Theorem 19 *For every integer n, we have that $6 \mid n$ iff $2 \mid n$ and $3 \mid n$.*

PROOF: Let n be an integer.

($\Rightarrow$) ...

($\Leftarrow$) ($2 \mid n$ and $3 \mid n$) $\Rightarrow$ $6 \mid n$.

Assume ① $2 \mid n$; That is, $n = 2i$ for int i

and ② $3 \mid n$; That is, $n = 3j$ for int j

RTP: $6 \mid n$; That is, $n = 6k$ for int k.

From ① and ②, $2i = 3j$ Then $i = \frac{3j}{2}$ int.

$\boxed{\text{Since 2 does divide 3 Then it must divide } j.}$

So $j = 2k$ for an int. k and hence $n = 3j = 3 \cdot 2 \cdot k$
$= 6 \cdot k$ as required

---

(1) $n = 2i$ (i int)
(2) $n = 3j$ (j int) $\overset{?}{\Longrightarrow}$ $n = 6k$ (k int)

scratch work

(1) $\Rightarrow 3n = 6i$
(2) $\Rightarrow 2n = 6j$ $\Longrightarrow$ $n = 3n - 2n = 6i - 6j = 6(i-j)$

$\boxtimes$

$$(2 \mid n \wedge 3 \mid n) \Leftrightarrow 6 \mid n$$

?

$\boxed{?}$ $\forall a, b$ int. $\forall n$ int. $(a \mid n \wedge b \mid n) \Leftrightarrow (a \cdot b) \mid n$?

$\boxed{?}$ $(2 \mid n \wedge 3 \mid n \wedge 5 \mid n) \Leftrightarrow 30 \mid n$?

Exercises.

Existential quantifications

- How to *prove* them as goals.
- How to *use* them as assumptions.

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,

α-equivalence

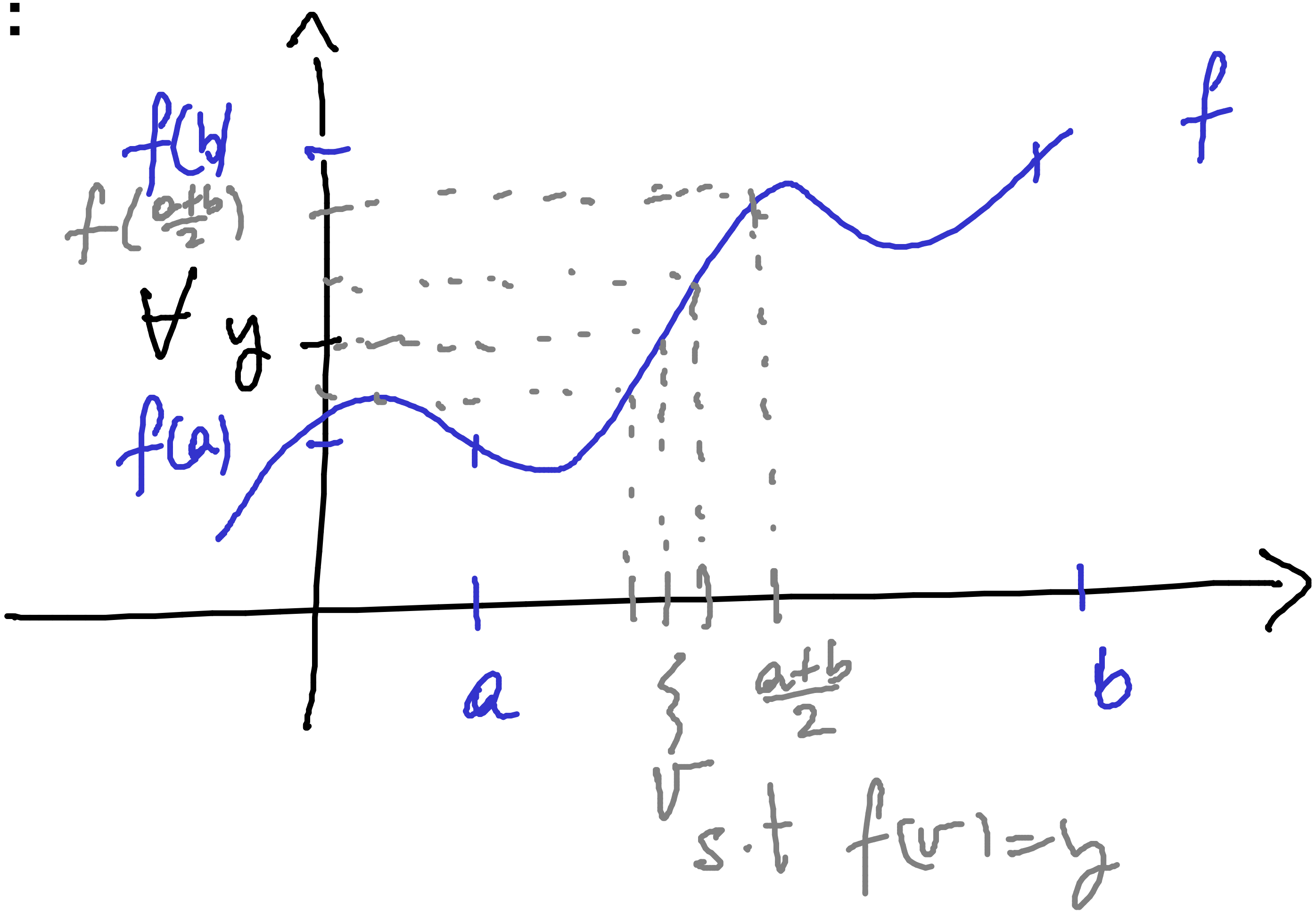
$$\boxed{\exists x.\, P(x)} \equiv \exists y.\, P(y)$$

