1. **Definition.**

Let S be a subset of $\mathbb{R}$.

Let $\lambda \in S$.

λ is said to be a **least element of** *S if*

$$(\lambda \leq x \text{ whenever } x \in S).$$

Well-Ordering Principle for integers (WOPI).

Let S be a non-empty subset of $\mathbb{N}$.

S has a least element.

Remark. A more formal way to express '*S has a least element*' is: *there exists some $\lambda \in S$ such that λ is a least element of S.*

2. **Theorem (DAN). (Division Algorithm for natural numbers.)**

Let $m, n \in \mathbb{N}$. Suppose $n \neq 0$.

Then there exist some unique $q, r \in \mathbb{N}$ such that $m = qn + r$ and $0 \leq r < n$.

Remark on terminology. In the statement of Theorem (DAN), the numbers q, r are called the **quotient** and **remainder** in the division of m by n.

Proof of Theorem (DAN). The result follows from Lemma (E) and Lemma (U). The argument for Lemma (E) relies on the Well-Ordering Principle for integers.

3. **Lemma (E). (Existence part of Theorem (DAN).)**

Let $m, n \in \mathbb{N}$. Suppose $n \neq 0$.

Then there exist some $q, r \in \mathbb{N}$ such that $m = qn + r$ and $0 \leq r < n$.

Lemma (U). (Uniqueness part of Theorem (DAN).)

Let $m, n \in \mathbb{N}$. Suppose $n \neq 0$.

Let $q, r, q', r' \in \mathbb{N}$.

Suppose $m = qn + r$ and $0 \leq r < n$ and $m = q'n + r'$ and $0 \leq r' < n$.

Then $q = q'$ and $r = r'$.

What is Theorem (DAN) about, in plain words?

Answer. It tells us that, given any $m \in \mathbb{N}$, $n \in \mathbb{N} \setminus \{0\}$, there is one and only one correct answer to the school maths question on 'long division' below:

? ← 'quotient'

n) m

?? ← 'remainder'

The argument for the 'existence part' of Theorem (DAN) suggests an 'algorithm' for finding the answer to the question above. This 'algorithm' is probably what we came across as motivation for the notion of division (for natural numbers) in school maths:

School maths problem:

How many apples will remain from a bag with 100 apples if they are to be distributed fairly to 13 children and the maximum number of apples are given away?

'Solution':

$100 - 13 = 87$

$87 - 13 = 74$

$74 - 13 = 61$

$61 - 13 = 48$

$48 - 13 = 35$

$35 - 13 = 22$

$22 - 13 = 9$ ← Stop the distribution at this point. ($9 - 13 = ???$) 9 apples remain.

4. **Proof of Lemma (E).**

Let $m, n \in \mathbb{N}$. Suppose $n \neq 0$.

[Idea for the argument.
Remember that we want to name appropriate natural numbers q, r satisfying both $m = qn + r$ and $0 \leq r < n$.
We put these two conditions in the form $0 \leq m - qn = r < n$.
This suggests we look for a candidate for r from the list of natural numbers

$$m - 0 \cdot n, m - 1 \cdot n, m - 2n, m - 3n, \cdots$$

This is a descending arithmetic progression. Does it terminate or not?
It has to terminate; otherwise, it would 'descend into the negative integers'.
A candidate for r is 'located' where this list terminates. (Why?)
With this candidate for r we also obtain a candidate for q. Now we are ready to proceed with the formal argument.]

Proof of Lemma (E).

Let $m, n \in \mathbb{N}$. Suppose $n \neq 0$.

(Ea) Define $S = \{x \in \mathbb{N} : \text{There exists some } k \in \mathbb{N} \text{ such that } x = m - kn\}$.

By definition, S is a subset of $\mathbb{N}$.

[Ask: Is S the empty set or not?]

Note that $m = m - 0 \cdot n$ and $0 \in \mathbb{N}$. Therefore $m \in S$. Then $S \neq \emptyset$.

Hence S is a non-empty subset of $\mathbb{N}$. By (WOP I), S has a least element, say, r.

(Eb) Since $r \in S$, we have $r \in \mathbb{N}$.

Also, since $r \in S$, there exists some $q \in \mathbb{N}$ such that $r = m - qn$.

So $m = qn + r$ for these q, r.

(Ec) [Ask: $0 \leq r < n$?]

By definition, $r \geq 0$.

We verify that $r < n$:

- [Proof-by-contradiction argument]

  Suppose it were true that $r \geq n$.

  Write $\hat{r} = r - n$.

  We would have $\hat{r} \in \mathbb{N}$ and $\hat{r} < r$.

  Note that

  $$\hat{r} = r - n = m - qn - n = m - (q+1)n.$$

  Since $q \in \mathbb{N}$, $q + 1 \in \mathbb{N}$.

  Then $\hat{r} \in S$.

