Lecture 2

The division algorithm

$$\begin{array}{r} 7 \\ 6\,\overline{)\,44} \\ \underline{42} \\ 2 \end{array}$$

$$\underbrace{44}_{a} = \underbrace{7}_{q} \cdot \underbrace{6}_{b} + \underbrace{2}_{\substack{r = \text{remainder} \\ \geq 0}}$$

Thm: (The Division Theorem)

Let $a \in \mathbb{Z}$ and $b \in \underbrace{\mathbb{N}}_{\text{positive integers}}$.

Then there EXISTS a UNIQUE pair of integers q, r, with $\boxed{0 \leq r < b}$, such that

$$\boxed{a = qb + r.}$$

Ex: $a = -111$, $b = 12$,

$q = -10$, $\quad -111 = \underbrace{\overbrace{-10}^{q} \cdot 12}_{-120} + \underbrace{9}_{r}$

Proof: (Existence):

Let T = set of all non-negative remainders

$\left\{ a - xb \; ; \; x \in \mathbb{Z} \text{ and } a - xb \geq 0 \right\}$

Let $r \overset{def}{:=} \min(T)$.

Write $a - qb = r$, so $a = qb + r$.

We claim that $r < b$.

Indeed $r - b = a - qb - b = a - (q+1)b$ it is a remainder, so it must be negative, since it is smaller than r,

<u>Uniqueness:</u> Suppose that

$\boxed{q_2 b + r_2 = a = q_1 b + r_1}$ and

$0 \leq r_i < b$, for $i = 1$ and 2,

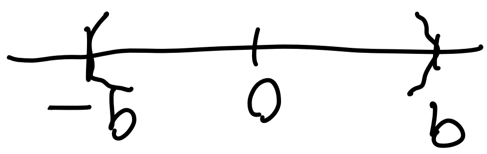
$$q_2 b + r_2 - (q_1 b + r_2) = 0$$

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

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

so $b \mid r_2 - r_1$. Note that

$$-b < -r_1 \leq (r_2 - r_1) \leq r_2 < b$$



So $r_2 - r_1 = 0$. So $r_2 = r_1 = r$.

$$q_2 b + r = q_1 b + r$$

So $q_2 b = q_1 b$, $b > 0$

So $q_2 = q_1$. So

$(q_1, r_1) = (q_2, r_2)$. $\square$

<u>Lemma</u>: (3.5.2) Any common multiple of two integers a, b is also a multiple of $\operatorname{lcm}(a, b)$.

<u>Rephrasing</u>: Let $a, b \in \mathbb{Z}$, not both zero. If $a \mid x$ and $b \mid x$, then $\operatorname{lcm}(a, b) \mid x$.

