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 integer.

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

Assume ① $2 \mid n$ and ② $3 \mid n$

RTP: $6 \mid n \Leftrightarrow n = 6k$ for some int k.

By ①, $n = 2i$ for an int. i. $\Rightarrow 6 \mid 3n$

By ②, $n = 3j$ for an int. j. $\Rightarrow 6 \mid 2n$

$\Rightarrow 6 \mid 3n - 2n = n$

Lemma: $c \mid a \wedge c \mid b \Rightarrow c \mid pa + qb$

$\boxtimes$

Existential quantifications

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

Existential quantification

Existential statements are of the form

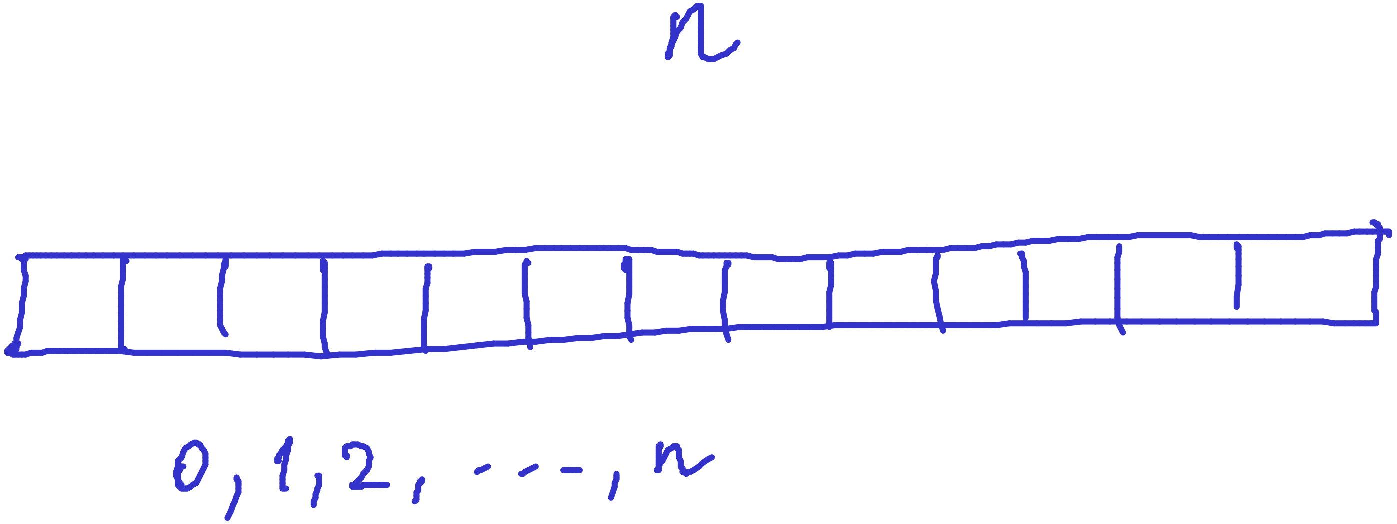
> **there exists** an individual x in the universe of discourse for which the property $P(x)$ holds

