Lecture 4: The Division Algorithm

Def: Let a, b be integers. We say that "a divides b" and write $a \mid b$, if there exists an integer q, such that $b = qa$.

Ex: $2 \mid 12$, because $12 = 4 \cdot 3$
(a = "2", b = "12", q = "4")

$-3 \mid 12$, " $12 = (-4)(-3)$

$2 \nmid 5$.

$0 \mid 5$ because $5 = q \cdot 0$ does not have an integer solution q.

Prop 2.11: Let a, b, c be integers.

(i) (transitivity) If $a \mid b$ and $b \mid c$, then $a \mid c$.

(ii) If $a \mid b$ and $a \mid c$, then $a \mid (xb + yc)$, for every integers x, y. In particular, $a \mid b+c$ and $a \mid b-c$.

(iii) If $a \mid b$ and $b \mid a$, then $|a| = |b|$.

(iv) If $a \mid b$ and $b \neq 0$, then $|a| \leq |b|$.

Proof: (i) Assume that $a \mid b$ and $b \mid c$. Then there exist integers q_1, q_2 such that $b = q_1 a$ and $c = q_2 b$.

So $c = q_2 b = q_2(q_1 a) = (q_2 q_1) a$, where $q_2 q_1 \in \mathbb{Z}$.

So $a \mid c$.

(ii) Assume that $a \mid b$ and $a \mid c$, so there exist integers q_1, q_2 such that $b = q_1 a$ and $c = q_2 a$. Let x, y be integers. Then

$$xb + yc = x(q_1 a) + y(q_2 a) = (\underbrace{x q_1 + y q_2}_{q}) a.$$

Hence $a \mid xb + yc$.

(iii) Assume that $a \mid b$ and $b \mid a$. Then there exist integers q, r such that $b = qa$ and $a = rb$.

So $\boxed{b = qa = q(rb) = (qr)b.}$ (†)

If $b = 0$, then $a = 0$, since $b \mid a$.

If $b \neq 0$, then (†) implies that $qr = 1$. So either

$q = r = 1$ or $q = -1 = r$,

$\Downarrow$

$b = qa = 1 \cdot a$

$\Downarrow$ w

1

$b = qa = -a$,

$\Downarrow$ w

-1

So $b = a$

So $|b| = |a|$

So $|b| = |a|$.

iv) Assume $a \mid b$ and $b \neq 0$.

Then $b = qa$, for some integer $q \neq 0$.

So $|b| = |q||a| \geq |a|$.

$\Downarrow$ w

1

Q.E.D

Theorem: (The Division Algorithm)

If a and b are integers, with $b > 0$, then there exists a unique pair of integers q, r such that $a = qb + r$, where

$0 \le r < b$.

Note: r is called the REMAINDER of division of a by b.

Ex: $a = 17$, $b = 3$,

$$\underset{a}{17} = \underset{q}{5} \cdot \underset{b}{3} + \underset{r}{2}$$

Let $a = -17$, $b = 3$. Then

$$-17 = \underset{q}{(-6)}3 + \underset{r}{1}$$

Proof:

Existence: case $a \ge 0$

[We are looking for $q, \underset{\ge 0}{r}, b$ such that $a = qb + r$]

Consider the set

$$S = \{ x \in \mathbb{Z},\ x \ge 0,\ \underset{\ge 0}{x}b \le a \}.$$

The set S is finite. Choose q to be the maximal element of S, set $r = a - qb$.
Check that indeed $0 \le r < b$.

Case $a < 0$: Let S be the set $S = \{x \text{ integer}, x \le 0 : xb > a\}$
S is a finite set.
Choose $q := -1 + \min(S)$.
Then $q \notin S$, $q+1 \in S$.

(*) $qb \le a$ (because $q \notin S$)

(**) $(q+1) \cdot b > a$. ($\vee$ $q+1 \in S$)

So $r := a - qb \ge 0$, by (*), and
$r = a - qb < b$, by (**).

Uniqueness: Assume that

$a = q_1 b + r_1$ and $a = q_2 b + r_2$

where $0 \leq r_1, r_2 < b$.

So $0 = a - a = (q_1 b + r_1) - (q_2 b + r_2)$

$= (q_1 - q_2) b + (r_1 - r_2)$.

So $r_2 - r_1 = (q_1 - q_2) b$,

So $b \mid (r_2 - r_1)$.

We show that $r_2 - r_1 = 0$, by contradiction. If $r_2 - r_1 \neq 0$, then

$b = |b| \leq |r_2 - r_1|$, by Prop 2.11 (ii).

Now

$$-b < -r_1 \leq \underset{\substack{\vee\\ 0}}{\overset{\substack{b\\ \vee}}{r_2}} - \underset{\substack{\vee\\ 0}}{\overset{\substack{b\\ \vee}}{r_1}} \leq r_2 < b$$

So $|r_2 - r_1| < b$. A contradiction. Hence $r_2 - r_1 = 0$

So $r_2 = r_1$.

$r_1 = a - q_1 b =$

$r_2 = a - q_2 b$

So $a - q_1 b = a - q_2 b$.

So $q_1 b = q_2 b$

So $q_1 = q_2$ (since $b \neq 0$).

Hence $(q_1, r_1) = (q_2, r_2)$. Q.E.D

Example: $a = 381$, $b = 72$.

