37181 DISCRETE MATHEMATICS

Lecture 6: division and remainder; Euclidean algorithm

PLAN

- Division and remainder lemma
- Euclidean algorithm

RECALL

$\mathbb{N} = \{0, 1, 2, 3, \ldots\}$ 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.

$\mathbb{N} = \{0, 1, 2, 3, \dots\}$ 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.

only one.

Lemma

First elements are unique.

Proof: Suppose $S \subseteq \mathbb{N}$, $b, c \in S$, $b \neq c$, and b, c both first elements.

(contradiction)

Treating b as a first element and $c \in S$ any element then $b \leq c$

Now, taking c as first element and $b \in S$ any element

then $c \leq b$.

But $b \leq c$ and $c \leq b$ implies $b = c$. Contradiction! $\square$

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

$\mathbb{N} = \{0, 1, 2, 3, \ldots\}$ 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 $n = qd + r$.

remainder

Proof:

$n = 50 \quad d = 17$

$50 = \underbrace{2}\,17 + \underbrace{16}_{0 \leq \quad < 17}$

34
16

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 $n = qd + r$.

n, d fixed, given to us.

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

50, 17

	M
q=0	50
1	33
2	
3	
-1	67
-2	⋮
⋮	⋮

APPLICATION: DIVISION AND REMAINDER

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 $\mathbb{N}$.

nonempty
subset
of $\mathbb{N}$
$\rightarrow$ first element.

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 $\mathbb{N}$.

$n - 0 \cdot d = n \in M$ ✓

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).

$$-qd = \underbrace{-100 \cdot n \cdot d}_{pos} \qquad \begin{array}{l} d > 0 \\ n < 0 \end{array}$$

$$n - qd = n - 100nd = \underbrace{n}_{neg}(\underbrace{1 - 100d}_{neg})$$

$pos.$

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 $n = qd + r$.

"create me"

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 $q \in \mathbb{Z}$.

$\forall n, d \quad \exists q, r$

$n = qd + r$

$0 \leq r <^{?} d$

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

Need to show $r < d$.

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. $\square$

Definition

$d \geq 0$

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

- $\boxed{\text{gcd}(3, 9) = 3}$
- $\boxed{\text{gcd}(6, 8) = 2}$

$d = 3$:

$3 \mid 3 \qquad 3 \mid 9$

$1 \mid 3 \qquad 1 \mid 9$

-1

$-3 \mid 3 \qquad -3 \mid 9$

$9 = (-3)(-3)$

$1 \mid 6 \qquad 1 \mid 8$

$2 \mid 6 \qquad 2 \mid 8$

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

- $\mathbf{gcd}(3, 9)$

- $\mathbf{gcd}(6, 8)$

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

Input 54, 186.

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

$$\begin{array}{r} 54 \\ 3 \\ \hline 162 \end{array}$$

$186 = 3 \cdot 54 + 24$

$54 = q_2 24 + r_2$

$0 \leq r_2 < 24$

$$\begin{array}{r} 54 \\ 48 \\ \hline 6 \end{array}$$

$54 = 2 \cdot 24 + 6$

$24 = q_3 6 + r_3$

$0 \leq r_3 < 6$

$24 = 4 \cdot 6 + 0$

OUTPUT

STOP when $r_i = 0$

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 $r_i = 0$.

$$\begin{array}{r} 21 \\ 6 \\ \hline 126 \end{array}$$

Input 154, 287.

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

Repeat until you get $r = 0$.

$287 = 1 \cdot 154 + 133$

$154 = 1 \cdot 133 + 21$

$133 = 6 \cdot 21 + 7$

$21 = 3 \cdot 7 + 0$

OUTPUT

STOP

Claim:

$\boxed{\gcd(154, 287) = 7}$

Lemma

only one

a / pair of

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

Proof.

We already showed q, r exist. ✓ ✓

Suppose $\exists (q_1, r_1), (q_2, r_2) \in \mathbb{Z}$ and $(q_1, r_1) \neq (q_2, r_2)$

$0 \leq r_1 < d$, $0 \leq r_2 < d$

$n = q_1 d + r_1 = q_2 d + r_2$.

$(q_1 - q_2) \cdot d = r_2 - r_1$

$-d < (r_2 - r_1) < d$

Contradiction.

$\Rightarrow q_1 - q_2 = 0 \Rightarrow r_1 = r_2$

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.

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 $q_1 = q_2$. $\square$

NEXT

Next week:

- induction
- correctness of computer code