**Theorem 20** *For every integer* $n$, *we have that* $6 \mid n$ *iff* $2 \mid n$ *and* $3 \mid n$.

PROOF: Let $n$ be an arbitrary integer.

($\Rightarrow$) $6 \mid n$ Then $2 \mid n \wedge 3 \mid n$.

($\Leftarrow$) Assume $\underline{2 \mid n}$ and $\underline{3 \mid n}$. $n = 3\ell$ for some int. $\ell$

$n = 2k$ for some int. $k$

Consider

$$6(k - \ell) = 6k - 6\ell = 3n - 2n = n$$

Hence $6 \mid n$. $\square$

$$15 \mid n \overset{?}{\Longleftrightarrow} (3 \mid n \wedge 5 \mid n)$$

$\boxed{?}$ Can we generalise: $30 \mid n \overset{?}{\Longleftrightarrow} (2 \mid n \wedge 3 \mid n \wedge 5 \mid n)$

$$(a_1 \cdots a_k) \mid n \overset{?}{\Longleftrightarrow} (a_1 \mid n \wedge \ldots \wedge a_k \mid n)$$

# Existential quantification

Existential statements are of the form

> **there exists** an individual $x$ in the universe of discourse for which the property $P(x)$ holds

or, in other words,

> **for some** individual $x$ in the universe of discourse, the property $P(x)$ holds

or, in symbols,

$$\boxed{\exists x.\, P(x)}$$

implication

forall $n$

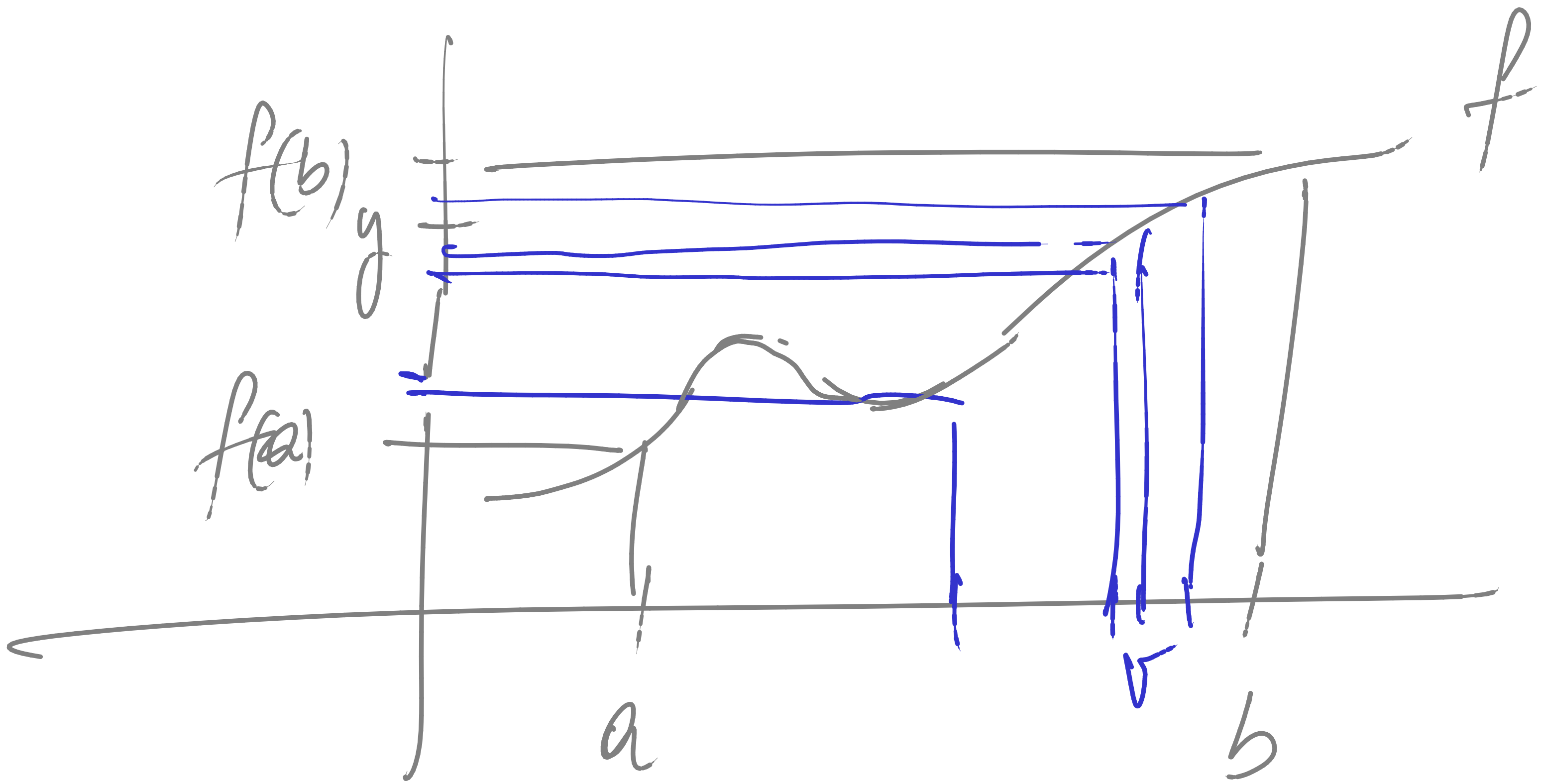
**Example:** The Pigeonhole Principle.

