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.*

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 $n = k \cdot d$.*

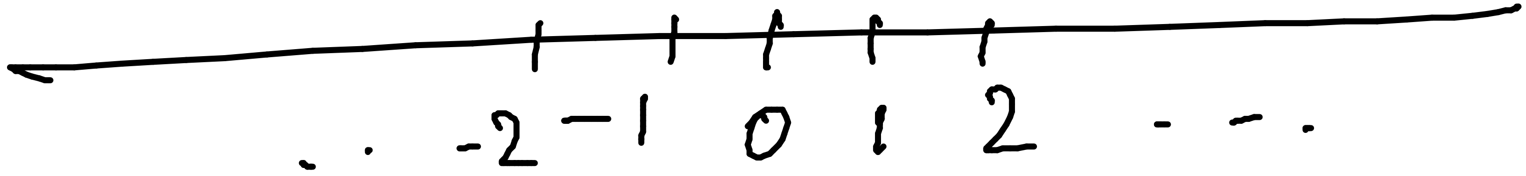
Example 13 *The statement $2 \mid 4$ is true, while $4 \mid 2$ is not.*

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

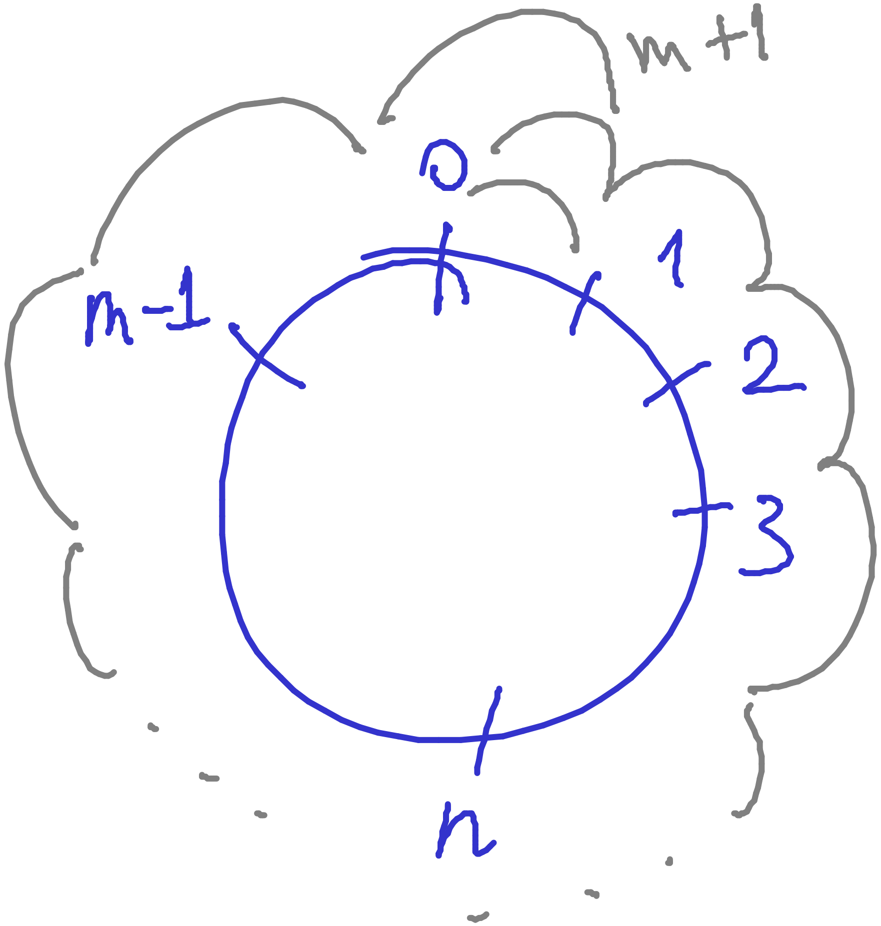
Example 15

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

number line



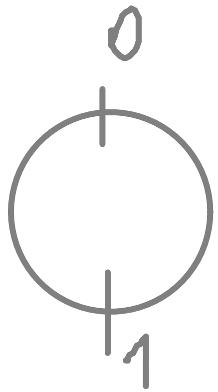
modular arithmetic (modulo m)



$m+1 \equiv 1 \pmod{m}$

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:

(2)($\Longrightarrow$) Assume n odd; i.e. $n = 2k+1$ for an int k.

RTP: $n \equiv 1 \pmod 2$; $n-1 = 2i$ for an int i.

By assumption, it follows that $n-1 = 2k$ and we are done.

($\Longleftarrow$) Assume $n \equiv 1 \pmod 2$; i.e. $n-1 = 2k$ for an int k.

RTP: $n = 2j+1$ for an int j.

By assumption, $n = 2k+1$ and we are done. ☒

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.

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,

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

equivalent to $\forall y.\, P(y) \equiv \forall z.\, P(z)$ ...

Example 18

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.

   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:

Assumptions	unprovable Goal
⋮	for all integers n, $n \geq 1$
$n > 0$	≡ ∀int k. k ≥ 1
⋮	
not fresh	
~~n an integer~~	~~RTP: n ≥ 1~~ ✗
INSTEAD	
k is an integer (fresh)	RTP: k ≥ 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 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.

$\forall$ int. a, b. ($a \equiv b$ mod m) $\Longleftrightarrow$ ($\forall$ pos. int n. $na \equiv nb$ mod (nm))

Let a, b be arbitrary integers.

RTP: ($\Rightarrow$) Assume $a \equiv b$ mod m. — That is, $a - b = im$ for an int i. (*)

RTP: $\forall$ pos. int n. $na \equiv nb$ (mod nm)

Let n be an arbitrary pos. int.

RTP: $na \equiv nb$ (mod nm); That is,

$na - nb = nmk$ for some int. k

By (*), $na - nb = i \cdot nm$ and we are done

RTP: ($\Leftarrow$)

($\Leftarrow$) $\left[\forall \text{ pos. int. } n.\ na \equiv nb \pmod{nm}\right] \Longrightarrow \left[a \equiv b \pmod{m}\right]$

<u>Assume:</u> $\forall$ pos. int. n. $na \equiv nb \pmod{nm}$

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

By instantiation, we have

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

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
	$P \wedge Q$
⋮	

After using the strategy

Assumptions	Goal	Assumptions	Goal
	P		Q
⋮		⋮	

The use of conjunctions:

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

Theorem 20 *For every integer* n*, we have that* $6 \mid n$ *iff* $2 \mid n$ *and* $3 \mid n$*.*

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

Let n be an arbitrary integer.

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

($\Rightarrow$) Assume $6|n$; that is, $n = 6k$ for an int. k.

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

RTP: $2|n$

By assumption, $n = 2\cdot(3k)$, so $n = 2i$ for the int $i = 3k$.

RTP: $3|n$

By assumption, $n = 3(2k)$; so $n = 3j$ for j the int. $2k$. ☒

($\Leftarrow$) $(2|n \wedge 3|n) \Rightarrow 6|n$

<u>Assume</u>: $(2|n \wedge 3|n)$; That is,

$n = 2p$ for an int p

and also

$n = 3q$ for an int q.

<u>RTP</u> $6|n$; That is, $n = 6 \cdot r$ for an int r.