4. Integers

4.1 Natural numbers and integers

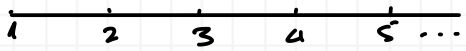
Natural numbers just means positive integers.

Warning: Some people include 0 as a natural number. We don't, but in practice it doesn't matter much.

Notation: The set of all natural numbers is written as $\mathbb{N}$.

This is N written in "blackboard bold". This is usually used for particular sets of numbers.

We are used to visualising $\mathbb{N}$ as a number line:



$\mathbb{N}$ has some useful features:

- addition and multiplication both work in $\mathbb{N}$, and satisfy familiar rules, like $(a+b)+c = a+(b+c)$
  $a(b+c) = ab + ac$.

- $\mathbb{N}$ has an ordering $<$, which also satisfies rules:

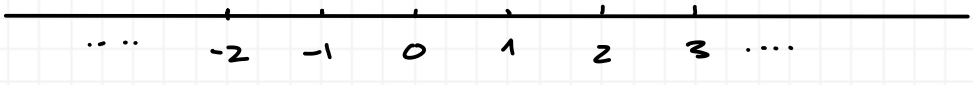
  if $a<b$ and $b<c$, then $a<c$
  if $a<b$, then $a+c < b+c$ and $ac < bc$

But there are things we can't do in $\mathbb{N}$. The most basic one is subtraction: $1, 4 \in \mathbb{N}$, but there is no natural number $1-4$. This means: there is no natural number x such that $x+4=1$.

So we extend to a bigger number system.
$\mathbb{Z}$ denotes the set of all integers.

$$\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, 3, \ldots\}$$

$\mathbb{Z}$ can also be visualised as a number line:



$\mathbb{Z}$ has some nice properties:

- addition and multiplication still work, and satisfy the same rules as before.
- we now have subtraction as well, which satisfies nice rules, like $a-(b+c) = (a-b)-c$
  $c(b-c) = ab-ac.$
- we can extend the order $<$, but we have to be slightly careful: if $a<b$, then
  $ac<bc$ if $c>0$
  $ac>bc$ if $c<0$.

(There is no smallest integer, so we can't do proof by induction in $\mathbb{Z}$.)

4.2 Divisibility and primes

In this section we work mostly in $\mathbb{N}$. Most of the concepts extend naturally to $\mathbb{Z}$, but we don't gain anything.

Definition: Suppose $d, n \in \mathbb{N}$. We say d <u>divides</u> n if $n = dk$ for some $k \in \mathbb{N}$.
We write $d \mid n$ to mean "d divides n".

e.g. $2 \mid 20$ because $20 = 2 \times 10$
$3 \nmid 20$ because there is no $k \in \mathbb{N}$ such that $20 = 3 \times k$.

$d \mid d$ for every $d \in \mathbb{N}$.

$1 \mid n$ for every $n \in \mathbb{N}$.

<u>Warning</u>: Don't confuse

$d \mid n$ "d divides n" is a statement:
it says $n = dk$ for some $k \in \mathbb{N}$

d / n "d divided by n" is a number.

Other ways to say $d \mid n$:

- d is a factor of n
- d is a divisor of n
- n is divisible by d
- n is a multiple of d.

For example, the factors of 12 are

1, 2, 3, 4, 6 and 12.

The multiples of 12 are

12, 24, 36, 48, ...

Lemma 4.1: Suppose $a, b, c \in \mathbb{N}$. If $a \mid b$ and $b \mid c$, then $a \mid c$.

Pf: Since $a \mid b$ and $b \mid c$, there are $k, l \in \mathbb{N}$ such that

$b = ka$ and $c = lb$. So

$c = l(ka) = (lk)a$.

Since $lk \in \mathbb{N}$, this means that $a \mid c$. □

Proof tip: If the theorem says $a \mid b$, write this as $b = ak$ for $k \in \mathbb{N}$. Equations are easier to work with.