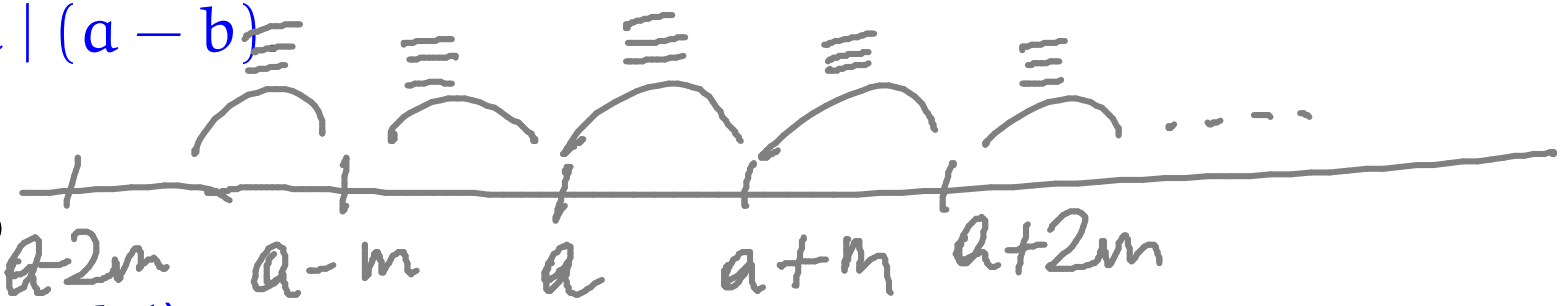
Divisibility and congruence

Definition 12 *Let* d *and* n *be integers. We say that* d divides n, *and write* $d \mid n$, *whenever there is an integer* k *such that* $n = k \cdot d$.

Example 13 *The statement* $2 \mid 4$ *is true, while* $4 \mid 2$ *is not.*

Definition 14 *Fix a positive integer* m. *For integers* a *and* b, *we say that* a *is congruent to* b *modulo* m, *and write* $a \equiv b \pmod{m}$, *whenever* $m \mid (a - b)$.



Example 15

1. $18 \equiv 2 \pmod{4}$
2. $2 \equiv -2 \pmod{4}$
3. $18 \equiv -2 \pmod{4}$

NB: $a = b \pmod{m}$, $b = c \pmod{m}$ $\Rightarrow$ $a \equiv c \pmod{m}$

Proposition 16 *For every integer* n,

1. n *is even if, and only if,* $n \equiv 0 \pmod 2$, *and*

2. n *is odd if, and only if,* $n \equiv 1 \pmod 2$.

PROOF: Let n be an integer.

(1) ($\Rightarrow$) n even $\Rightarrow$ $n \equiv 0 \pmod 2$

Assume n even.

RTP: $n \equiv 0 \pmod 2$; that is, $n - 0 = 2i$ for an int i.

($\Leftarrow$) ...

$\boxtimes$

The use of bi-implications:

To use an assumption of the form $P \iff Q$, use it as two separate assumptions $P \implies Q$ and $Q \implies P$.

Universal quantifications

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

$fun\, x \to x \equiv fun\, y \to y$ α-equivalence

Universal quantification

Universal statements are of the form

> **for all** individuals x of the universe of discourse, the property $P(x)$ holds

or, in other words,

> no matter what individual x in the universe of discourse one considers, the property $P(x)$ for it holds

or, in symbols,

$\forall x.\, P(x) \Leftrightarrow \forall y.\, P(y)$

Example 17

2. *For every positive real number* x*, if* $\sqrt{x}$ *is rational then so is* x*.*

3. *For every integer* n*, we have that* n *is even iff so is* n^2*.*

The main proof strategy for universal statements:

To prove a goal of the form

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

let x stand for an arbitrary individual and prove $P(x)$.

Proof pattern:

In order to prove that

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

1. Write: Let x be an arbitrary individual.

   Warning: Make sure that the variable x is new (also referred to as fresh) in the proof! If for some reason the variable x is already being used in the proof to stand for something else, then you must use an unused variable, say y, to stand for the arbitrary individual, and prove $P(y)$.

2. Show that $P(x)$ holds.

Scratch work:

Before using the strategy

Assumptions	Goal
	$\forall x.\, P(x)$

$\vdots$

After using the strategy

Assumptions	Goal
	$P(x)$ (for a new (or fresh) x)

$\vdots$

Let x be arbitrary.

