37181 DISCRETE MATHEMATICS

Lecture 6: division and remainder; Euclidean algorithm

PLAN

- Division and remainder lemma
- Euclidean algorithm

RECALL

$\mathbb{N} = \{0, 1, 2, 3, \dots\}$ is the set of all *natural numbers*. For this subject, it will always contain 0.

An element s in a subset $S \subseteq \mathbb{N}$ is called a *first element* in S if $s \leqslant x$ for every $x \in S$.

Eg: $\{5, 4, 6, 7\}$ has a first element, 4.

RECALL

$\mathbb{N} = \{0, 1, 2, 3, \dots\}$ is the set of all *natural numbers*. For this subject, it will always contain 0.

An element s in a subset $S \subseteq \mathbb{N}$ is called a *first element* in S if $s \leqslant x$ for every $x \in S$.

Eg: $\{5, 4, 6, 7\}$ has a first element, 4.

Lemma

First elements are unique.

RECALL

$\mathbb{N} = \{0, 1, 2, 3, \dots\}$ is the set of all *natural numbers*. For this subject, it will always contain 0.

An element s in a subset $S \subseteq \mathbb{N}$ is called a *first element* in S if $s \leqslant x$ for every $x \in S$.

Eg: $\{5, 4, 6, 7\}$ has a first element, 4.

Lemma

First elements are unique. *(So we can say "the" first element).*

RECALL

$\mathbb{N} = \{0, 1, 2, 3, \dots\}$ is the set of all *natural numbers*. For this subject, it will always contain 0.

An element s in a subset $S \subseteq \mathbb{N}$ is called a *first element* in S if $s \leqslant x$ for every $x \in S$.

Eg: $\{5, 4, 6, 7\}$ has a first element, 4.

Lemma

First elements are unique. *(So we can say "the" first element).*

Axiom (Well ordering principle)

Every non-empty subset of $\mathbb{N}$ has a first element.

axiom = fact which does not follow from other facts.

Lemma

Let $n, d \in \mathbb{Z}$ with $d > 0$. Then there exist $q, r \in \mathbb{Z}$ with $0 \leqslant r < d$ such that $n = qd + r$.

Proof:

Lemma

Let $n, d \in \mathbb{Z}$ with $d > 0$. Then there exist $q, r \in \mathbb{Z}$ with $0 \leqslant r < d$ such that $n = qd + r$.

Proof: Define $M = \{n - qd \mid q \in \mathbb{Z}\}$.

Lemma

Let $n, d \in \mathbb{Z}$ with $d > 0$. Then there exist $q, r \in \mathbb{Z}$ with $0 \leqslant r < d$ such that $n = qd + r$.

Proof: Define $M = \{n - qd \mid q \in \mathbb{Z}\}$. Then $M \cap \mathbb{N}$ is a subset of $\mathbb{N}$.

Lemma

Let $n, d \in \mathbb{Z}$ with $d > 0$. Then there exist $q, r \in \mathbb{Z}$ with $0 \leqslant r < d$ such that $n = qd + r$.

Proof: Define $M = \{n - qd \mid q \in \mathbb{Z}\}$. Then $M \cap \mathbb{N}$ is a subset of $\mathbb{N}$.

It is non-empty because if $n \geqslant 0$ you can take $q = 0$ and if $n < 0$ take $q = 100n$ (which is a negative number, so $-qd$ is a big positive number).

Lemma

Let $n, d \in \mathbb{Z}$ with $d > 0$. Then there exist $q, r \in \mathbb{Z}$ with $0 \leqslant r < d$ such that $n = qd + r$.

Proof: Define $M = \{n - qd \mid q \in \mathbb{Z}\}$. Then $M \cap \mathbb{N}$ is a subset of $\mathbb{N}$.

It is non-empty because if $n \geqslant 0$ you can take $q = 0$ and if $n < 0$ take $q = 100n$ (which is a negative number, so $-qd$ is a big positive number).