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.

Theorem 20 (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: 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 21 *For every positive integer* k, *there exist natural numbers* i *and* j *such that* $4 \cdot k = i^2 - j^2$.

PROOF: Let k be a positive integer.

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

Given k

Let $i = k+1$

Let $j = k-1$

k	$4k$	i	j	$i^2 - j^2$
1	4	2	0	$4 - 0 = 4$
2	8	3	1	8
3	12	$\vdots$	$\vdots$	

and calculate that $i^2 - j^2 = (k+1)^2 - (k-1)^2$

$= \ldots = 4k$

$\boxtimes$

Assumptions

Goal

$\vdots$

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

$\vdots$ 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.

Theorem 23 *For all integers* l, m, n, *if* $l \mid m$ *and* $m \mid n$ *then* $l \mid n$.

PROOF: Let l, m, n be int.

Assume: $l \mid m \overset{①}{\iff} \exists$ int i. $m = l i$

and $m \mid n \overset{②}{\iff} \exists$ int j. $n = m j$

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

By ①, let i_0 be an int s.t. $m = l \cdot i_0$

By ②, let j_0 be an int s.t. $n = m \cdot j_0$

$n = m \cdot j_0$
$= l \cdot \underbrace{i_0 \cdot j_0}$

Let $k = i_0 \cdot j_0$. Then, $n = l \cdot k$ and we are done. $\boxtimes$

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,

$$\exists x.\, P(x) \;\wedge\; \Big(\forall y.\, \forall z.\, \big(P(y) \wedge P(z)\big) \implies y = z\Big)$$

existence

uniqueness.

Example: The congruence property modulo m uniquely characterises the natural numbers from 0 to $m-1$.

Proposition 24 *Let m be a positive integer and let n be an integer.*

Define

$$P(z) = \left[\, 0 \leq z < m \,\wedge\, z \equiv n \pmod{m} \,\right] .$$

Then

$$\forall x, y.\, P(x) \wedge P(y) \implies x = y .$$

PROOF: Let x and y be arbitrary

Assume (1) $P(x) \iff (0 \leq x < m \;\wedge\; x \equiv n \pmod{m})$

and

(2) $P(y) \iff (0 \leq y < m \;\wedge\; y \equiv n \pmod{m})$

RTP $x = y$

By ①, $x \equiv n \pmod{m}$
By ②, $y \equiv n \pmod{m}$ $\Big\}$ $\Longrightarrow$ $x \equiv y \pmod{m}$

That is, ⑤ $x - y = i \cdot m$ for an int. i

Then, ③ $|x-y| = |i| \cdot m$

By ①, $0 \le x < m$
By ②, $0 \le y < m$ $\Longrightarrow$ ④ $|x-y| < m$

From ③ and ④, $|i| \cdot m < m$. So $|i| = 0$

From ⑤, $x - y = 0$; That is, $x = y$. $\boxtimes$

A proof strategy

To prove

$$\forall\, x.\, \exists!\, y.\, P(x,y) \quad ,$$

for an arbitrary x construct the unique witness and name it, say as $f(x)$, showing that

$$P\big(x, f(x)\big)$$

and

$$\forall\, y.\, P(x,y) \implies y = f(x)$$

hold.

Disjunctions

- How to *prove* them as goals.
- How to *use* them as assumptions.

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: Let n be an int.

RTP $\left(n^2 \equiv 0 \pmod 4\right)$ or $\left(n^2 \equiv 1 \pmod 4\right)$

Try $n^2 \equiv 0 \pmod 4$ ✗

Try $n^2 \equiv 1 \pmod 4$ ✗

n	$\cdots$	-2	-1	0	1	2	$\cdots$
$n^2 \bmod 4$	$\cdots$	0	1	0	1	0	$\cdots$

Consider

① $n = 2i$ for int i.

Then $n^2 = 4i^2 \equiv 0 \pmod 4$

② $n = 2i+1$ for int i

Then $n^2 = 4i^2 + 4i + 1 \equiv 1 \pmod 4$

Hence, for all n, either $n^2 \equiv 0 \pmod 4$ or

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

$\boxtimes$