Let $n$ be a positive integer. If $n + 1$ letters are put in $n$ pigeonholes then there will be a pigeonhole with more than one letter.

existential

**Theorem 21 (Intermediate value theorem)** *Let $f$ be a real-valued continuous function on an interval $[a, b]$. For every $y$ in between $f(a)$ and $f(b)$, there exists $v$ in between $a$ and $b$ such that $f(v) = y$.*

**Intuition:**



**The main proof strategy for existential statements:**

To prove a goal of the form

$$\exists x.\, P(x)$$

find a ***witness*** for the existential statement; that is, a value of $x$, say $w$, for which you think $P(x)$ will be true, and show that indeed $P(w)$, i.e. the predicate $P(x)$ instantiated with the value $w$, holds.

**Proof pattern:**

In order to prove

$$\exists x.\, P(x)$$

1. Write: $\mathrm{Let}\ w = \ldots$ (the witness you decided on).
2. Provide a proof of $P(w)$.

**Scratch work:**

Before using the strategy

| Assumptions | Goal |
| --- | --- |
| | $\exists x.\, P(x)$ |
| $\vdots$ | |

After using the strategy

| Assumptions | Goals |
| --- | --- |
| | $P(w)$ |
| $\vdots$ | |

$w = \ldots$ (the witness you decided on)

**Proposition 22** *For every positive integer* $k$*, there exist natural numbers* $i$ *and* $j$ *such that* $4 \cdot k = i^2 - j^2$*.*

PROOF: $\forall k$ pos. int. $\exists$ nat. $i, j$. $4k = i^2 - j^2$.

Let $k$ be arbitrary.

RTP: $\exists$ nat $i, j$. $4k = i^2 - j^2$.

Take as witnesses $i = k+1$ and $j = k-1$

Then $(k+1)^2 - (k-1)^2 = \cdots = 4k$

Hence we are done. $\square$

| k | i | j |
|---|---|---|
| 1 | 2 | 0 |
| 2 | 3 | 1 |
| 3 | 4 | 2 |
| 4 | ... | |

Assumptions

Goal

$G$

$\exists x.\, P(x)$ ... let $x_0$ be such that $P(x_0)$

**The use of existential statements:**

To use an assumption of the form $\exists x.\, P(x)$, introduce a new variable $x_0$ into the proof to stand for some individual for which the property $P(x)$ holds. This means that you can now assume $P(x_0)$ true.

$d \mid k \overset{\text{def}}{\iff} \exists \text{ int. } j \,.\, d.j = k.$

**Theorem 24** *For all integers* $l$, $m$, $n$, *if* $l \mid m$ *and* $m \mid n$ *then* $l \mid n$.

PROOF:

$$\forall \text{ int. } l, m, n.$$
$$(\exists \text{ int } i.\ i.l = m \wedge \exists \text{ int } j.\ j.m = n)$$
$$\implies (\exists \text{ int. } k.\ k.l = n)$$

Let $l, m, n$ be arbitrary integers.

