Bi-implication

Some theorems can be written in the form

P is equivalent to Q

or, in other words,

P implies Q, and vice versa

or

Q implies P, and vice versa

or

P if, and only if, Q

P iff Q

or, in symbols,

$$P \iff Q$$

Proof pattern:

In order to prove that

$$P \iff Q$$

1. Write: $(\Longrightarrow)$ and give a proof of $P \implies Q$.
2. Write: $(\Longleftarrow)$ and give a proof of $Q \implies P$.

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

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 integer.

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

Assume n is even; That is, $n = 2i$ for an integere i.

RTP: $n - 0$ is a multiple of 2

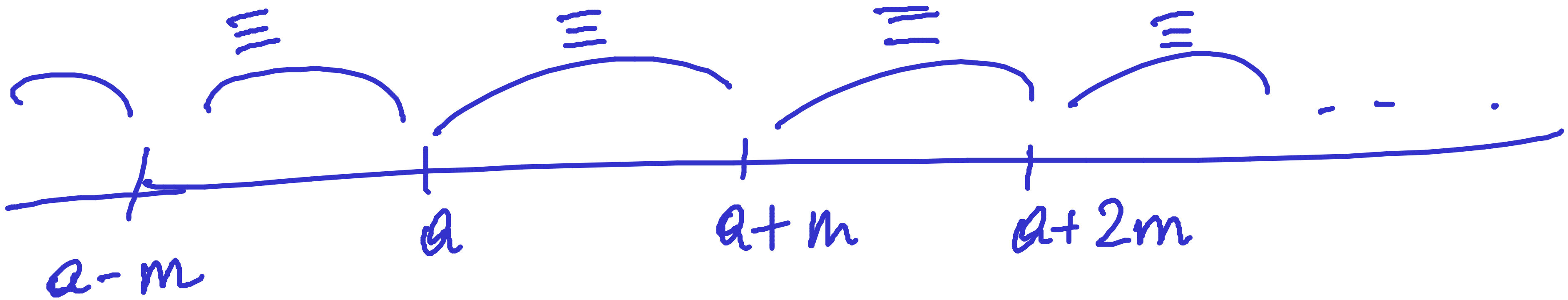
Which is the case because $n - 0 = n$.

($\Leftarrow$) $n \equiv 0 \pmod 2 \Rightarrow n$ is even. Exercise.

Assume $n \equiv 0 \pmod 2$ and show n is even.

⊠

Congruence modulo m



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.

PLs fun f(x) = x+1 ≈ fun f(y) = y+1

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,

NB:

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

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)
$\vdots$	

Example:

unprovable

Assumptions	Goal
⋮	for all integers n, $n \geq 1$
① $n > 0$	
⋮	

② Let n be an integer   RTP: $n \geqslant 1$

Then from ① and ②
we have $n \geqslant 1$.   ✗

Example:

Assumptions

⋮

$n > 0$

⋮

unprovable Goal

for all integers n, $n \geq 1$

$\equiv$ for all int. k, $k \geq 1$

Let k be an integer (with k fresh/new in the proof).

RTP: $k \geq 1$

which is not provable.

How to use universal statements

Assumptions

$$\vdots$$

$$\forall x.\, x^2 \geq 0$$

$$\vdots$$

$$\pi^2 \geq 0$$

$$e^2 \geq 0$$

$$0^2 \geq 0$$

$$\vdots$$

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 integer.
Let a and b be arbitrary integers.
(⇒) Assume ① $a \equiv b \pmod{m}$ ⟺ $a - b = im$ for some int i.
RTP: ∀ pos. int. n. $n \cdot a \equiv n \cdot b \pmod{n \cdot m}$
Let n be an arbitrary positive integer.
RTP: $na \equiv nb \pmod{nm}$
That is, $na - nb = k \cdot nm$ for an int k.
By ①, $n(a-b) = n \cdot i \cdot m$ and so $na - nb = n(a-b)$
is a multiple of $n \cdot m$

($\Leftarrow$) Assume (1) $\forall$ pos. int. n, $na \equiv nb \pmod{nm}$

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

Then from (1) by instantiation of n to 1 we have

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

as required. ☑

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.

Conjunctions

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

Conjunction

Conjunctive statements are of the form

$$\boxed{P \textbf{ and } Q}$$

or, in other words,

$$\boxed{\text{both } P \text{ and also } Q \text{ hold}}$$

or, in symbols,

$$\boxed{P \wedge Q} \qquad \text{or} \qquad \boxed{P \,\&\, Q}$$

The proof strategy for conjunction:

To prove a goal of the form

$$P \land Q$$

first prove P and subsequently prove Q (or vice versa).

Proof pattern:

In order to prove

$$P \wedge Q$$

1. Write: Firstly, we prove P. and provide a proof of P.
2. Write: Secondly, we prove Q. and provide a proof of Q.

Scratch work:

Before using the strategy

Assumptions	Goal
	$P \wedge Q$
$\vdots$	

After using the strategy

Assumptions	Goal	Assumptions	Goal
	P		Q
$\vdots$		$\vdots$	

The use of conjunctions:

To use an assumption of the form $P \wedge Q$,
treat it as two separate assumptions: P and Q.

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

PROOF:

RTP: $\forall$ int. n, $6|n \iff (2|n \wedge 3|n)$.

Let n be an arbitrary integer.

($\Rightarrow$) RTP: $6|n \Rightarrow (2|n \wedge 3|n)$

Assume: (1) $6|n \iff n = 6k$ for an int k.

RTP: $2|n \wedge 3|n$

RTP: $2|n$ $\iff$ $n = 2i$ for int i.

RTP: $3|n$

Exercise.

Since by ①, $n = 6k$. Then $n = 2(3k)$ and so $2 \mid n$.

Lemma: $(a \mid b \wedge b \mid c) \Rightarrow (a \mid c)$. Exercise.

($\Leftarrow$) RTP: $(2 \mid n \wedge 3 \mid n) \Rightarrow 6 \mid n$

Assume: $2 \mid n \wedge 3 \mid n$

So $2 \mid n \Leftrightarrow n = 2i$ ① for int i.

and $3 \mid n \Leftrightarrow n = 3j$ ② for int j

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

From ① and ②, $2i = 3j$ ...

From ①, $3n = 6i$. From ②, $2n = 6j$. ... Exercise.

Exercises $\forall n$

$$\left(2|n \wedge 3|n \wedge 5|n\right) \Leftrightarrow (30|n)$$

$\forall a, b,$

$$(a|n \wedge b|n) \Leftrightarrow (a \cdot b)|n \quad ?$$