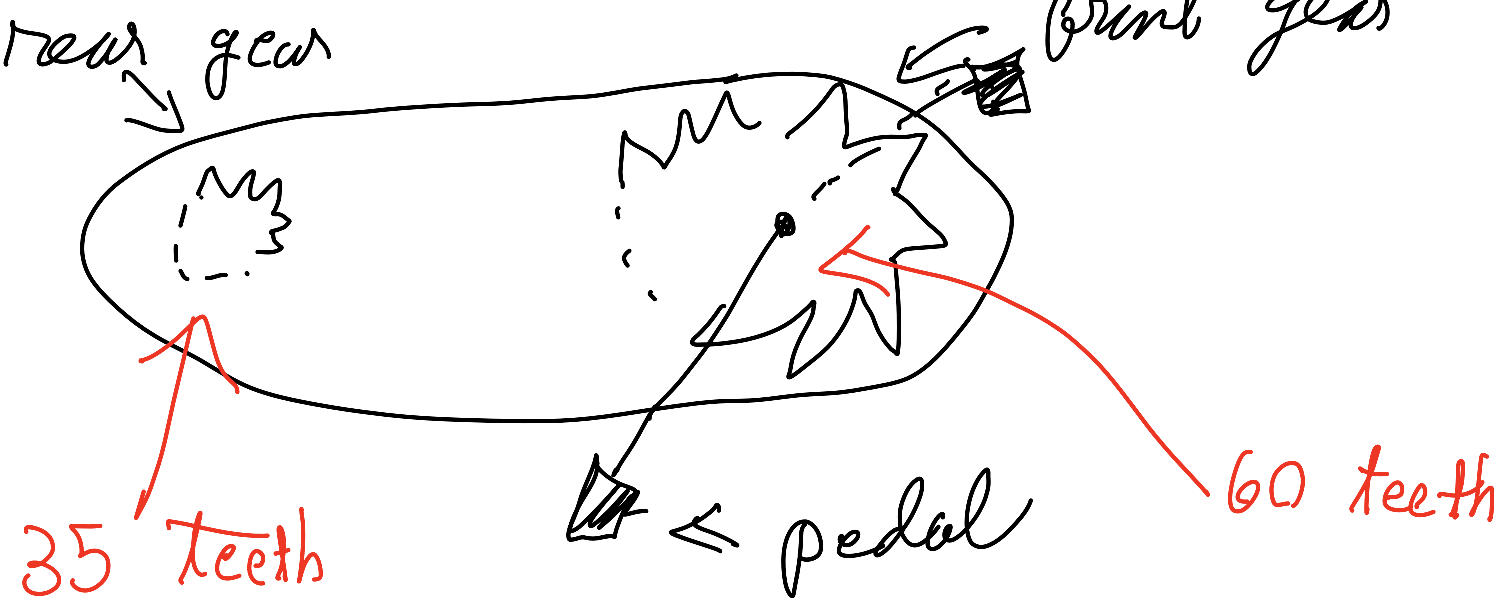
<u>Proof</u>: Using the Division Thm, there exists (a unique) pair (q, r) with $0 \leq r < \operatorname{lcm}(a, b)$,

such that $x = q \cdot \operatorname{lcm}(a,b) + r$.
It remains to show that $r = 0$.

Both x and $\operatorname{lcm}(a,b)$ are divisible by a and by b.
So $r = 1 \cdot x - q \cdot \operatorname{lcm}(a,b)$ is also divisible by both a, b, so r is a common multiple of a and b. But $0 \le r < \operatorname{lcm}(a,b)$
So $r = 0$, (otherwise, it would be a positive common multiple strictly less than $\operatorname{lcm}(a,b)$).
$\square$

Example: (Involving lcm).

Consider a bicycle with two gears (front and rear)



The front gear of a bicycle has 60 teeth and the rear gear has 35 teeth. After how many full rotations of the pedals, will both gears return to their original position.

Answer: Let x = the numbers of chainlinks that get rotated. Then $35 | x$ and $60 | x$, when $x = lcm(35, 60)$ the gear return to their original position for the first time.

$$\#\text{rotations} = \frac{x}{60} = ?$$

$$35 = 5 \cdot 7, \quad 60 = 3 \cdot 2^2 \cdot 5$$

$$x = \operatorname{lcm}(35, 60) = 2^2 \cdot 3 \cdot 5 \cdot 7 = 60 \cdot 7 = 420$$

$$\frac{x}{60} = 7 = \#\text{ full rotations.} \quad \square$$

Ch 4:

Sec 4.1 The Euclidean Alg

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

$$a = q_1 \cdot b + r_1$$

$$\underset{a}{381} = \underset{\substack{\vee \\ 5}}{q_1} \cdot 72 + \underset{\substack{\shortparallel \\ r_1}}{\boxed{21}}$$

$$0 \le r_1 < \underset{\substack{\shortparallel \\ 72}}{b}$$

We claim that
$$\gcd(\underset{(a}{381}, \underset{b)}{72}) = \gcd(\underset{(b,}{72}, \underset{r_1)}{21})$$

Lemma: Let $a \in \mathbb{Z}$, $b \in \mathbb{N}$ (positive integer).

Write $\boxed{a = qb + r}$, $0 \le r < b$.