Then $381 = 5 \cdot 72 + 21$.

q r

$0 \leq r < 72$

Def; Let a, b be two integers.

1) An integer c is a COMMON DIVISOR of a and b if $c \mid a$ and $c \mid b$.

2) Assume that $a \neq 0$ OR $b \neq 0$.

The GREATEST COMMON DIVISOR of a and b, denoted by $\gcd(a, b)$, is the largest (positive) integer dividing both a and b.

Note; If $c \mid a$ and $c \mid b$, and $a \neq 0$, then $|c| \leq |a|$, by Prop 2.11 (2V).

So the set $\{c : c \text{ and } c \mid a \text{ and } c \mid b\}$ is finite, since every element c in this set satisfies

$|c| \leq \max\{|a|, |b|\}$.

Def: $\gcd(0,0) \overset{\text{def}}{:=} 0$.

Ex: $\gcd(2,3) = 1$.

$\gcd(6,10) = 2$.

$\gcd(6,-10) = 2$

$\gcd(6,0) = 6$.

$\gcd(a,0) = |a|$.

$\gcd(a,b) = \gcd(|a|,|b|)$.

Ex: Let $a = 381$, $b = 72$

Find $\gcd(381, 72)$.

Improvement step:

$$\underset{a}{381} = \underset{q_1}{5} \cdot \underset{b}{72} + \underset{r_1}{21}$$

Claim: $\gcd(381, 72) = \gcd(72, 21)$.

$$gcd(a,b) = gcd(b, r_1)$$
$$\uparrow$$
$$b$$

Prop: If a, b are integers and $a = qb + r$, then

$$gcd(a,b) \overset{(\dagger)}{=} gcd(b, r).$$

Proof: If $a = 0$ and $b = 0$, then $r = 0$ and the equality $(\dagger)$ holds. So assume that one of a or b is non-zero. Then one of b or r is non-zero.

In order to show equality $(\dagger)$ it suffices to show that the sets

$$S = \{c : c \mid a \text{ and } c \mid b\}$$ is equal to the set

$$T = \{c : c \mid b \text{ and } c \mid r\}$$

$S \subseteq T$:
Assume that $c \in S$. Then $c \mid a$ and $c \mid b$.
Then $c \mid \underbrace{a - qb}_{= r}$, by Prop 2.11 (ii).
So $c \mid a$ and $c \mid r$, so $c \in T$.

$T \subseteq S$: Assume that $c \in T$. Then
$c \mid b$ and $c \mid r$. So
$c \mid \underbrace{qb + r}_{a}$, by Prop 2.11 (ii).
So $c \mid b$ and $c \mid a$. So $c \in S$.
Hence $S = T$. Q.E.D

Ex: Find $\gcd(381, 72)$, $a > b$.

$381 = 5 \cdot 72 + 21$. Hence

$a = 381$, $q_1 = 5$, $b = 72$, $r_1 = 21$.

$\gcd(381, 72) = \gcd(72, 21)$. (Prop above)

$72 = 3 \cdot 21 + 9$ (Division Alg)

$b = 72$, $q_2 = 3$, $r_1 = 21$, $r_2 = 9$, $0 \leq r_2 < 21$

$\gcd(72, 21) = \gcd(21, 9)$ (Prop above)

$r_1 = 21$, $r_2 = 9$

Division Alg:

$21 = 2 \cdot 9 + 3$

$r_1 = 21$, $q_3 = 2$, $r_2 = 9$, 3

$\gcd(21, 9) = \gcd(9, 3)$. (Prop above)

Division Alg:

$$\underbrace{9}_{r_2} = \underbrace{3}_{q_3} \cdot \underbrace{3}_{r_3} + \underbrace{0}_{r_4}$$

$$\gcd(9,3) \overset{\text{prop above}}{=} \gcd(3,0) = \boxed{3} = r_3$$

Theorem: (Euclidean Algorithm)

Let a, b be positive integers with $b < a$.

(i) If $b \mid a$, then $\gcd(a,b) = b$.

(ii) If $b \nmid a$, then $\gcd(a,b)$ is the last non-zero remainder r_n in the following list of equation obtained by repeated application of the division algorithm;

Eq 1: $a = q_1 b + r_1$, $0 < r_1 < b$.

Eq 2: $b = q_2 r_1 + r_2$, $0 \le r_2 < r_1$.
(if $r_2 \neq 0$)

$r_1 = q_3 r_2 + r_3$, $0 \le r_3 < r_2$

$\vdots$

$r_{n-2} = q_n r_{n-1} + r_n$, $0 \le r_n < r_{n-1}$,

Eq n-1 $r_{n-1} = q_{n+1} r_n + \underbrace{0}_{r_{n+1}}$

non-zero by assumption

Proof: (i) If $a > b > 0$ and $b \mid a$, and c is a common divisor, then $|c| \le |b| = b$, by Prop 2.11 (iv). Hence $|c| \le b$. Now b is a common divisor of a, b. So $b = \gcd(a, b)$.

(ii) $\gcd(a,b) \overset{\text{Eq 1}}{=} \gcd(b, r_1) \overset{\text{Eq 2}}{=} \gcd(r_1, r_2) =$

+ Prop + Prop

$= \cdots = \gcd(r_{n-1}, r_n) = \gcd(r_n, 0)$

$= r_n$

$r_n = s \cdot r_{n-1} + t \cdot r_{n-2}$

Q.E.D