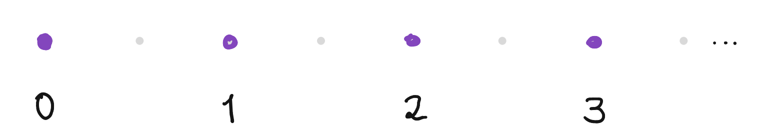
# Lecture 1

## Module 1 - Integers

- Symbol $:=$ (colon-equals) means "by definition" or "will denote".

- The set of natural numbers $\mathbb{N} := \{0, 1, 2, 3, \dots\}$ ← In this course
  - Different people define $\mathbb{N}$ in different ways: $\mathbb{N} := \{1, 2, 3, \dots\}$
  - $\mathbb{N}$ has "an order" $(<)$: $0 < 1 < 2 < 3 < \dots$



- The set of integers $\mathbb{Z} := \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$
  - $\mathbb{Z}$ comes from the German word Zahlen (= number)
  - $\mathbb{Z}$ has "an order" $(<)$ : $\cdots < -3 < -2 < -1 < 0 < 1 < 2 < 3 < \cdots$
  - $\mathbb{N} \subset \mathbb{Z}$

    $\cdots \quad -3 \quad -2 \quad -1 \quad 0 \quad 1 \quad 2 \quad 3 \quad \cdots$

- Axiom: A statement that is self-evident. ← building blocks of a theory

Need to be Proved

Proposition: A statement that is true or false.

Theorem: A very important proposition.

Lemma: A proposition used to prove a theorem.

Corollary: A result from a theorem. Usually has a short proof.

**Well-Ordering Axiom:** Every non-empty subset of $\mathbb{N}$ contains a smallest element.

Ex:


Finite subsets : $\{4, 6, 8, 10\}$ $\qquad$ $\{n, 3n, 9n\}$

Infinite subsets : $\{5, 6, 7, 8, \dots\}$ $\qquad$ $\{10^r \mid r = 2, 3, 4, \dots\}$ $\quad$ 100 is the smallest

- The smallest element lies to the left of all the other elements in the subset.
- The axiom does not hold in $\mathbb{Z}$ because infinite subsets don't have a smallest element.
- The axiom does not hold in $\mathbb{Q} := \{p/q : p, q \in \mathbb{Z}\}$. For example,

$\{1/n \mid n = 1, 2, 3, \dots\}$ does not have a smallest element.

# The Division Algorithm

Dividing 98 by 5 means finding numbers $q$ and $r$ such that

$$98 = 5q + r$$

$$\begin{array}{r}
q \\
b\,\overline{)\,a} \\
\vdots \\
r
\end{array}
\qquad\qquad a = bq + r$$

$$b > 0 \quad \& \quad 0 \leq r < b$$

Quotient

$$\begin{array}{rr}
\text{Divisor} & \begin{array}{r} 19 \\ 5\,\overline{)\,98} \\ \underline{5\phantom{0}} \\ 48 \\ \underline{45} \\ 3 \end{array} \\
\text{Remainder} &
\end{array}
\quad \text{Dividend}$$

We stop when the remainder is less than the divisor

$$98 = 5 \times 19 + 3$$ ← This is how we must think about division

$$\frac{98}{5} = 19 + \frac{3}{5}$$ ← Not this

$98 = 5 \times 19 + 3$

IDEA: Division is just repeated subtraction.

98 divided by 5

subtract multiples of 5

$\vdots$

$\vdots$

until the result is a number less than 5.

$$
\begin{aligned}
98 - 5 \cdot 1 &= 93 \\
98 - 5 \cdot 2 &= 88 \\
98 - 5 \cdot 3 &= 83 \\
98 - 5 \cdot 4 &= 78 \\
98 - 5 \cdot 5 &= 73 \\
&\vdots \\
98 - 5 \cdot 18 &= 8 \\
98 - 5 \cdot 19 &= 3
\end{aligned}
$$

Need to consider the set $\{98 - 5x \mid x \in \mathbb{Z} \text{ and } 98 - 5x \geq 0\}$ and find its smallest element ($r$).