Then $\gcd(a, b) = \gcd(b, r)$.

Proof: We will show that

$$A = \{c : c \mid a \text{ and } c \mid b\} = \{c ; c \mid b \text{ and } b \mid r\} = B.$$

($\subseteq$) Assume that $c \mid a$ and $c \mid b$.

Then $c \mid 1 \cdot a - qb = r$, so $c \mid r$.

So $c \in B$.

($\supseteq$) If $c \mid b$ and $c \mid r$, then

$c \mid q \cdot b + 1 \cdot r = a$, so $c \mid a$.

So $c \in A$. $\square$

$\gcd(381, 72)$

$$\underbrace{381}_{a} = \underbrace{5}_{q_1} \cdot \underbrace{72}_{b} + \underbrace{21}_{r_1} \qquad \gcd(72, 21)$$

$$\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad ||$$

$$72 = \underbrace{\boxed{3}}_{q_2}\, \underbrace{21}_{r_1} + \underbrace{\boxed{9}}_{r_2} \qquad \gcd(21, 9)$$

$$\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad ||$$

$$21 = \underbrace{\boxed{2}}_{q_3}\, \underbrace{9}_{r_2} + \underbrace{\boxed{3}}_{r_3} \qquad \gcd(9, 3)$$

$$\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad ||$$

$$9 = \underbrace{\boxed{3}}_{q_4}\, 3 + \underbrace{\boxed{0}}_{r_4} \qquad \gcd(3, 0) = 3$$

<u>Thm:</u> (The Euclidean Algorithm)

Let a, b be natural number, with $a \geq b$.

(i) If $b | a$, 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 equations provided by the division Theorem:

$$a = q_1 b + r_1, \quad 0 \le r_1 < b$$

$$b = q_2 r_1 + r_2, \quad 0 \le r_2 < r_1$$

$$r_1 = q_3 r_2 + r_3 \qquad \vdots$$

$$\vdots$$

$$+ r_n$$

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

The algorithm terminates in a finite number of steps.

<u>Proof</u>: (i) clear, (ii) Terminates after finite number of steps, because $0 \le r_{i+1} < r_i$

$$\gcd(a,b) \underset{\uparrow}{=} \gcd(b, r_1) = \gcd(r_1, r_2) = \cdots =$$

Prev. Lemma

$$= \gcd(r_n, \underbrace{r_{n+1}}_{0}) = r_n.$$

$\square$

Theorem: (Another characterization of the $gcd(a,b)$).

If $d > 0$ and d is a common divisor of a and b, and there exist $x, y \in \mathbb{Z}$, such that $d = ax + by$, then $d = gcd(a,b)$.

Proof: Let c be a positive common divisor of a and b. Then $c \mid d = ax + by$. So $0 < c \leq d$. So d is the greatest common divisor of a and b.

$\square$

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

We saw ~~that~~ $\gcd(a,b) = 3$,

Find $x, y \in \mathbb{Z}$, such that $3 = ax + by$
$= 381x + 72y$.

(1) $\overset{=a}{381} = 5 \cdot \overset{=b}{72} + \overset{=r_1}{21}$

(2) $\overset{=b}{72} = 3 \cdot \overset{=r_1}{21} + \overset{=r_2}{9}$

(3) $21 = 2 \cdot \overset{=r_2}{9} + \boxed{3}^{=r_3}$

(4) $9 = 3 \cdot 3 + 0$

$$\underset{(3)}{\overset{=r_3}{3}} = \overset{=r_1}{21} - 2 \cdot \underbrace{\overset{=r_2}{9}}_{= 72 - 3 \cdot 21} = -2 \cdot 72 + 7 \cdot \underbrace{21}_{= 381 - 5 \cdot 72}$$

$$= (-2 + 7(-5))72 + 7 \cdot 381 =$$

$$= \underbrace{7}_{x} \cdot 381 + \underbrace{(-37)}_{y} 72$$

$3 = \gcd(381, 72) \Rightarrow$