How to use implication assumptions

Logical Deduction by Modus Ponens

A main rule of *logical deduction* is that of *Modus Ponens*:

> From the statements P and $\mathrm{P} \implies \mathrm{Q}$,
> the statement Q follows.

or, in other words,

> If P and $\mathrm{P} \implies \mathrm{Q}$ hold then so does Q.

or, in symbols,

$$\frac{\mathrm{P} \qquad \mathrm{P} \implies \mathrm{Q}}{\mathrm{Q}}$$

Proof

Assumptions Goal

$$\begin{array}{c} \vdots \\ P \Rightarrow Q \\ \vdots \\ \dfrac{P}{Q} \end{array}$$

The use of implications:

To use an assumption of the form $P \implies Q$, aim at establishing P.
Once this is done, by Modus Ponens, one can conclude Q and so further assume it.

Theorem 11 *Let* P_1, P_2, *and* P_3 *be statements. If* $P_1 \implies P_2$ *and* $P_2 \implies P_3$ *then* $P_1 \implies P_3$.

PROOF: Consider P_1, P_2, P_3.

Assume: (1) $P_1 \Rightarrow P_2$

(2) $P_2 \Rightarrow P_3$

Show: $P_1 \Rightarrow P_3$

Assume: (3) P_1

Show: P_3

By (1) and (3), we have (4) P_2

By (2) and (4), we have P_3 as required ☒

NB: We typically reason by

$P_1 \Rightarrow P_2 \Rightarrow P_3 \Rightarrow \cdots \Rightarrow P_n$

Then

$P_1 \Rightarrow P_n$

Bi-implication

Some theorems can be written in the form

$\boxed{P \text{ is equivalent to } Q}$

or, in other words,

$\boxed{P \text{ implies } Q\text{, and vice versa}}$

or

$\boxed{Q \text{ implies } P\text{, and vice versa}}$

or

$\boxed{P \text{ if, and only if, } Q}$ $\boxed{P \text{ iff } Q}$

or, in symbols,

$$\boxed{P \iff Q}$$

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 $m \mid (a - b)$.*

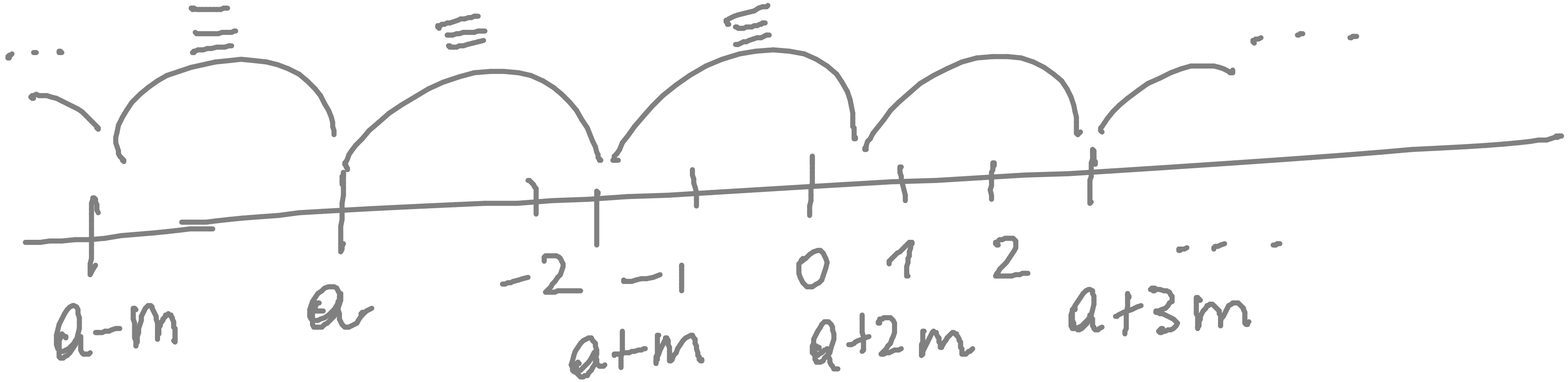
Example 15

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

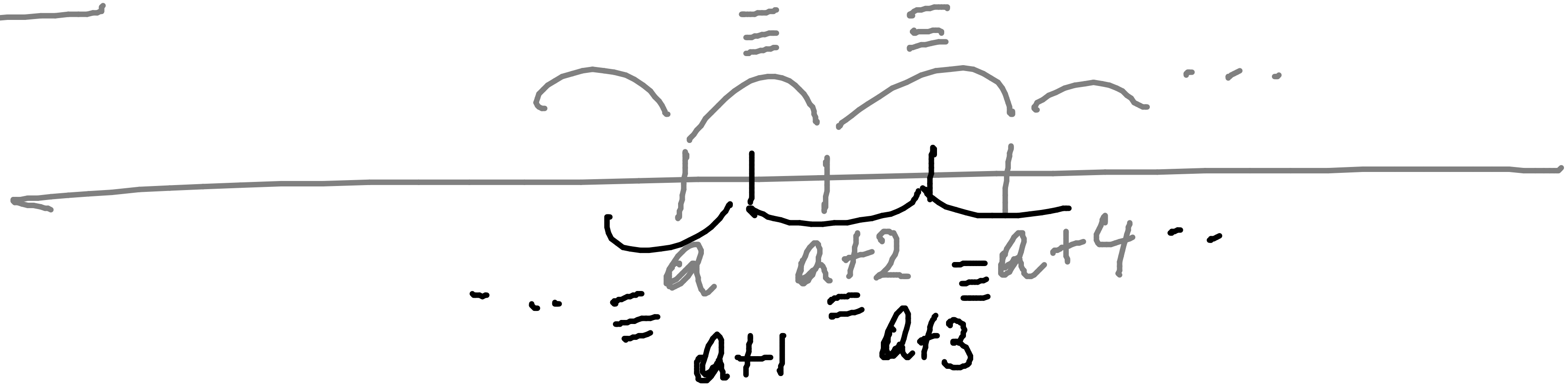
Exercise:

$a \equiv b \pmod{m}$
and $b \equiv c \pmod{m}$

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



mod 2 :



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 ($\Longrightarrow$) Assume n even; that is, $n = 2i$ for an int. i (1)

RTP: $n \equiv 0 \pmod 2$; That is $n - 0 = 2j$ for int. j

By (1), we are done.

($\Longleftarrow$) Assume: $n \equiv 0 \pmod 2$; That is, $n - 0 = 2k$ for an int. k (2)

By (2), we are done. $\boxtimes$

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.

