Divisibility

a, b integers

$a \mid b$ a <u>divides</u> b

Def $b = ka$ for an integer k.

Congruence

Fix a positive natural number m.

For integers a and b,

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

iff$_{def}$ $\quad m \mid (a-b)$

iff $\quad a-b = m.k$ for some k integer

iff $\quad a = mk+b$ for some k integer.

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

Example 16

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

<u>Lemma</u> If $a \equiv b \pmod{m}$ and $b \equiv c \pmod{m}$ then $a \equiv c \pmod{m}$

<u>Lemma</u> $a \equiv a \pmod{m}$

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:

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,

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

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)
$\vdots$	

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 fixed positive integer.
Let a and b be arbitrary integers.
RTP: $a \equiv b \pmod{m} \iff \forall$ pos. int. n. $na \equiv nb \pmod{nm}$

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

RTP: $a \equiv b \pmod{m}$
By instantiation, $1 \cdot a \equiv 1 \cdot b \pmod{1 \cdot m}$
So we are done.

($\Rightarrow$) Assume $a \equiv b \pmod{m}$ $\Leftrightarrow$ $m \mid a-b$ $(*)$

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

Let n be an arbitrary pos. int

RTP: $na \equiv nb \pmod{nm}$

Equivalently, $nm \mid (na - nb)$

From $(*)$ and Lemma, we are done. $\boxtimes$

Lemma: $i \mid j \Rightarrow ki \mid kj$.

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.

Conjunction

Conjunctive statements are of the form

$$\boxed{P \text{ **and** } Q}$$

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).

Remark: $P \Leftrightarrow Q \stackrel{def}{=} (P \Rightarrow Q) \wedge (Q \Rightarrow P)$

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 $P \land Q$,
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: Let n be an arbitrary integer.

<u>RTP</u>: $6 \mid n \iff (2 \mid n \wedge 3 \mid n)$

<u>Lemma</u>. $a \mid b \wedge b \mid c \Rightarrow a \mid c$

$(\Longrightarrow)$ Assume $6 \mid n$.

<u>RTP</u>: $2 \mid n \wedge 3 \mid n$

<u>RTP</u>: $2 \mid n$

Since $2 \mid 6$ and by assumption $6 \mid n$ then by Lemma $2 \mid n$

<u>RTP</u>: $3 \mid n$

... analogous ...

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

Assume: $2|n \wedge 3|n$; so ① $2|n$ and also ② $3|n$

RTP: $6|n \Leftrightarrow n = 6k$ for some int. k.

We have by ①, $n = 2i$ for an int i; and, by ②, $n = 3j$ for an int. j.

Then, $3n = 6i$ and $2n = 6j$

So $n = 3n - 2n = 6i - 6j = 6(i-j)$

and we are done.

$\boxtimes$

$$6 \mid n \iff (2 \mid n \wedge 3 \mid n)$$

$$(a \cdot b) \mid n \overset{?}{\iff} (a \mid n \wedge b \mid n)$$

not generally true; a counter example is:

$4 \mid 12 \wedge 6 \mid 12$ $\quad 24 \nmid 12$

$$(abc) \mid n \overset{?}{\iff} a \mid n \wedge b \mid n \wedge c \mid n$$

Exercise:

$$30 \mid n \iff 2 \mid n \wedge 3 \mid n \wedge 5 \mid n$$