Therefore by the well ordering principle $M \cap \mathbb{N}$ has a first element, call it r.

Since $r \in M \cap \mathbb{N}$ we have $r \geqslant 0$ and $r = n - qd$ for some $q \in \mathbb{Z}$.

Since $r \in M \cap \mathbb{N}$ we have $r \geqslant 0$ and $r = n - qd$ for some $q \in \mathbb{Z}$.

If $r \geqslant d$ (for contradiction) then $r - d \geqslant 0$ and $r - d = n - (q + 1)d$ so belongs to $M \cap \mathbb{N}$, and is smaller than r, contradicting our choice of r as first element. $\square$

APPLICATION OF DIVISION LEMMA

Definition

Let $a, b \in \mathbb{Z}$. Then $d \in \mathbb{N}$ is called the *greatest common divisor* of a and b if $d \mid a$, $d \mid b$, and if $c \mid a, c \mid b$ then $c \mid d$.

Eg: compute

- $\gcd(3, 9)$
- $\gcd(6, 8)$

APPLICATION OF DIVISION LEMMA

Definition

Let $a, b \in \mathbb{Z}$. Then $d \in \mathbb{N}$ is called the *greatest common divisor* of a and b if $d \mid a$, $d \mid b$, and if $c \mid a, c \mid b$ then $c \mid d$.

Eg: compute

- $\gcd(3, 9)$
- $\gcd(6, 8)$

The following algorithm claims to compute $\gcd$. It is called the *Euclidean algorithm*. We should not believe this claim, until we know how to prove algorithms are correct (lecture 8):

1. stops 2. gives the correct output

EUCLIDEAN ALGORITHM

Input $54, 186$.

Use the lemma to write $186 = q_1 \cdot 54 + r_1, \quad 0 \leqslant r_1 < 54$

EUCLIDEAN ALGORITHM

Input $54, 186$.

Use the lemma to write $186 = q_1 \cdot 54 + r_1, \quad 0 \leqslant r_1 < 54$

Use the lemma to write $54 = q_2 \cdot r_1 + r_2, \quad 0 \leqslant r_2 < r_1$

Repeat until you get $r_i = 0$.

YOUR TURN

Input $154, 287$.

Use the lemma to write $287 = q \cdot 154 + r$.

Repeat until you get $r = 0$.

ONE MORE PROOF

Lemma

Let $n, d \in \mathbb{Z}$ with $d > 0$. Then there exist unique integers q, r with $0 \leqslant r < d$ such that $n = qd + r$.

Proof.

ONE MORE PROOF

Lemma

Let $n, d \in \mathbb{Z}$ with $d > 0$. Then there exist unique integers q, r with $0 \leqslant r < d$ such that $n = qd + r$.

Proof.

We already proved some q, r values exist. Suppose they are not unique.

ONE MORE PROOF

Lemma

Let $n, d \in \mathbb{Z}$ with $d > 0$. Then there exist unique integers q, r with $0 \leqslant r < d$ such that $n = qd + r$.

Proof.

We already proved some q, r values exist. Suppose they are not unique.

Then we have q_1, q_2, r_1, r_2 and $n = q_1 d + r_1 = q_2 d + r_2$ so

Lemma

Let $n, d \in \mathbb{Z}$ with $d > 0$. Then there exist unique integers q, r with $0 \leqslant r < d$ such that $n = qd + r$.

Proof.

We already proved some q, r values exist. Suppose they are not unique.

Then we have q_1, q_2, r_1, r_2 and $n = q_1 d + r_1 = q_2 d + r_2$ so $r_1 - r_2 = d(q_2 - q_1)$.

This means d divides $r_1 - r_2$, but since they are both between 0 and $d - 1$ we must have $r_1 - r_2 = 0$, so $r_1 = r_2$ and then $q_1 - q_2 = 0$ so $q_1 = q_2$. □

NEXT

Next week:

- induction
- correctness of computer code