Divisibility

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

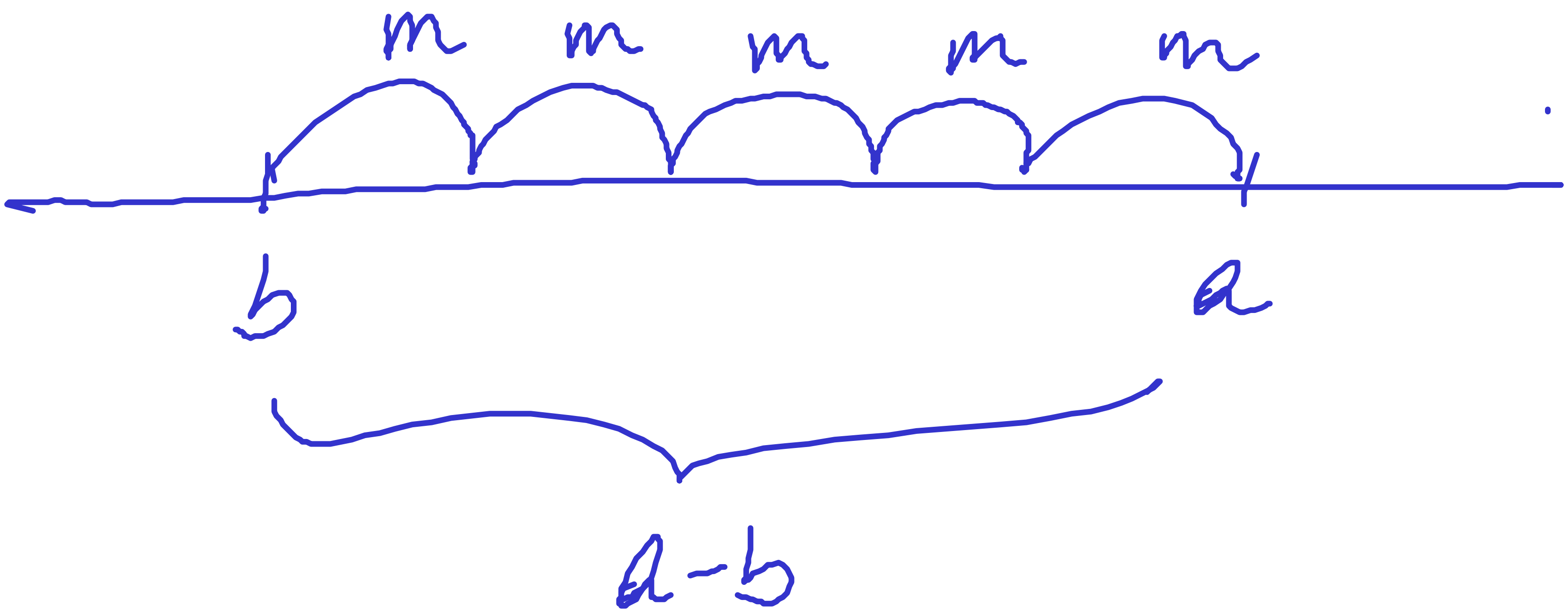
d divides n
d is a factor of n
n is a multiple of d

$n = kd$ for some integer k.

