Divisibility and congruence

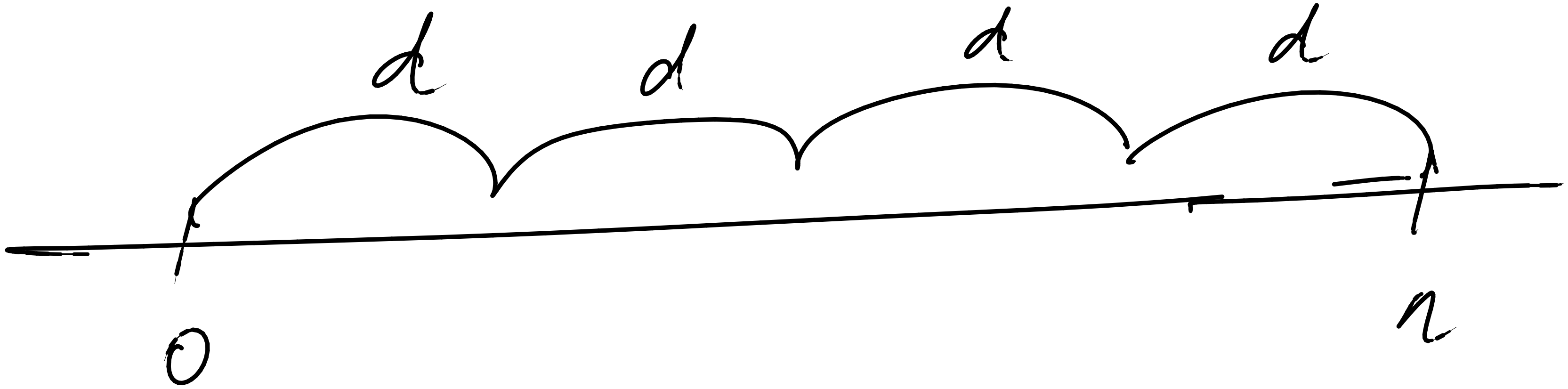
Definition 13 *Let* d *and* n *be integers. We say that* d *divides* n*, and write* $d \mid n$*, whenever there is an integer* k *such that* $n = k \cdot d$*.*

