Math 321

Baby Number theory → goal: cryptography

0, •, ••, •••, ••••, •••••, •••••• , ... → ..., -2, -1, 0, 1, 2, ...

1, 2, 3, 4, 5, 6, 7, ...

$\mathbb{Z}$

Ops $+, -, \times$, Share

Division

function f a,b that returns a number

$\frac{2}{3} = 0.\overline{6}$

Division(2,3) → number

Reals

Divides

function f a,b that returns True/False

(propositional function)

Divides(a,b) → T/F

a divides b → T/F (can't share)

share

people | stuff | can share

Def a divides b : $a \mid b$

$a \mid b$ is true if there is a $n \in \mathbb{Z}$ $a \cdot n = b$

false: $a \nmid b$ "a doesn't divide b"

Ex $2 \mid 8$ only 2^3. b/c $2 \cdot 4 = 8$

$2 \nmid 9$

$3 \mid 9$ only 3^2.

$3 \nmid 10$

$3 \cdot 3 = 9$

$s \mid t$ means $\exists n \in \mathbb{Z}$ $s \cdot n = t$

s is a factor of t

t is a multiple of s (product)

Properties $a, b, c \in \mathbb{Z}$, $a \neq 0$

Thm

1. $a \mid b \wedge a \mid c \rightarrow a \mid (b+c)$
2. $a \mid b \rightarrow a \mid b \cdot n$ (n is an integer)
3. $a \mid b \wedge b \mid c \rightarrow a \mid c$

Pf

$a \mid b$ means $a \cdot n_1 = b$

$b \mid c$ means $b \cdot n_2 = c$

$\therefore (a \cdot n_1) \cdot n_2 = c \rightarrow a \cdot (n_1 \cdot n_2) = c$

So $a \mid c$

Corollary $a|b \wedge a|c$

then $a|(bn_1 + cn_2)$ $\quad n_1, n_2 \in \mathbb{Z}$

How do we share? if you have d people and a amount to share.

$d|a$? (vs) $d \nmid a$?

Division Algorithm

$$a = d \cdot q + r \qquad 0 \le r < d$$

a: dividend, d: divisor, q: quotient, r: remainder

$r \in \{0, 1, 2, \ldots, d-1\}$

$r = 0$ then $d|a$

$r \neq 0$ then $d \nmid a$

(ex) $d = 3 \quad a = 14 \quad 14 = 3 \cdot 4 + 2$

$d = 5 \quad a = 8 \quad 8 = 5 \cdot 1 + 3$

$d = 5 \quad a = -8 \quad -8 = 5(-2) + 2$

$d = 3 \quad a = -14 \quad -14 = 3(-5) + 1$

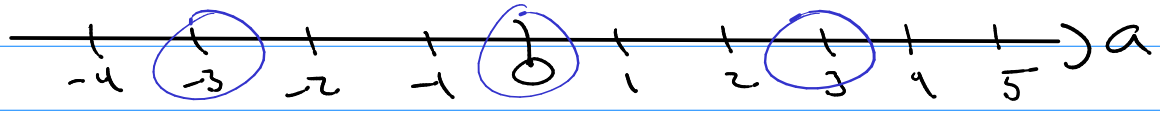
r $\qquad$ q

$a \operatorname{div} d = q$ & $a = d \cdot q + r$

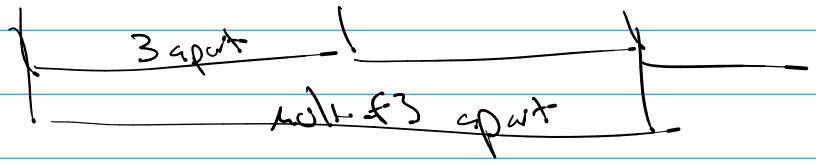
$a \bmod d = r$

$d = 3$

$a \text{ div } 3$ $\quad -2 \; -1 \; -1 \; -1 \; 0 \; 0 \; 0 \; 1 \; 1 \; 1$



$a \bmod 3$ $\quad 2 \; 0 \; 1 \; 2 \; 0 \; 1 \; 2 \; 0 \; 1 \; 2$



under mod 3 call $\ldots -3, 0, 3, 6, \ldots$ the

"Same" → Congruence