NB: fun $f(x) = x+1 \equiv$ 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,

α- equivalence

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

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

$$\forall x. P(x) \equiv \forall y. P(y)$$

1. Write: Let x be an arbitrary individual. / Let y be arbitrary

   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. / $P(y)$

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:

Assumptions

$\vdots$

1 $n > 0$

$\vdots$

2 Let n be integer

unprovable

Goal

~~for all integers n,~~ $n \geq 1$

Goal: $n \geq 1$

From 1 and 2, we are done.

Assumptions

$\vdots$

$n > 0$

$\vdots$

Let m integer (fresh)

Goal

$\forall n$ int. $n \geq 1$

$\equiv$

$\forall m$ int. $m \geq 1$

<u>RTP:</u> $m \geq 1$

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 pos. int. m.

Let a and b be integers

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

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

($\Rightarrow$) Assume: $a \equiv b \pmod{m}$; That is,

① $a - b = i\,m$ for an int. i

RTP: $\forall$ pos. int. n. $na \equiv nb \pmod{n \cdot m}$

Let n be an arbitrary pos. int.

RTP: $na \equiv nb \pmod{nm}$; that is,

$\underbrace{na - nb}_{n(a-b)} = j \cdot nm$ for some int j.

From ①, $n(a-b) = \underbrace{n \cdot i \cdot m}_{i \cdot (n \cdot m)}$ for an int i

and we are done.

$(\Leftarrow)$ Assume: ② $\forall$ pos. int. n, $na \equiv nb \pmod{nm}$

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

By ②, $1 \cdot a \equiv 1 \cdot b \pmod{1 \cdot m}$ and we are done. $\boxtimes$

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

$$P \wedge Q$$

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
$\vdots$		$\vdots$	

Assumptions   Goal

$$\begin{array}{c} \vdots \\ P \wedge Q \\ \vdots \\ P \qquad Q \\ \vdots \end{array}$$

The use of conjunctions:

To use an assumption of the form $\mathrm{P} \wedge \mathrm{Q}$,
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: Let n be an integer.

RTP: $6 \mid n \iff (2 \mid n \text{ and } 3 \mid n)$

$(\Rightarrow)$ Assume: (1) $6 \mid n$; That is, $n = 6i$ for an int. i.

RTP: $2 \mid n$ and $3 \mid n$

RTP: $2 \mid n$; i.e $n = 2j$ for int j
From (1), $n = 2 \cdot (3i)$
and we are done

RTP: $3 \mid n$
... exercise ...

$(\Leftarrow)$ exercise.