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,

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

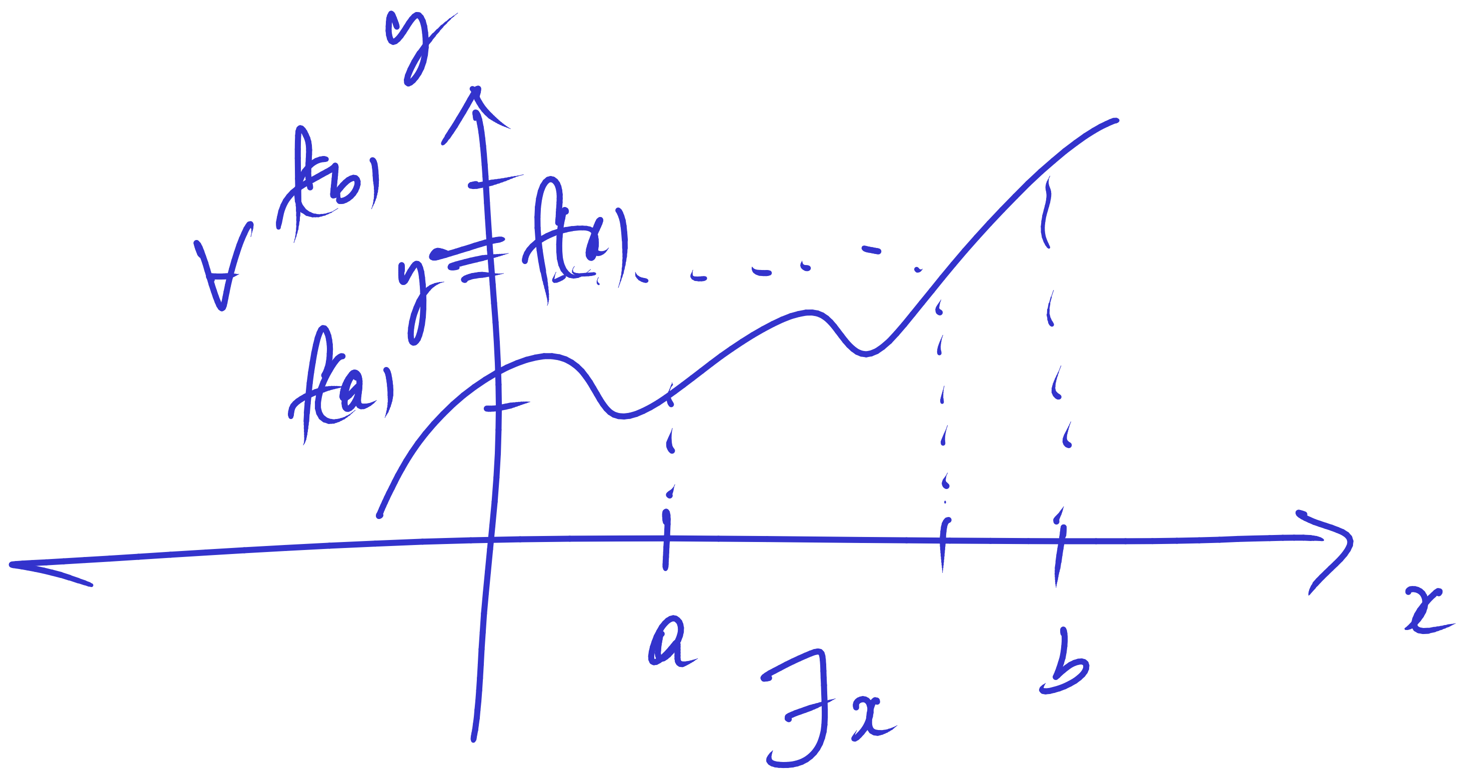
$$p_1 + p_2 + \cdots + p_n = n+1 \Longrightarrow \exists\, i = 1, \ldots, n.$$
$$p_i > 1$$