**Theorem:** Let $a, b$ be integers with $b > 0$. Then there exist unique integers $q$ and $r$ such that

$$a = bq + r \quad \text{and} \quad 0 \leq r < b.$$

**Proof:** **Have:** $a, b \in \mathbb{Z}$ and $b > 0$

**Want:**
1. $\exists\, q, r \in \mathbb{Z}$ st $a = bq + r$
2. $0 \leq r < b$
3. $q$ and $r$ must be unique

Suppose we have fixed integers $a$ and $b$ with $b > 0$. Let $S$ be the set

$$S := \{ a - bx \mid x \in \mathbb{Z} \text{ and } a - bx \geq 0 \} \subseteq \mathbb{N}$$

**Step 1:** Show that $S$ is not empty by finding a number $x$ s.t. (such that) $a - bx \geq 0$.

Observe that the number $-|a|$ is s.t. $a - b(-|a|) \geq 0$ :

$b \geq 1$ because by hypothesis $b \in \mathbb{Z}$ and $b > 0$

$\Rightarrow |a| b \geq |a|$ because $|a| \geq 0$

$\Rightarrow |a| b \geq -a$ because $|a| \geq -a$

$\Rightarrow a + b|a| \geq 0$

Thus, $a + b|a| \in S$, i.e. $S \neq \emptyset$.

## Step 2:

Find $q$ and $r$ such that $a = bq + r$ and $r \geqslant 0$.

By step 2 and the Well-Ordering Axiom, $S$ contains a smallest element, call it $r$.

$$r \in S \implies r = a - bq \text{ for some } q \in \mathbb{Z} \ \& \ a - bq \geqslant 0$$

$$\implies r = a - bq \ \& \ r \geqslant 0$$

$$\implies a = bq + r \text{ with } r \geqslant 0$$

STEP 3: $\boxed{\text{Show that } r < b.}$

By contradiction.

because $b > 0$

Suppose that $r \geq b$. Then $r - b \geq 0$ and $r > r - b$.

Observe that $0 \leq r - b = (a - bq) - b = a - b(q+1)$.

because $r = a + bq$ from step 2

Then $r - b$ must be an element of $S$.

Thus we have that

$$\underbrace{r - b < r \quad \text{and} \quad r - b \in S}_{\text{contradiction !!!}}$$

because $r$ was the smallest, not $r - b$.

Then $r < b$. :)

STEP 4: Show that $q$ and $r$ are the only numbers s.t. $a = qb + r$ with $0 \le r < b$.

Suppose there are integers $q_1$ and $r_1$ s.t.

1. $a = qb + r$ and $a = q_1 b + r_1$
2. $0 \le r < b$ and $0 \le r_1 < b$

From 1, $qb + r = q_1 b + r_1$ then $b(q - q_1) = r_1 - r$ $(\star)$

From 2, $-b < -r \le 0$ then $-b < r_1 - r < b$ $(\dagger)$
$0 \le r_1 < b$

By (*) and (†) we have

$$-b < b(q - q_1) < b$$

$$-1 < q_1 - q_1 < 1$$

Since $q - q_1 \in \mathbb{Z}$, then $q - q_1$ must be equal to zero. This is $q - q_1 = 0$, i.e. $q = q_1$.

Using (*) again, $r - r_1 = b(q - q_1) = 0$, i.e. $r = r_1$. $\blacksquare$

# Divisibility (when the remainder is zero)

**Def:** Let $a, b \in \mathbb{Z}$ with $b \neq 0$. We say that b divides $a$ (or that $a$ is a multiple of $b$) if $a = bc$ for some $c \in \mathbb{Z}$.

Notation: $b \mid a$ — b divides $a$ $\qquad$ $b \nmid a$ — b does not divide $a$

**Ex:**

- $(-3) \mid 9$ because $9 = (-3) \times (-3)$
- $5 \nmid 14$ because $14 = 2 \times 7 = (-2) \times (-7)$
- $b \mid 0 \ \forall b \in \mathbb{Z}$ because $0 = b \times 0$ for all $b \in \mathbb{Z}$.
- $1 \mid a \ \forall a \in \mathbb{Z}$ because $a = 1 \times a$ for all $a \in \mathbb{Z}$.