Section 1.5: Divisibility I

Def: If $a, b \in \mathbb{Z}$, we say that a <u>divides</u> b if $\exists c \in \mathbb{Z}$ for which $ac = b$.

b is a <u>multiple</u> of a

a is a <u>divisor</u> of b

a is a <u>factor</u> of b

Notation: $\boxed{a \mid b}$ if a divides b

$\boxed{a \nmid b}$ otherwise

→ a \mid b

→ a \nmid b

Note: a, b can be positive or negative

Eg: The divisors of 27 are

$\pm 1, \pm 3, \pm 9, \pm 27$

$-3 \mid 27$

$5 \nmid 27$

Facts:

- $1 \mid n$ for each n
- $0 \nmid n$ for each n
- $n \mid 1$ $\underbrace{\text{iff}}_{\text{if and only if}}$ $n = \pm 1$
- $n \mid 0$ for every n
- $a \mid b$ iff $\frac{b}{a} \in \mathbb{Z}$ and $a \neq 0$

Basic Results

Thm: If $a, b, c \in \mathbb{Z}$ and $a \mid b$ and $b \mid c$, then $a \mid c$

↳ divisibility is transitive

Proof: WTS: $a \mid c$, meaning $\exists k \in \mathbb{Z} : ka = c$

Know: $a \mid b$, meaning $\exists m \in \mathbb{Z} : am = b$

$b \mid c$, meaning $\exists n \in \mathbb{Z} : bn = c$

$c = bn = (am)n = a(mn)$

Since $m, n \in \mathbb{Z}$, $m \cdot n \in \mathbb{Z}$

So $a \mid c$

Thm: If $a, b, c, m, n \in \mathbb{Z}$ and if $c \mid a$ and $c \mid b$, then $c \mid \underbrace{(ma + nb)}_{\text{int. lin. comb. of } a \text{ and } b}$

$\hookrightarrow$ if a, b are multiples of c, then so is any integer lin. comb. of a and b

Ex: $a = 15$, $b = 10$, $c = 5$

$\longrightarrow$ $5 \mid 15m + 10n$

Proof: WTS: $\exists k : ck = ma + nb$

Know: $c \mid a$, meaning $\exists r : cr = a$

$c \mid b$, meaning $\exists s : cs = b$

So $ma + nb = mcr + ncs$

$= c(mr + ns)$

Since $m, r, n, s \in \mathbb{Z}$, so is $mr + ns$

Hence $c \mid ma + nb$

Q: What can we say when $b \nmid a$?

or if we don't know?

Recall: $b \mid a$ iff $b \neq 0$ and $\frac{a}{b} \in \mathbb{Z}$

Ex:

$$
\begin{array}{r}
42 \\
3\overline{)127} \\
-120 \\
\hline
7 \\
-6 \\
\hline
1
\end{array}
\longrightarrow \frac{127}{3} = 42 + \frac{1}{3}
$$

Important:

$1 \geq 0$: if we had gotten $42 + \frac{-1}{3}$, we would rather write $41 + \frac{2}{3}$

$1 < 3$: if we had gotten $42 + \frac{4}{3}$, we would rather write $43 + \frac{1}{3}$

Lesson: $0 \leq$ numerator $<$ denominator

$$\frac{127}{3} = 42 + \frac{1}{3}$$

$$\Leftrightarrow \quad \underbrace{127}_{a} = \underbrace{3}_{b} \cdot \underbrace{42}_{q} + \underbrace{1}_{r}$$

Thm: If $a, b \in \mathbb{Z}$ with $b > 0$, then there are unique $q, r \in \mathbb{Z}$ so that $a = bq + r$ and $0 \leq r < b$.

Euclidean division algorithm

Note: $a = bq + r \iff \frac{a}{b} = q + \frac{r}{b}$

q - quotient

r - remainder

Proof: $T = \{a - bk \in \mathbb{N} \mid k \in \mathbb{Z}\}$

$T \neq \emptyset$ because any $k \leq \frac{a}{b}$ has $bk - a \leq 0 \iff a - bk \geq 0$

