The Division Algorithm

NUMBER THEORY Topics #1

Ex: $3 \mid 14$ No (F).

$3 = b$ goes into $14 = a$ $4 = q$ times (quotient)

assure $b > 0$

$3 \times 4 = 12$

$3 \times 5 = 15$ too big

remainder? $r = 2$ = remainder

Key property: $0 \le r < 3$

$14 = 3 \cdot 4 + 2$

$a \quad b \cdot q \quad r$

$\exists! \, q, r \in \mathbb{Z}$

Theorem (The Division Algorithm): If $a, b \in \mathbb{Z}$ (a = dividend, b = divisor) and $b > 0$ then there exist unique $q, r \in \mathbb{Z}$ with $a = bq + r$, and $0 \le r < b$.

Ex a. if $a = 26$, $b = 7$, does TDA apply? If so, find q, r.

$q = 3$, $r = 5$

$7 \cdot 3 + 5 = 21 + 5 = 26$ ✓

Different answer for q, r?

$q = 4,\ r = -2$

$7 \cdot 4 + (-2) = 28 - 2 = 26$

$r < 0$, doesn't work / doesn't satisfy

b. if $a = 4$, $b = 7$? Does TDA apply? If so, find q, r

$\boxed{q = 0,\ r = 4}$

~~$= 7 \cdot 0 + 7 = 0 + 7 =$~~

$4 = 7 \cdot 0 + 4 = 4$

$a = b\,q + r$ ✓ $\quad 0 \le 4 < 7$ ✓

c. if $a = -8$, $b = 3$, does the Division Algorithm apply? Y

q, r

$-8 = 3 \cdot q + r$ and $0 \le r < 3$

$q = -3,\ r = 1$

$3 \cdot (-3) + 1 = -9 + 1 = -8$

$b\ \ q\ \ + r \qquad a$ ✓

$0 \le r < 3$ ✓

Theorem (The Division Algorithm): If $a, b \in \mathbb{Z}$ and $b > 0$ then there exist unique $q, r \in \mathbb{Z}$ with $a = bq + r$, and $0 \le r < b$.

FACT: if $A \subseteq \mathbb{Z}$, if A has an upper bound, then A has a largest element.

upper bound of 4

E $\{\ldots, -3, -2, -1, 0, 1, 2, 3\}$ largest element $= 3$

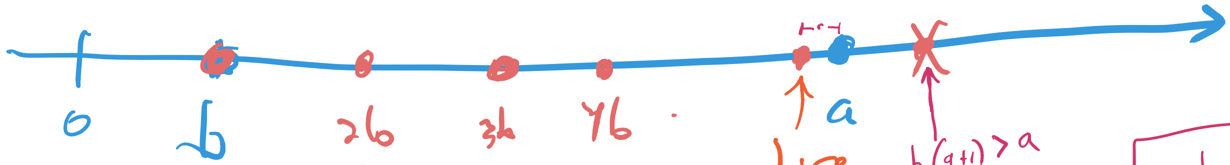
NOTE two things to prove (given $a, b \in \mathbb{Z}, b > 0$):

① there are some $q, r \in \mathbb{Z}$, $a = bq + r$, $0 \le r < b$

② this q, r are unique

Proof Suppose $a, b \in \mathbb{Z}$, $b > 0$.

Part 1 (Existence) let $A = \{bn : n \in \mathbb{Z} \text{ and } bn \le a\}$



$b \cdot 1 = b$

$b \cdot 2 = 2b$

$b(q+1) > a$

$bq + b > a$

$-bq \quad -bq$

$b > a - bq$

$\boxed{a - bq < b}$

$\boxed{r < b}$

$14 \div 3$

Note: A is bounded above by a.

$A \subseteq \mathbb{Z}$, A has an upper bound a.

Thus A has ~~an upper~~ greatest element bq, $q \in \mathbb{Z}$, $bq \le a$

let $r = a - bq$, note $r \in \mathbb{Z}$ by closure of $\mathbb{Z}$ under $-, \times$.

Note $bq \le a$

$-bq \quad -bq$

$0 \le a - bq$

so $r \ge 0$

Qus: is $r < b$?

Y.