Example:

Assumptions

$\vdots$

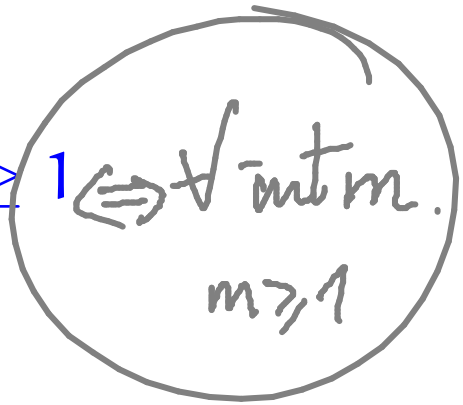
$n > 0$

$\vdots$

unprovable

Goal

for all integers n, $n \geq 1$



RTP: $n \geqslant 1$

$n > 0 \Rightarrow n \geqslant 1$

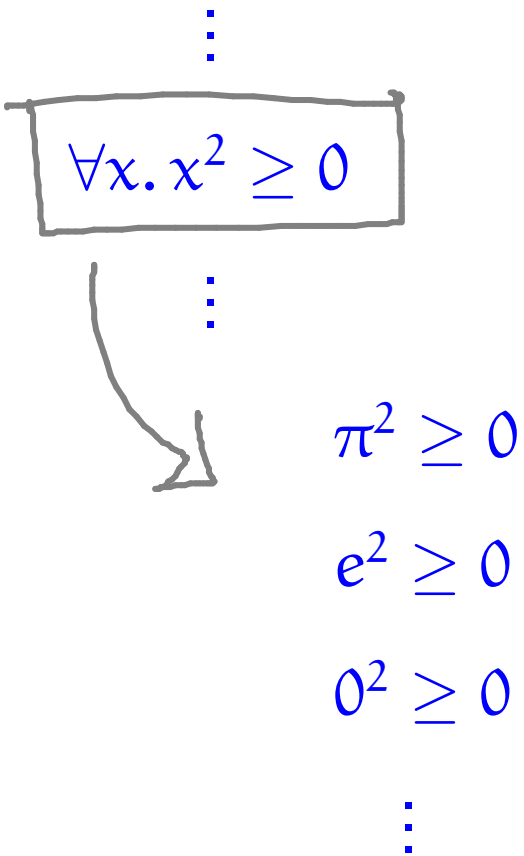
So we are done ✗

RTP: $m \geqslant 1$

which is not provable as we wanted.

How to use universal statements

Assumptions



Goal

P

The use of universal statements:

To use an assumption of the form $\forall x.\, P(x)$, you can plug in any value, say a, for x to conclude that $P(a)$ is true and so further assume it.

This rule is called *universal instantiation*.

Proposition 18 *Fix a positive integer* m*. For integers* a *and* b*, we have that* $a \equiv b \pmod{m}$ *if, and only if, for all positive integers* n*, we have that* $n \cdot a \equiv n \cdot b \pmod{n \cdot m}$*.*

PROOF: Let m be a positive int.

Let a and b be arbitrary integers.

RTP: $a \equiv b \pmod{m}$

$\iff$ $(\forall$ pos int $n.\ n \cdot a \equiv n \cdot b \pmod{n \cdot m})$

($\Rightarrow$) Assume $a \equiv b \pmod{m}$; That is (1) $a - b = m \cdot i$ for an integer i.

RTP: $\forall$ pos. int. $n.\ n \cdot a \equiv n \cdot b \pmod{n \cdot m}$

Let n be a pos. int.

RTP: $na \equiv nb \pmod{nm}$. That is,

$na - nb = j \cdot n \cdot m$ for some int j.

From assumption ①, $n(a-b) = i \cdot n \cdot m$ for some int. i.

Since $na - nb$ $=$ $n(a-b)$

we are done. ☒

($\Leftarrow$) RTP: ($\forall$ pos int n. $n \cdot a \equiv n \cdot b \pmod{n \cdot m}$)

$\Rightarrow a \equiv b \pmod{m}$

Assume

② $\forall$ pos. int. n. $na \equiv_n b \pmod{nm}$

RTP: $a \equiv b \pmod{m}$

By ②, from instantiation, we have (taking $n = 1$)

$$1 \cdot a \equiv 1 \cdot b \pmod{1 \cdot m}$$

and we are done.

$\square$

Equality in proofs

Examples:

- If $a = b$ and $b = c$ then $a = c$.
- If $a = b$ and $x = y$ then $a + x = b + x = b + y$.

Equality axioms

Just for the record, here are the axioms for *equality*.

- Every individual is equal to itself.

$$\forall x.\ x = x$$

- For any pair of equal individuals, if a property holds for one of them then it also holds for the other one.

$$\forall x. \forall y.\ x = y \implies \big(P(x) \implies P(y)\big)$$

NB From these axioms one may deduce the usual intuitive properties of equality, such as

$$\forall x. \forall y.\ x = y \implies y = x$$

and

$$\forall x. \forall y. \forall z.\ x = y \implies (y = z \implies x = z) \quad .$$

However, in practice, you will not be required to formally do so; rather you may just use the properties of equality that you are already familiar with.