Scratch Proofs.

Assumptions.

$P = A \Rightarrow B$

Modus Ponens

Rule for using implications

Goal

$\cancel{P \Rightarrow Q}$

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 $P \implies Q$, 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: P_1, P_2, P_3 statements

Assume (1) $P_1 \Rightarrow P_2$ and (2) $P_2 \Rightarrow P_3$

RTP: $P_1 \Rightarrow P_3$

Assume (3) P_1

RTP: P_3

By MP from (1) and (3) we have (4) P_2

By MP from (4) and (2) we have P_3

So we are done.

$\boxtimes$

In practice:

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

$\cdots \Rightarrow P_n$

If P_1 then P_n

Bi-implication

Some theorems can be written in the form

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

or, in other words,

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

or

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

or

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

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 $Q \implies P$.

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

PROOF: Assume n is an integer.

($\Rightarrow$) n is even Then n^2 is even

Assume: n is even. That is $n = 2i$ for some integer i

RTP: n^2 is even

But $n^2 = 2 \cdot (2i^2)$

Therefore $n^2 = 2j$ for an integer j $(= 2i^2)$

($\Leftarrow$) n^2 is even then n even.

Assume: n^2 is even That is $n^2 = 2k$ for an integer k

RTP: n is even

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

By contrapositive, show n odd $\Rightarrow$ n^2 odd

which is a corollary of the proposition that

the product of odd numbers is odd.

$\boxtimes$

Divisibility and congruence

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

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

$a-b$ is a multiple of m.

Example 16

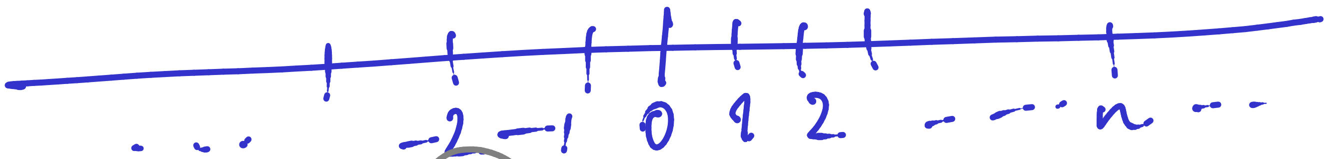
1. $18 \equiv 2 \pmod{4}$
2. $2 \equiv -2 \pmod{4}$
3. $18 \equiv -2 \pmod{4}$

Proposition 17 *For every integer* n,

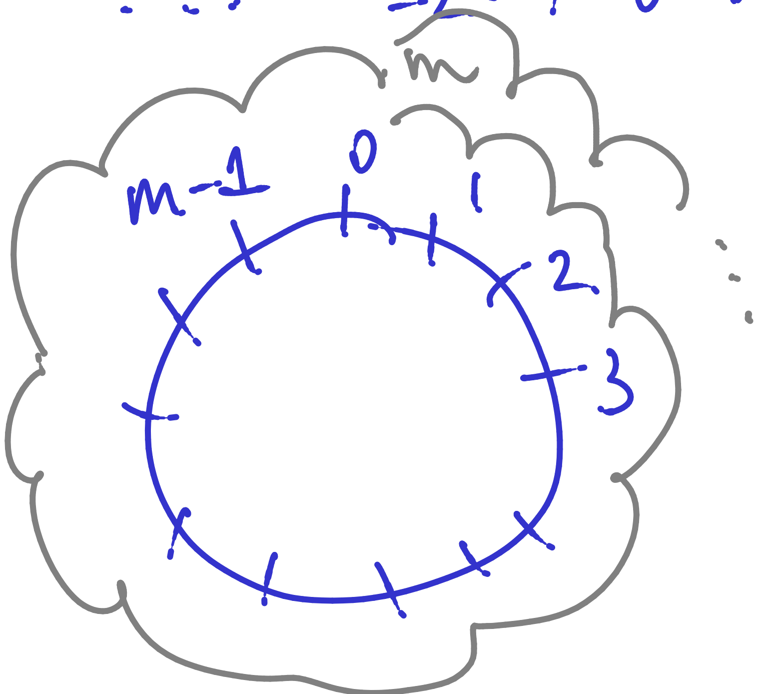
1. n *is even if, and only if,* $n \equiv 0 \pmod{2}$, *and*
2. n *is odd if, and only if,* $n \equiv 1 \pmod{2}$.

PROOF:

Integers



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 $Q \implies P$.

c.f. 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, What about $\forall y. P(y)$?

$$\boxed{\forall x. P(x)}$$

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.

   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)
$\vdots$	

Assumptions

$\forall x. P(x)$

$P(a), P(b), \ldots$

Goal

Q

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: Assume m is a positive integer.
Let a and b be arbitrary integers.

($\Longrightarrow$) $a \equiv b \pmod{m}$ Then $\forall$ pos. int. n. $na \equiv n \cdot b \bmod (n \cdot m)$

Assume ① $a \equiv b \pmod{m}$ that is, $a - b = \ell m$ for some int ℓ

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

Let n be an arbitrary positive integer

RTP: $na \equiv nb \pmod{n m}$

that is $na - nb = k\,nm$ for some int k

By ①, $na - nb = n(a-b) = n\ell m = \ell n m$

and we are done.

($\Leftarrow$) $\forall$ pos. int n. $n.a \equiv n b \pmod{nm}$

Then

$a \equiv b \pmod{m}$

<u>Assume</u>: ① $\forall$ pos. int n. $n a \equiv n b \pmod{n.m}$

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

By ① instantiating for $n = 1$, we have

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

That is

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

$\boxtimes$

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.

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

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.