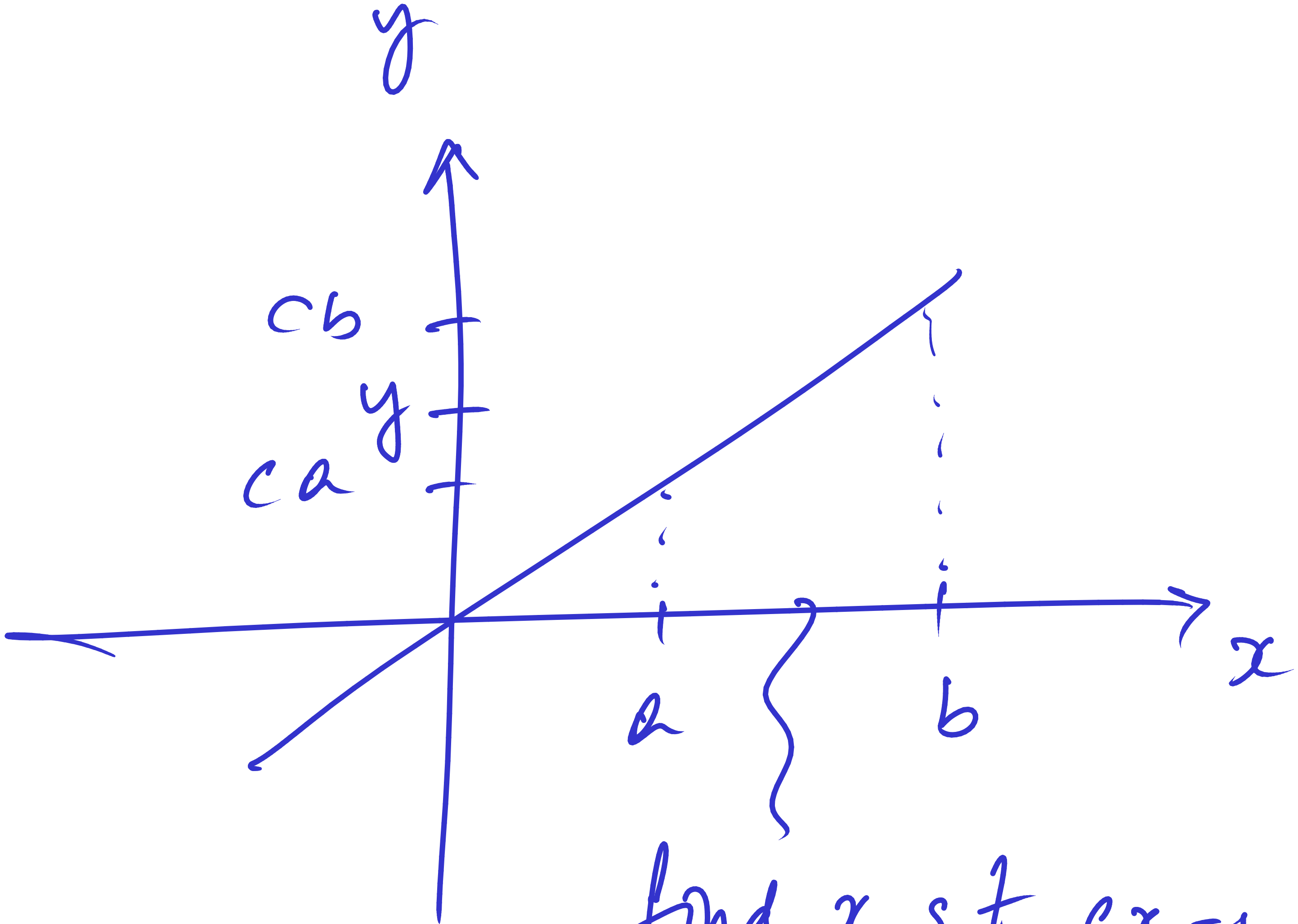
Example: The Pigeonhole Principle.

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:





find x s.t $cx = y$

Take $x = y/c$

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: $\text{Let } w = \ldots$ (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 an arbitrary pos. int.