Assume ① $\exists i.\ i.l = m \implies i_0.l = m$ for some int $i_0$

② $\exists j.\ j.m = n \implies j_0.m = n$ for some int $j_0$

RTP: $\exists k.\ k.l = n$

Let $k = j_0.i_0$ Then

$k.l = \cdots = n$

So we are done $\square$

# Unique existence

The notation

$$\exists!\, x.\, P(x)$$

stands for

the *unique existence* of an $x$ for which the property $P(x)$ holds .

That is,

$$\overbrace{\exists x.\, P(x)}^{\text{existence}} \;\wedge\; \underbrace{\Big(\forall y.\, \forall z.\, \big(P(y) \wedge P(z)\big) \implies y = z\Big)}_{\text{uniqueness.}}$$

# Disjunction

Disjunctive statements are of the form

$$\boxed{P \text{ or } Q}$$

or, in other words,

$$\boxed{\text{either } P,\ Q, \text{ or both hold}}$$

or, in symbols,

$$\boxed{P \vee Q}$$

**The main proof strategy for disjunction:**

To prove a goal of the form

$$P \vee Q$$

you may

1. try to prove $P$ (if you succeed, then you are done); or
2. try to prove $Q$ (if you succeed, then you are done); otherwise
3. break your proof into cases; proving, in each case, either $P$ or $Q$.

**Proposition 25** *For all integers* $n$, *either* $n^2 \equiv 0 \pmod 4$ *or* $n^2 \equiv 1 \pmod 4$.

PROOF: $\forall$ int $n$. $\left(n^2 \equiv 0 \pmod 4 \vee n^2 \equiv 1 \pmod 4\right)$

Let $n$ be an arbitrary integer.

RTP $n^2 \equiv 0 \pmod 4$ or $n^2 \equiv 1 \pmod 4$

Try to show $n^2 \equiv 0 \pmod 4$ ———— oops!

Try to show $n^2 \equiv 1 \pmod 4$ ———— oops!

Consider two cases: (1) $n$ is even.

(2) $n$ is odd.

N.B. These cover all possibilities for $n$.

Case 1: $n$ is even, that is of the form $2k$ for some int. $k$.

Then $n^2 = (2k)^2 = 4 \underbrace{k^2}_{\text{integer}}$

Hence $n^2 \equiv 0 \pmod 4$

Case 2 $n$ is odd, that is of the form $2k+1$ for some int $k$.

Then $n^2 = (2k+1)^2 = 4k^2 + 4k + 1 = 4\overbrace{(k^2+k)}^{\text{integer}} + 1$

Hence $n^2 \equiv 1 \pmod 4$.

$\square$

Assumptions

⋮

$P_1 \vee P_2$

Goal

$Q$

**The use of disjunction:**

To use a disjunctive assumption

$$P_1 \ \vee \ P_2$$

to establish a goal $Q$, consider the following two cases in turn: $(i)$ assume $P_1$ to establish $Q$, and $(ii)$ assume $P_2$ to establish $Q$.

**Scratch work:**

Before using the strategy

| Assumptions | Goal |
| --- | --- |
| | $Q$ |
| $\vdots$ | |
| $P_1 \vee P_2$ | |

After using the strategy

| Assumptions | Goal | Assumptions | Goal |
| --- | --- | --- | --- |
| | $Q$ | | $Q$ |
| $\vdots$ | | $\vdots$ | |
| $P_1$ | | $P_2$ | |

**Proof pattern:**

In order to prove $Q$ from some assumptions amongst which there is

$$P_1 \vee P_2$$

write: We prove the following two cases in turn: (i) that assuming $P_1$, we have $Q$; and (ii) that assuming $P_2$, we have $Q$. Case (i): Assume $P_1$. and provide a proof of $Q$ from it and the other assumptions. Case (ii): Assume $P_2$. and provide a proof of $Q$ from it and the other assumptions.