so $a - bk \in T$

$T \subseteq \mathbb{N}$ by definition

Hence, T has a least element,

call it r

Note: $r = a - bq$

$\rightarrow a = bq + r$

Remains to show: $0 \leq r < b$

$0 \leq r$ because $r \in T \subseteq \mathbb{N}$

Suppose, by $\not\downarrow$, $\underline{r \geq b}$

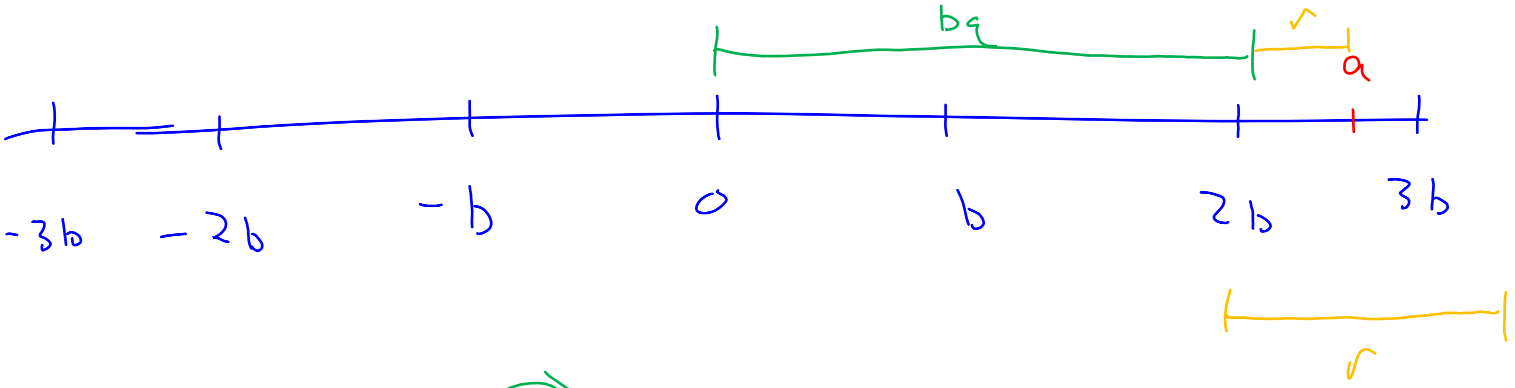
(Goal: Show that r isn't least!)

$$a = bq + r = bq + b + (r - b)$$
$$= b(q+1) + (r-b)$$

$$\rightarrow \underbrace{r - b}_{\geq 0} = \underbrace{a - b(q+1)}_{\text{of form } a - bk} \in T$$

$\rightarrow r - b < r$ b/c $b > 0$

This contradicts the minimality of r, hence $r < b$



$$a = bq + r$$

To show that q, r are unique,

suppose $a = bq_1 + r_1 = bq_2 + r_2$

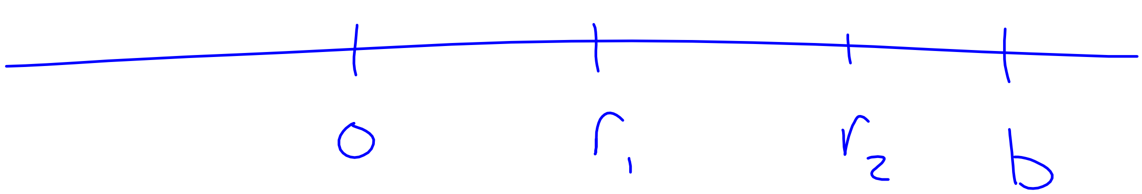
and $0 \le r_1 < b$, $0 \le r_2 < b$

Goal: Show $q_1 = q_2$, $r_1 = r_2$

$$bq_1 + r_1 = bq_2 + r_2$$

$$r_1 - r_2 = bq_2 - bq_1 = b(q_2 - q_1)$$

So, $b \mid r_1 - r_2$



$$0 \le r_1 < b, \quad 0 \le r_2 < b$$

$$\underline{-b} < -r_2 \le \underline{r_1 - r_2} < b - r_2 \le \underline{b}$$

$$-b < r_1 - r_2 < b$$

But $r_1 - r_2$ is a multiple of b

The only multiple of b between $-b$ and b is 0, so $r_2 - r_1 = 0$

So $r_2 = r_1$

From before: $b(q_1 - q_2) = r_2 - r_1 = 0$

$$\rightarrow q_1 - q_2 = 0 \rightarrow q_1 = q_2$$

Hence, q and r are unique!

GCDs I

Def: If $a, b \in \mathbb{Z}$ (one of which is nonzero), then the <u>greatest common divisor</u> is

$$\max\{k \in \mathbb{Z} : k \mid a \text{ and } k \mid b\}$$

$$=: \gcd(a,b) = (a,b)$$

$$(0,0) = 0$$