or, in other words,

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

or, in symbols,

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

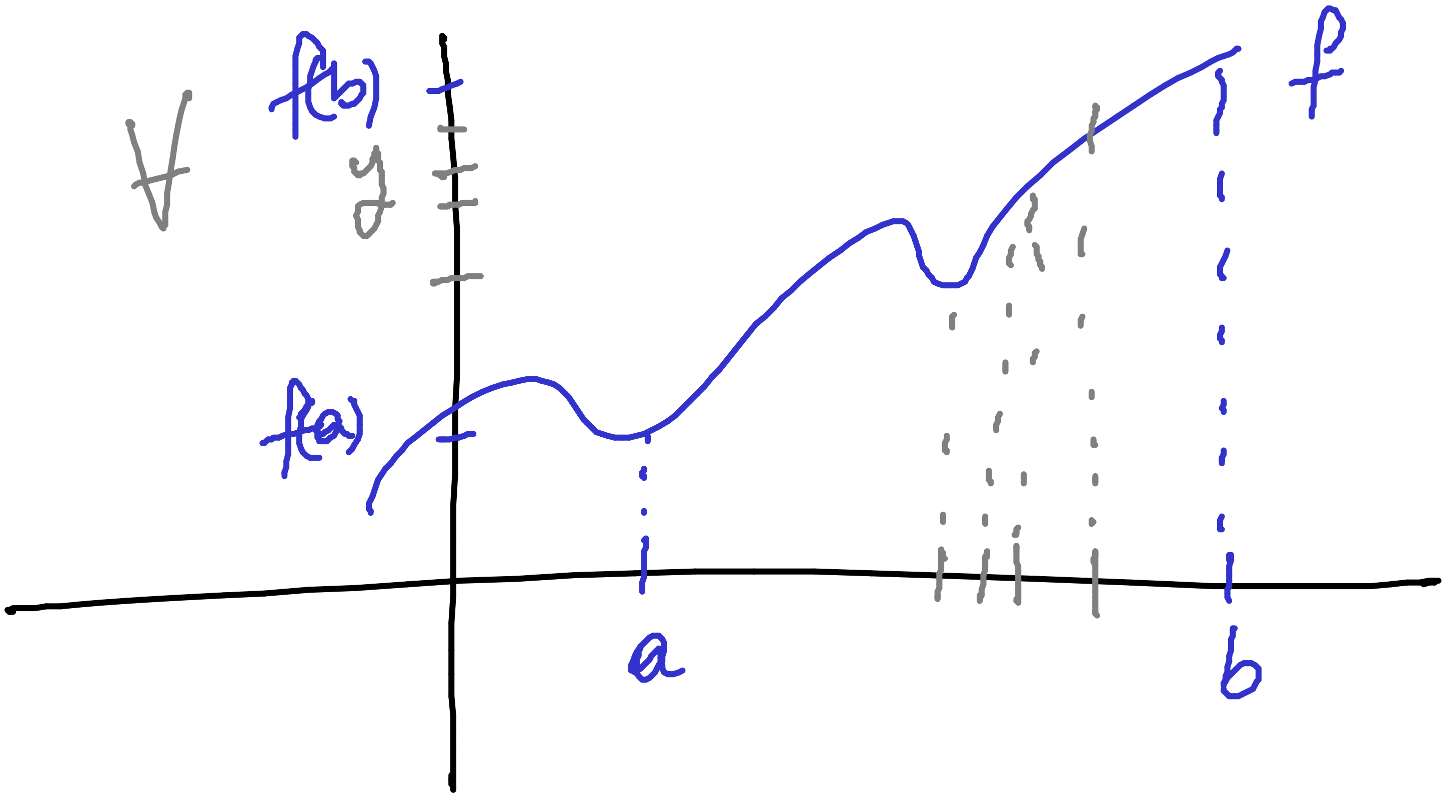


Example: The Pigeonhole Principle.

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 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: 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: Let k be a positive integer.

k	$4k$	i_0	j_0	$i_0^2 - j_0^2$
1	4	2	0	$4 - 0$
2	8	3	1	$9 - 1$
3	12			

Goal

$\exists$ nat. i, j.

$4k = i^2 - j^2$

Goal

$4k = i_0^2 - j_0^2$

Define $i_0 = k+1$

and $j_0 = k-1$

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

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

PROOF: Let l, m, n be integers.

<u>RTP</u> $(l \mid m \wedge m \mid n) \Rightarrow l \mid n$

<u>Assumptions</u>

① $l \mid m \iff \exists$ int i. $m = l \cdot i$

② $m \mid n \iff \exists$ int j. $n = m \cdot j$

Let i_0 be an int. $m = l \cdot i_0$

~~Let i_0 be an int. $n = m \cdot i_0$~~

Let j_0 be an int. $n = m \cdot j_0$

Let k_0 be the int $i_0 \cdot j_0$

<u>Goal</u>

$l \mid n$

$\iff \exists$ int k.

$n = l \cdot k$

<u>Goal</u>

$n = l \cdot k_0$

$n = m \cdot j_0 = l \cdot i_0 \cdot j_0$. $\boxtimes$

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

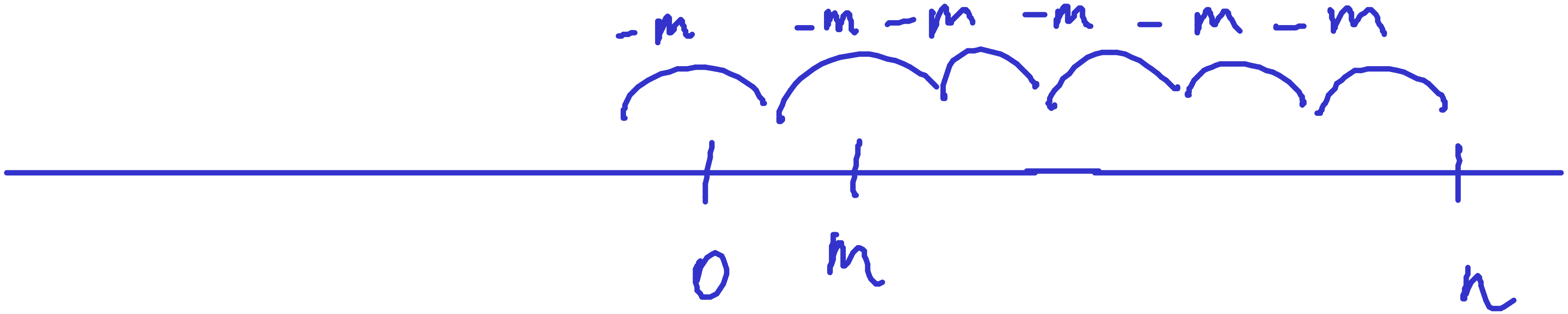
Define

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

Then

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

PROOF:



Let m be a pos. int and n be an int.
Let x and y be arbitrary.

Goal

$x = y$

Assumptions

$P(x) \Leftrightarrow$ (1) $0 \le x < m$, (2) $x \equiv n \pmod{m}$

and $P(y) \Leftrightarrow$ (3) $0 \le y < m$, (4) $y \equiv n \pmod{m}$

Lemma

$a \equiv b,\ c \equiv d$
$\Rightarrow a + c \equiv b + d$

$a \equiv b \Rightarrow ax \equiv bx$

Then (5) $x - y \equiv 0 \pmod{m}$

By (1) and (3), (6) $-m < x - y < m$

By (5), $x - y = m \cdot i$ for an int i. (7)

By (6) and (7), $i = 0 \Rightarrow x - y = 0 \longrightarrow x = y$ $\boxtimes$