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

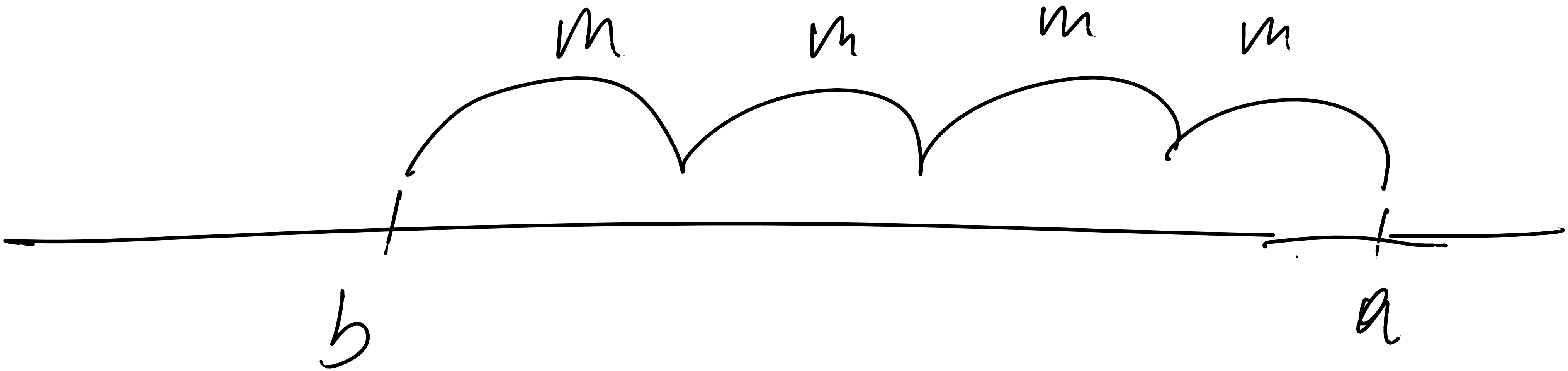
Example 16

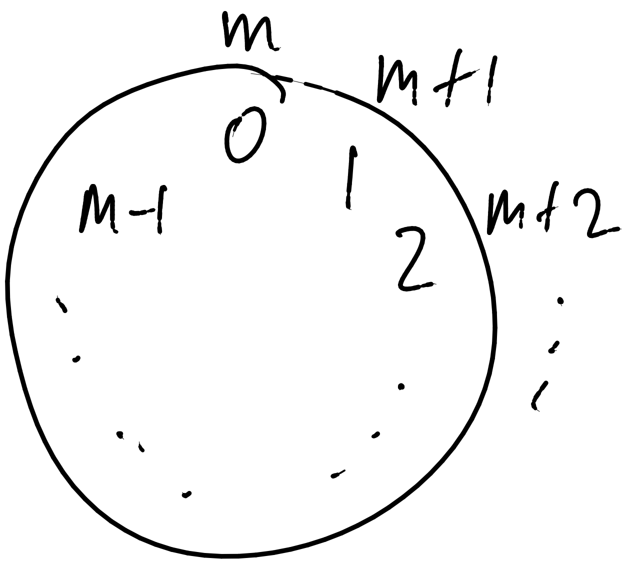
1. $18 \equiv 2 \pmod{4}$
2. $2 \equiv -2 \pmod{4}$
3. $18 \equiv -2 \pmod{4}$



$d \mid n$

$a \equiv b \pmod{m}$





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

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

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,

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

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

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.

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

Example $\forall x. \forall y. \forall z. P(x,y,z)$ ~ Let x, y, z be arbitrary individuals

$P(x,y,z)$

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	Goal
...	G

$\forall x. P(x)$ $\quad P(a)$

$P(b)$ ....

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: $\forall a, b$ integers.

$a \equiv b \pmod{m} \iff (\forall$ positive int. n. $n \cdot a \equiv n \cdot b \pmod{n \cdot m})$

Let a and b be arbitrary int.

$(\Longrightarrow)$ Assume $\boxed{a \equiv b \pmod{m}}$ $\rightsquigarrow$ $a - b = k \cdot m$ for int k

Need show $\boxed{\forall \text{ positive int. } n \;\; n \cdot a \equiv n \cdot b \pmod{n \cdot m}}$

Let n be an arbitrary positive int.

Need show $\boxed{n \cdot a \equiv n \cdot b \pmod{n \cdot m}}$ $\rightsquigarrow$ $na - nb = \ell n \cdot m$ for an int ℓ

Since $a-b=km$, it follows that

$$\underbrace{n(a-b)}_{na-nb} = \underbrace{nkm}_{k(nm)}$$

and so $na \equiv nb \pmod{nm}$.

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

$\Downarrow$?

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

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

Required to prove $a \equiv b \pmod{m}$.

$\Downarrow$ for $n=1$

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

as required $\square$

$$a \equiv b \pmod{m} \overset{?}{\Longrightarrow} a+c \equiv b+c \pmod{m}$$

$$\overset{?}{\Longrightarrow} a \cdot c \equiv b \cdot c \pmod{m}$$

$$\overset{?}{\Longrightarrow} a^k \equiv b^k \pmod{m}$$

$$\overset{?}{\Longrightarrow} c^a \equiv c^b \pmod{m}$$

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

$$\boxed{P \textbf{ and } Q}$$

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
	$P \land Q$
$\vdots$	

After using the strategy

Assumptions	Goal	‖	Assumptions	Goal
	P	‖		Q
$\vdots$		‖	$\vdots$	

Assuption   Goal

$P \wedge Q$ G

$P \quad , \quad Q$

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

($\Longrightarrow$) $\boxed{\text{Assume } 6|n}$; that is, $n = 6k$ for k int

Then $n = 2(3k)$ and $n = 3(2k)$

$(\Leftarrow)$ Assume $(2|n \wedge 3|n)$

Then $\boxed{2|n}$ and also $\boxed{3|n}$

$\Downarrow$ $\quad\quad$ $\Downarrow$

$n = 2k$ (k int) $\quad\quad$ $n = 3\ell$ (ℓ int)

$k = 3j$ $\quad\quad$ $\ell = 2j$

$j = 3j - 2j = k - \ell$

PROOF IDEA

$6|n \rightsquigarrow n = 6j$ (j int)