# Part I Warm Up

A(3) Main outline of Pf of Division Algorithm

Thm:

① Existence: $\exists\, q, r \in \mathbb{Z}$ s.t. $n = qd + r$ with $0 \le r < d$.

② Uniqueness: if there if another expression $n = q'd + r'$ with $0 \le r' < d$
$\Rightarrow r' = r,\ q' = q$.

B(7) If $a, b, c \in \mathbb{Z}$, $a|b$, $b|c \Rightarrow a|c$

Pf $a|b \Rightarrow \exists\, s \in \mathbb{Z}$ s.t. $b = as$
$b|c \Rightarrow \exists\, t \in \mathbb{Z}$ s.t. $c = bt$
$\Rightarrow c = (st)a$
$s \in \mathbb{Z}, t \in \mathbb{Z} \Rightarrow st \in \mathbb{Z} \Rightarrow a|c$

C. connection between "divides $(|)$" are division algorithm.

Division algorithm: For any $n, d \in \mathbb{Z}$, $(d > 0)$
$\exists$ unique $q, r \in \mathbb{Z}$ s.t. $\boxed{n = qd + r,\ 0 \le r < d}$

可以发现 if $d \mid n \Rightarrow r=0$

## Part 2(b) Division Thm: Existence

Let $n, d \in \mathbb{Z}$ with $d>0$

Def $S=\{n-dx \mid x\in\mathbb{Z}, n-dx\geq 0\}$

$\boxed{\text{(2) } S \text{ is non empty}}$

Pf. (Find a value for $\underset{\in\mathbb{Z}}{x}$ s.t. $n-dx\geq 0$)

We consider $\boxed{x=-|n|}$

Since $d\geq 1$ ($\in\mathbb{Z}^+$) and $|n|\geq 0$,

$d|n|\geq |n|\geq -n \Rightarrow n+d|n|\geq 0$

$\boxed{\text{(3) } S \text{ has a smallest element}}$

Pf Since $n-dx\geq 0$ and $n-dx\in\mathbb{Z}^+$,

$\Rightarrow$ it has a minimal element which is $\geq 0$.

$\boxed{\text{(4) Let } r \text{ be the smallest element of } S.}$

$\boxed{\text{Prove } r<d}$

Pf Assume for sake of contradiction that $r \geq d$. Let $r = d + k$ for some $k \geq 0 \in \mathbb{Z}$

Since $r = n - dx$

$\Rightarrow d + k = n - dx$

$\Rightarrow k = n - d(x+1) \geq 0$

$\Rightarrow k \in S$ and $k < r$ since $r = d + r$

$\Rightarrow k$ is the smallest element of $S$ $\Rightarrow$ contradicts

$\Rightarrow r < d$

(5) Prove the existence part of Division Algorithm.

We have prove the existence of smallest element of $S$: $r = n - dx$ for some $x \in \mathbb{Z}$, with $r \geq 0$ and $r < d$

$\Rightarrow n = xd + r \;, 0 \leq r < d$

# Part 2 (E) Division Algorithm: Uniqueness.

Let $n, d \in \mathbb{Z}$ with $d \geq 1$.

Suppose $n = qd + r = q'd + r'$, where

$q, r, q', r' \in \mathbb{Z}$ and $0 \leq r, r' < d$

## (1) Show $d \mid (r - r')$

Pf Since $n = qd + r = q'd + r'$

$\Rightarrow d(q' - q) = (r - r')$

$\Rightarrow$ By def, $d \mid (r - r')$

## (2) Show $|r - r'| < d$

Pf Since $0 \leq r, r' < d$

$\Rightarrow -d < -r' \leq 0$

plus $0 \leq r < d$

$\Rightarrow -d < r - r' < d$

$\Rightarrow |r - r'| < d$

$\boxed{(3) \text{ Show } |d(q-q')| < d}$

Since $d(q-q') = (r-r')$,

$\because |r-r'| < d$

$\Rightarrow |d(q-q')| < d$

$\boxed{(4) \text{ Show } q = q'}$

Since $|d(q-q')| < d$

$\Rightarrow |q-q'| < 1$

Since $q, q' \in \mathbb{Z}$, $q = q'$

$\boxed{(5) \text{ Show } r = r'}$

Since $q = q' \Rightarrow d(q-q') = 0$

$\Rightarrow r - r' = 0$

$\Rightarrow r = r'$

$\Rightarrow$ q.e.d.

我们总结 prove uniqueness 的办法:
assume two solutions then prove
they are equal.