Z})(n \in O \Rightarrow n^2 - 1$ is divisible by $4)$

i.e. $(\forall n \in \mathbb{Z})(n \in O \Rightarrow (\exists k \in \mathbb{Z})(n^2 - 1 = 4k))$

Pf: (overall this is a universal claim, so we begin as usual)

- Fix $n \in \mathbb{Z}$

(now we deal w/ the conditional)

- Assume $n \in O$.
(allowed to do this since if $n \notin O$ the conditional claim holds vacuously)
- hence $\exists k \in \mathbb{Z}$ s.t. $n = 2k+1$.
- hence $n^2 = (2k+1)^2 = 4k^2+4k+1$

$$\Rightarrow \quad n^2 - 1 = 4k^2+4k$$
$$= 4(k^2+k)$$
$$= 4M \quad (\text{where } M = k^2+k)$$

hence n^2-1 is divisible by 4.
- since $n \in \mathbb{Z}$ was arbitrary, the claim is proved. ✓

Ex ② (contrapositive). Let $E = \{\ldots -4, -2, 0, 2, 4, \ldots\}$

Prop'n $(\forall m, n \in \mathbb{Z})(mn \in E \Rightarrow ((m \in E) \vee (n \in E)))$

Pf: - fix $m, n \in \mathbb{Z}$..
(we argue the conditional by contrapositive)
- assume $\neg(m \in E \vee n \in E)$
i.e. $m \notin E \wedge n \notin E$.
- then m, n are both odd, i.e.
$\exists k, \ell \in \mathbb{Z}$ s.t. $m = 2k+1$
$n = 2\ell+1$

- so: $mn = (2k+1)(2\ell+1)$

$$= 4k\ell + 2k + 2\ell + 1$$
$$= 2(2k\ell + k + \ell) + 1$$
$$= 2N + 1 \quad (\text{where } N = 2k\ell + k + \ell)$$

- hence $m \cdot n$ is odd, i.e. $mn \notin E$.
- we've proved

$$(m \notin E \wedge n \notin E) \Rightarrow mn \notin E$$

i.e. $\neg(m \in E \vee n \in E) \Rightarrow \neg(mn \in E)$

- by contrapositive we've proved

$$mn \in E \Rightarrow m \in E \vee n \in E$$

- since $m, n \in \mathbb{Z}$ were arbitrary, claim is proved

---

<u>Ex 3</u> (Indirect)

<u>Prop'n</u> $(\forall x \in \mathbb{R})(x > 0 \Rightarrow x + \frac{1}{x} \geq 2)$

<u>Pf</u>: - fix $x \in \mathbb{R}$

- Sps $\underset{P}{x > 0}$ but $\underset{\neg Q}{x + \frac{1}{x} < 2}$

$\Rightarrow x^2 + 1 < 2x$ (inequality doesn't flip since $x > 0$)

$\Rightarrow x^2 - 2x + 1 < 0$

$\Rightarrow (x-1)^2 < 0$.

a contradiction, as squares are always ≥ 0.

- hence we must have

$$x > 0 \Rightarrow x + \frac{1}{x} \geq 2.$$

- since x was arbitrary, claim is proved.

Biconditional claims

General form: $P \Leftrightarrow Q$

Strategy: Prove $P \Rightarrow Q$ and $Q \Rightarrow P$

Ex Prop'n An integer is even iff its square is even, i.e.

$$(\forall n \in \mathbb{Z})(n \in E \Leftrightarrow n^2 \in E)$$

Pf: - fix $n \in \mathbb{Z}$

($\Rightarrow$) - Assume $n \in E$

- then $\exists k \in \mathbb{Z}$ s.t. $n = 2k$

- then $n^2 = 4k^2$
$$= 2(2k^2)$$
$$= 2M \quad (\text{where } M = 2k^2)$$

- hence n^2 is even, i.e. $n \in E$. ✓

($\Leftarrow$) To prove $n^2 \in E \Rightarrow n \in E$ we show the contrapositive: $n \notin E \Rightarrow n^2 \notin E$.

- So spr $n \notin E$.
- then n is odd, i.e. $\exists k \in \mathbb{Z}$ s.t. $n = 2k+1$
- hence $n^2 = (2k+1)^2$
$$= 4k^2 + 4k + 1$$
$$= 2(2k^2 + 2k) + 1$$
$$= 2N + 1 \quad (\text{where } N = 2k^2 + 2k)$$

hence n^2 is odd, so $n^2 \notin E$.

- we've shown (by contrapositive) $n^2 \in E \Rightarrow n \in E$.

Thus: $n \in E \Leftrightarrow n^2 \in E$

- since n was arbitrary, prop'n is proved ✓