Since bq is largest element of A,

$b(q+1) \notin A$

so $b(q+1) > a$

$$bq + b > a$$
$$-bq \qquad -bq$$

$$b > a - bq$$

so $b > r$, by substitution

So $0 \leq r < b$.

Finally consider

$bq + r =$

$bq + (a - bq) =$ by substitution

$= a$ $\square$ end of part 1 (existence).

Part 2 (uniqueness).

Suppose $q_1, r_1 \in \mathbb{Z}$, $a = bq_1 + r_1$, $0 \leq r_1 < b$

Suppose $q_2, r_2 \in \mathbb{Z}$ $a = bq_2 + r_2$, $0 \leq r_2 < b$

Substituting, we have:

$$bq_1 + r_1 = bq_2 + r_2$$
$$-bq_2 - r_1 \quad -bq_2 \quad -r_1$$

Goal: want to prove: $q_1 = q_2$

or $0 = q_2 - q_1$

$r_1 = r_2$

$bq_1 - bq_2 = r_2 - r_1$

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

<u>claim</u> $-b < r_2 - r_1 < b$

<u>proof:</u> $0 \le r_1 < b$ given

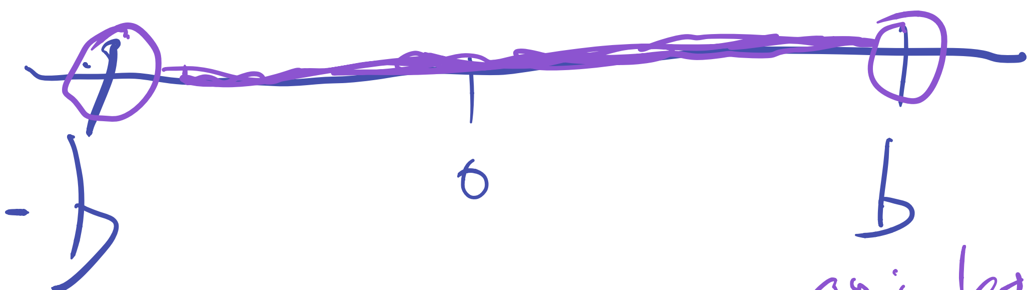
$\boxed{0 \le r_2 < b}$

multiply by -1:

$0 \ge -r_1 > -b$

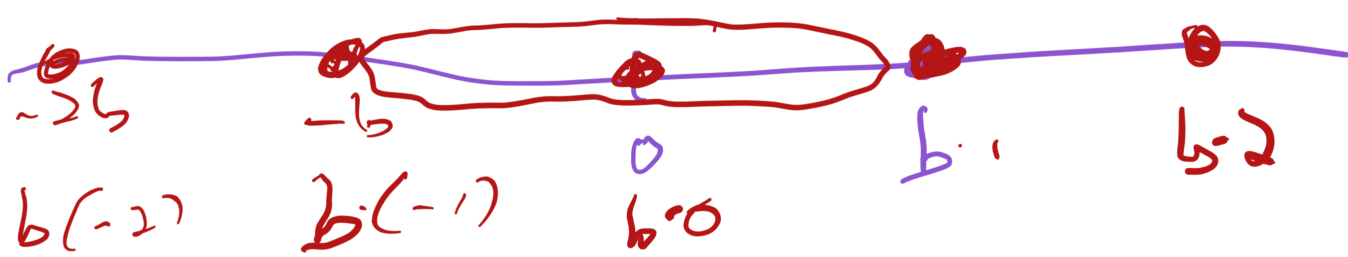
$$\boxed{-b < -r \le 0}$$

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



$$-b < \overbrace{b(q_1 - q_2)}^{\text{an integer}} < b$$

bc closure of $\mathbb{Z}$ under $-$.



since $q_1 - q_2 \in \mathbb{Z}$,

and $-b < b(q_1 - q_2) < b$

(Note $b > 0$ by assumption, so $b \neq 0$)

we have $q_1 - q_2 = 0$

$-q_2 \quad -q_2$

$$\boxed{q_1 = q_2}$$

$$b(0) = r_2 - r_1$$

$$0 = r_2 - r_1$$

$$\boxed{r_1 = r_2}$$

$\square$