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

Let $i = k+1$ and $j = k-1$

So

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

$$= \ldots$$

$$= 4k$$

$\boxtimes$

Scratch work

$4k$	k	i	j	$i^2 - j^2$
4	1	2	0	$4-0$
8	2	3	1	$9-1$
12	3	4	2	$16-4$
16	4			

$k \quad (k+1)(k-1)$

Assumptions

Goal

Q

$\vdots$

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

$\vdots$

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.

Using the existential statement

$P(x_0)$

Some non-sense

Assumptions

Let x be arbitrary

$\exists y. y=0$

missing the existential statement

$x=0$

proper use of existential statement

$y_0=0$

Goal

RTP: $\forall x. (\exists y. y=0) \Rightarrow x=0$

RTP: $(\exists y. y=0) \Rightarrow x=0$

RTP:

$x=0$

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 arbitrary integers.

Assume $l \mid m \overset{\text{by def}}{\iff} \exists \text{ int } i.\ li = m$ ①

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

RTP $l \mid n \overset{\text{by def}}{\iff} \exists k.\ lk = n$

Let $k = i_0 \cdot j_0$

From ①, we have i_0 int. $l \cdot i_0 = m$

From ②, we have j_0 int. $m \cdot j_0 = n$

Then $n = m \cdot j_0 = l \cdot (i_0 \cdot j_0)$. So $l \mid n$.

$\boxtimes$

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,

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

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 arbitrary integer.

Try to show that $n^2 \equiv 0 \pmod 4$ ✗

Try to show that $n^2 \equiv 1 \pmod 4$ ✗

By cases, consider 1 n is even and 2 n is odd.

CASE 1: $n = 2i$ for some int i.

Then $n^2 = 4i^2 \equiv 0 \pmod 4$ and we are done.

CASE 2: $n = 2j+1$ for some int j.

Then $n^2 = (2j+1)^2 = 4j^2 + 4j + 1 \equiv 1 \pmod 4$

and we are done. $\boxtimes$

Assumptions

$\vdots$

$P_1 \vee P_2$

$\vdots$

$$\frac{\text{Goal}}{Q}$$

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
$\vdots$	
$P_1 \lor P_2$	

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.

$a \equiv a \pmod{m}$

A little arithmetic

Lemma 27 *For all positive integers* p *and natural numbers* m*, if* $m = 0$ *or* $m = p$ *then* $\binom{p}{m} \equiv 1 \pmod{p}$.

PROOF: Let p be pos. int. and m nat. number.

Assume: $m=0 \vee m=p$.

RTP: $\binom{p}{m} \equiv 1 \pmod{p}$

$$\binom{p}{m} = \frac{p!}{m!\,(p-m)!}$$

CASE (1): Say $m=0$

Then $\binom{p}{0} = 1$

and we are done

CASE 2: Say $m=p$

Then $\binom{p}{p} = 1$

and we are done

$\boxtimes$

Lemma 28 *For all integers* p *and* m, *if* p *is prime and* $0 < m < p$ *then* $\binom{p}{m} \equiv 0 \pmod{p}$.

PROOF: Let p, m be an arbitrary integers.

Assume p is prime and $0 < m < p$.

RTP $\binom{p}{m} \equiv 0 \pmod{p} \iff \binom{p}{m}$ is a multiple of p.

Since

$$\binom{p}{m} = \frac{p!}{m!(p-m)!} = p \cdot \left[\frac{(p-1)!}{m!\,(p-m)!} \right]$$

we are done provided we show $\frac{(p-1)!}{m!\,(p-m)!}$ is an integer!

$$p \cdot \frac{(p-1)!}{m!\,(p-m)!} \text{ is an integer.}$$

Hence $m!\,(p-m)!$ divides $p \cdot (p-1)!$

As $m < p \quad p-m < p$

By prime factorisation theorem

$$m!\,(p-m)! \text{ divides } (p-1)!$$

and $\dfrac{(p-1)!}{m!\,(p-m)!}$ is an integer.

Proposition 29 *For all prime numbers* p *and integers* $0 \leq m \leq p$, *either* $\binom{p}{m} \equiv 0 \pmod{p}$ *or* $\binom{p}{m} \equiv 1 \pmod{p}$.

PROOF: