Proofs

Assumptions

$\vdots$

(statements)

P

$$\frac{A \Rightarrow B \qquad A}{B}\ (MP)$$

Goals

$\vdots$

(statements)

$\cancel{P \Rightarrow Q}$

Q

Logical Deduction
— Modus Ponens —

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

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

or, in other words,

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

or, in symbols,

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

The use of implications:

To use an assumption of the form $\mathrm{P} \implies \mathrm{Q}$, 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:

Assume $P_1 \Rightarrow P_2$, $P_2 \Rightarrow P_3$

<u>RTP</u> $P_1 \Rightarrow P_3$

Assume P_1

<u>RTP</u>: P_3

From (MP) P_1 and $P_1 \Rightarrow P_2$ we have P_2

From (MP) P_2 and $P_2 \Rightarrow P_3$ we have P_3

In practice

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

Then we have

$$P_1 \Rightarrow P_n$$

formally

$$\frac{\begin{array}{c} P_1 \Rightarrow P_2 \\ P_2 \Rightarrow P_3 \\ \vdots \\ P_{n-1} \Rightarrow P_n \end{array}}{P_1 \Rightarrow P_n}$$

Bi-implication

Some theorems can be written in the form

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

or, in other words,

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

or

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

or

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

or, in symbols,

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

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 $Q \implies P$.

Proposition 12 *Suppose that* n *is an integer. Then,* n *is even iff* n^2 *is even.*

PROOF: Let n be an integer.

$(\Rightarrow)$ n even $\Rightarrow n^2$ even.

Assume n even $\Leftrightarrow n = 2k$ for int. k

RTP: n^2 even.

So $n^2 = 4k^2 = 2(2k^2) = 2l$ for l the integer $2k^2$.

($\Leftarrow$) n^2 even $\Rightarrow$ n even

Assume n^2 even $\Leftrightarrow$ $n^2 = 2k$ for an integer k

RTP: $n = 2\ell$ for some int. ℓ.

We prove the contrapositive; i.e.

n odd $\Rightarrow$ n^2 odd.

is a corollary of the previously proved result that the product of two odd numbers is odd.

Divisibility and ~~congruence~~ predicate

Definition 13 *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 $n = k \cdot d$.*

d divides n / n is a multiple of d

whenever $n = k \cdot d$ for some int. k

Example 14 *The statement $2 \mid 4$ is true, while $4 \mid 2$ is not.*

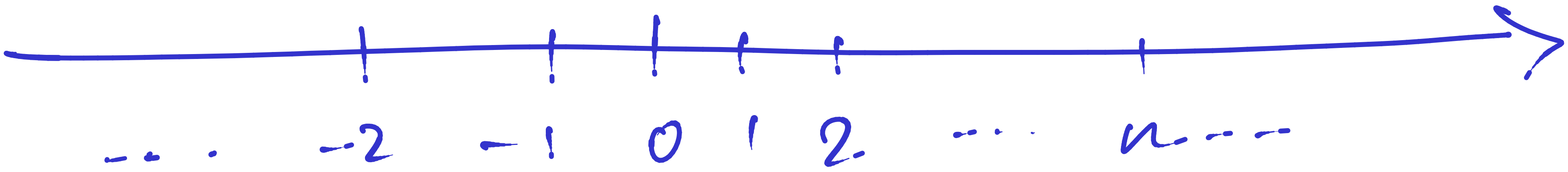
Definition 15 *Fix a positive integer m. For integers a and b, we say that a is congruent to b modulo m, and write $a \equiv b \pmod{m}$, whenever $m \mid (a - b)$.*