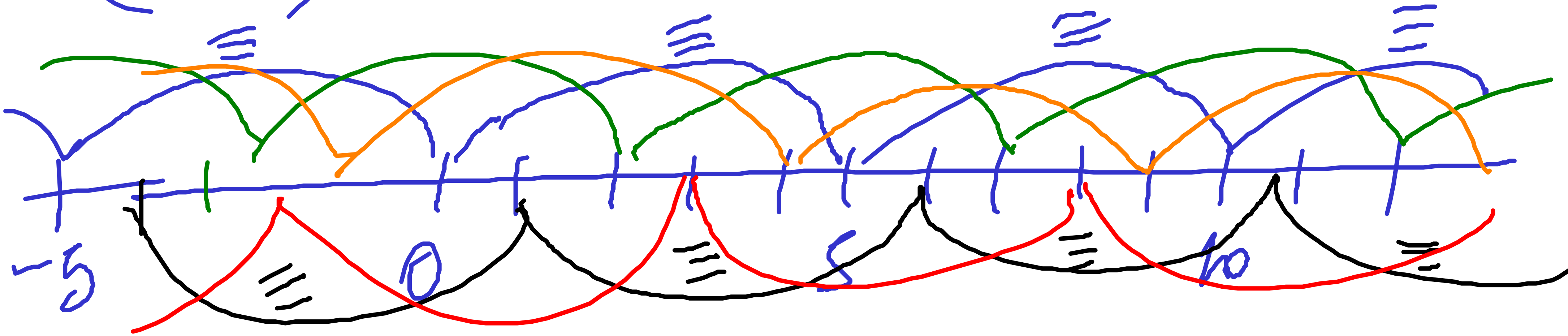
CONGRUENCE

$a \equiv b \pmod{m}$ iff $m \mid (a-b)$

iff $a - b = km$ for some integer k.



(mod 5)



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 $Q \implies P$.

$\lambda n. n+1 \equiv \lambda m. m+1$

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, ~~other notation $\forall x : P(x)$~~

> no matter what individual x in the universe of discourse one considers, the property $P(x)$ for it holds

or, in symbols,

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

$\equiv \forall y.\, P(y)$

In ML,
fn n => n+1
$\equiv$ fn m => m+1

Example 18

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

also referred to as fresh

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 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 fresh x)
$\vdots$	or new

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.
($\Longrightarrow$) We need show, if $a \equiv b \pmod{m}$ Then
$\forall$ integer n. $n \cdot a \equiv n \cdot b \mod (n \cdot m)$.
Assume ① $\boxed{a \equiv b \pmod{m}}$, and will show
Goal
$\forall$ integer n. $\boxed{n \cdot a \equiv n \cdot b \pmod{n \cdot m}}$.
So let n be an arbitrary positive integer.
By ①, $a - b = k m$ for some integer k.

So $n(a-b) = k \cdot n \cdot m$, and hence

$$na - nb = k(nm)$$

Thus, we are done.

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

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

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

So $1 \cdot a \equiv 1 \cdot b \pmod{1 \cdot m}$ hence we are done.

$\square$

To use an assumption

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

you may assume $P(a)$ for whatever a.

Conjunction

Conjunctive statements are of the form

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

or, in other words,

$$\boxed{\text{both } \mathrm{P} \text{ and also } \mathrm{Q} \text{ hold}}$$

or, in symbols,

$$\boxed{\mathrm{P}\ \&\ \mathrm{Q}} \qquad \text{or} \qquad \boxed{\mathrm{P} \wedge \mathrm{Q}}$$

The proof strategy for conjunction:

To prove a goal of the form

$$P \ \& \ Q$$

first prove P and subsequently prove Q (or vice versa).

NB: $(P \Leftrightarrow Q)$ equivalent to

$(P \Rightarrow Q)$ & $(Q \Rightarrow P)$

Proof pattern:

In order to prove

$$P \;\&\; Q$$

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
	$P \ \& \ Q$
$\vdots$	

After using the strategy

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

The use of conjunctions:

To use an assumption of the form $P \ \& \ Q$,
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: $[\forall \text{ int. } n.\ 6 \mid n \Leftrightarrow (2 \mid n \ \& \ 3 \mid n)]$

Let n be an arbitrary integer.

$(\Rightarrow)$ $6 \mid n \Rightarrow (2 \mid n \ \& \ 3 \mid n)$

$(*)$ $\boxed{\text{Assume } 6 \mid n}$. Show $2 \mid n$ & $3 \mid n$.

(1) Show $2 \mid n$

By $(*)$, $n = 6k$ for some int. k. Hence $n = 2j$ for $j = 3k$ and we are done.

(2) Show $3 \mid n$

By $(*)$, $n = 6k$ for some int. k. So $n = 3(2k)$ hence $3 \mid n$.

$(\Leftarrow)$ $(2|n \;\&\; 3|n) \overset{?}{\Longrightarrow} 6|n$.

Assume $2|n$ and $3|n$. Hence

(1) $n = 2i$ for some int i

and

(2) $n = 3j$ for some int j

Want to show

$n = 6k$ for some int k.

$$\left[\begin{array}{l} = 2\cdot(3k) \\ = 3\cdot(2k) \end{array}\right]$$

idea: i, j should tell us the value k

We test the idea by calculating

$$6(i-j) = \cdots$$