  But r is a least element of S.

  Contradiction arises. □

5. **Proof of Lemma (U)**.

Let $m, n \in \mathbb{N}$. Suppose $n \neq 0$.

Suppose $q, r, q', r' \in \mathbb{N}$.

Suppose $m = qn + r$ and $0 \leq r < n$ and $m = q'n + r'$ and $0 \leq r' < n$.

We have

$$qn + r = m = q'n + r'.$$

Then $(q - q')n = r' - r$.

Therefore $|q - q'| \cdot n = |r' - r|$. (Why?)

Since $0 \leq r \leq n-1$ and $0 \leq r' \leq n-1$,

$$|r' - r| \leq n - 1.$$

Now $0 \leq |q - q'| \cdot n = |r' - r| \leq n - 1$. —— $(\ast)$

Since $|q - q'| \in \mathbb{N}$, we have $|q - q'| \cdot n = 0$ or $|q - q'| \cdot n \geq n$.

By $(\ast)$, we have $|q' - q| \cdot n = 0$. Then $|q' - q| = 0$.

Therefore $q' = q$. Hence $r' = r$ also. $\square$

Corollary (DAZ1). (Division Algorithm for integers.)

Let $m, n \in \mathbb{Z}$. Suppose $n > 0$.

Then there exist some unique $q, r \in \mathbb{Z}$ such that $m = qn + r$ and $0 \leq r < n$.

Corollary (DAZ2). (Division Algorithm for integers.)

Let $m, n \in \mathbb{Z}$. Suppose $n \neq 0$.

Then there exist some unique $q, r \in \mathbb{Z}$ such that $m = qn + r$ and $0 \leq r < |n|$.

Proof of Corollary (DAZ2). Exercise.

Remark on terminology. In each of Corollary (DAZ1) and Corollary (DAZ2), the numbers q, r are called the **quotient** and **remainder** in the division of m by n.

6. **Corollary (DAZ1). (Division Algorithm for integers.)**

Let $m, n \in \mathbb{Z}$. Suppose $n > 0$.

Then there exist some unique $q, r \in \mathbb{Z}$ such that $m = qn + r$ and $0 \leq r < n$.

Proof of Corollary (DAZ1).

(a) ['Existence argument'.] Let $m, n \in \mathbb{Z}$. Suppose $n > 0$. Note that $m \geq 0$ or $m < 0$.

- (Case 1). Suppose $m \geq 0$. Then, by Theorem (DAN), there exists some $q, r \in \mathbb{N}$ such that $m = qn + r$ and $0 \leq r < n$.
- (Case 2). Suppose $m < 0$. [Idea: Is there an integer in the list

$$m + 0 \cdot n, m + 1 \cdot n, m + 2n, m + 3n, \cdots$$

which is non-negative? If yes, can we apply Theorem (DAN) to this non-negative integer?]

Note that $-m \in \mathbb{N}$. Since $n > 0$, we have $m + (-m)n = -m(n-1) \in \mathbb{N}$.
By Theorem (DAN), there exists some $p, r \in \mathbb{N}$ such that $m + (-m)n = pn + r$ and $0 \leq r < n$.

Now define $q = p + m$. Since $p, m \in \mathbb{Z}$, we have $p + m \in \mathbb{Z}$.
For these q, r, we have $m = -(-m)n + pn + r = (m+p)n + r = qn + r$.

(b) ['Uniqueness argument'.] Exercise.

7. Refer to Theorem (2) in the Handout *De Moivre's Theorem and roots of unity:*

Let n be a positive integer. Write $\theta_n = \dfrac{2\pi}{n}$. *Define* $\omega_n = \cos(\theta_n) + i\sin(\theta_n)$.

(a) ω_n *is an n-th root of unity.*

(b) *The n-th roots of unity are the n complex numbers of modulus 1, given by* 1, $\omega_n, \omega_n^{\,2}, \ldots, \omega_n^{\,n-1}$.

Corollary (DAZ1) is the tacit assumption needed in the argument for this result.

8. **Theorem (DIV).**

Let $m, n \in \mathbb{Z}$. Suppose $n \neq 0$. m is divisible by n iff the remainder is 0 in the division of m by n.

Proof of Theorem (DIV). Exercise.

Remark. This result provides the connection between the definition of divisibility and Division Algorithm.

Definition.

Let $n \in \mathbb{Z}$.

(a) *n is said to be* **even** *if n is divisible by 2.*

(b) *n is said to be* **odd** *if n is not divisible by 2.*

Theorem (O). (Equivalent formulation of the definition of odd-ness for integers.)

Let $n \in \mathbb{Z}$. The statements (†), (‡) are logically equivalent:

(†) *n is odd.*

(‡) *There exists some $k \in \mathbb{Z}$ such that $n = 2k + 1$.*

Proof of Theorem (O). Exercise.