$a \equiv b \pmod{m} \iff a - b = km$ for some int k

Example 16

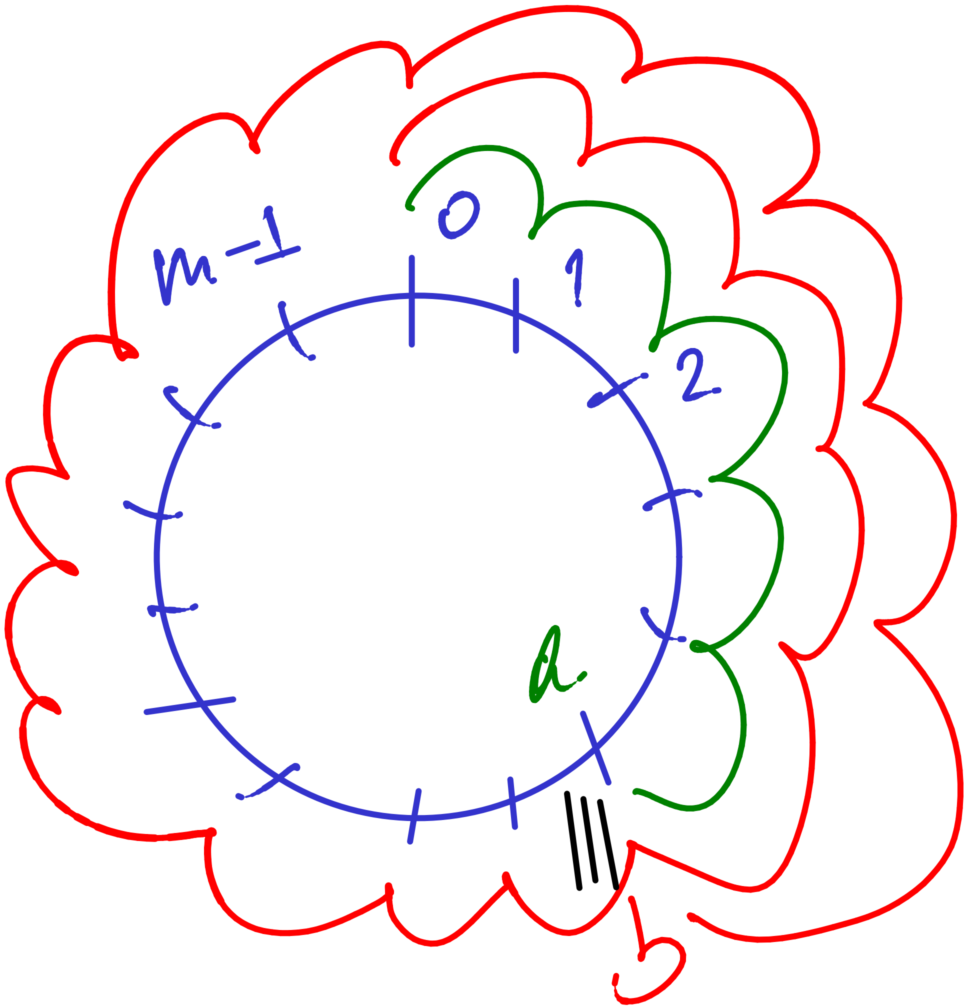
1. $18 \equiv 2 \pmod 4$
2. $2 \equiv -2 \pmod 4$
3. $18 \equiv -2 \pmod 4$

arithmetic



modulo m

$a \equiv b$



Proposition 17 *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:

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 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,

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

α- equivalence

Example 18

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

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.

   generic
   unconstrained.

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

Assumptions

⋮

Let x be a number

Let y be arbitrary..

$P(y)$

Goals

⋮

$\forall x. P(x)$

$\cancel{\forall y. P(y)}$

fresh/new

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)
$\vdots$	

Assumption	Goal
$\forall x.\, P(x)$	Q
$P(a)$
$P(b)$
$\vdots$

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 19 *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.

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

$n \cdot a \equiv n \cdot b \pmod{n \cdot m})$

$(\Longrightarrow)$ Assume $a \equiv b \pmod{m} \iff a - b = km$ for some int k

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

Assume n is a pos. int.

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

$\iff na - nb = l\, n \cdot m$ for some int l

By assumption

$$a-b = km \qquad \text{for an int } k$$

So

$$na - nb = n(a-b) = n \cdot k \cdot m.$$

That is, $na \equiv nb \pmod{n \cdot m}$

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

<u>RTP</u>: $a \equiv b \pmod m$

By univ. instantiation, we have

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

and so we are done. $\boxtimes$

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.

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

Leibniz equality

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.