Math 321

Ch 4 Number Theory

Numbers:

1, 2, 3, 4, 5, 6, 7, 8, ..

Objects: $\mathbb{Z}$ Operations $+, -, *$

4.1 Divisibility and Modulus

(share fairly)

Def "a divides b", "a is a factor of b"
"b is a multiple of a"

Symbols $a \mid b$

when we $a \cdot c = b$ for integer c

ex $3 \mid 12$ yes b/c $3 \cdot 4 = 12$

$4 \mid -16$ yes b/c $4(-4) = -16$

if not $a \nmid b$

ex $3 \mid 10$ No b/c $3 \cdot ? = 10$ Nothing!

So we say $\boxed{3 \nmid 10}$

properties of $a|b$

thm ① $(a|b \wedge a|c) \rightarrow a|(b+c)$

pf (direct)

assume $(a|b \wedge a|c)$ ✓

<u>means</u>: $a \cdot k_1 = b \wedge a \cdot k_2 = c$ some ints k_1, k_2

so $b+c = ak_1 + ak_2 = a(k_1+k_2)$

so $b+c = a(k_1+k_2)$ by def of divides

$a|(b+c)$ ✓

② $a|b \rightarrow a|b \cdot c$ for all $c \in \mathbb{Z}$

③ $a|b \wedge b|c \rightarrow a|c$

Corollary

$a|b \wedge a|c \rightarrow a|mb+nc$

(any $m, n \in \mathbb{Z}$)

<u>Note</u>: $3|6$ but $3 \nmid 8$

can I consider this as a problem to work with.

$8 = 3 \cdot 2 + 2$

and $3 \nmid 7 \rightarrow 7 = \boxed{3 \cdot 2} + \boxed{1}$

$3|6 \rightarrow 6 = \boxed{3 \cdot 2} + \boxed{0}$

Division Algorithm $a \in \mathbb{Z}$ $d \in \mathbb{Z}^+$

there are unique $q, r \in \mathbb{Z}$ and $0 \le r < d$

such that $a = d \cdot q + r$

a: dividend q: quotient (div)

d: divisor r: remainder (mod)

ex $a = 17$ $d = 3$

$$17 = 3 \cdot 5 + 2$$

$a = -17$ $d = 3$

$$-17 = 3(\underline{\underline{-6}}) + 1$$

div, mod as operations

quotient remainder

$a \text{ div } d = q$ $\text{div}(a, d) = q$

$a \text{ mod } d = r$ $\text{mod}(a, d) = r$

ex $-18 \text{ mod } 4 = 2$ b/c $-18 = 4 \cdot (-5) + \underline{\underline{2}}$

$18 \text{ mod } 4 = 2$ b/c $18 = 4 \cdot 4 + \underline{\underline{2}}$

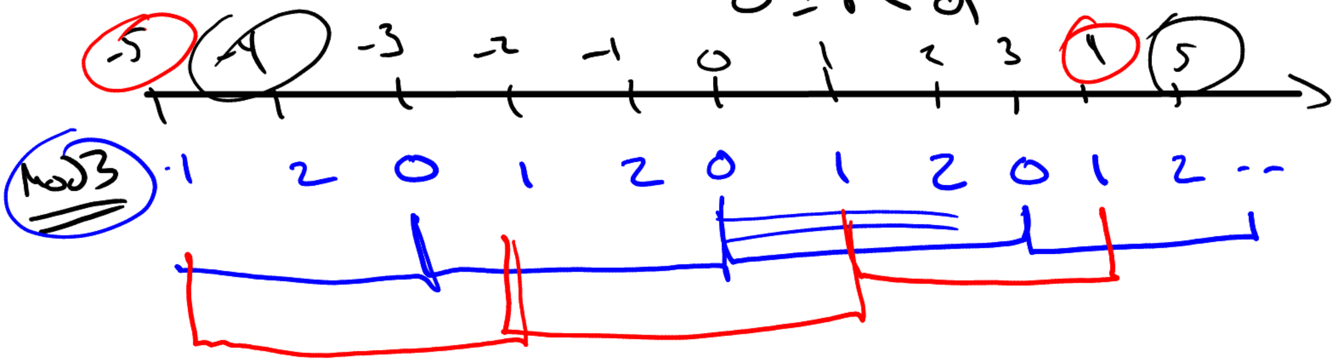
$-18 \text{ div } 4 = -5$

$18 \text{ div } 4 = 4$

It looks like modulus is useful.

$$\underset{\mathbb{Z}}{a} = d \cdot q + r$$

$$0 \le r < d$$



Def a is congruent to b under modulo m

symbols: $a \equiv b \pmod m$

or $a \underset{m}{\equiv} b$

iff $\boxed{m \mid (a-b) \text{ def}}$

Thm $a \underset{m}{\equiv} b$ iff

① $a \bmod m = b \bmod m$

② $a = b + km$

all mean $a \underset{m}{\equiv} b$

---

ex of above $\cdot\ -3 \underset{3}{\equiv} 0 \underset{3}{\equiv} 3 \underset{3}{\equiv} 6 \underset{3}{\equiv} 9$

$\cdots -2 \underset{3}{\equiv} 1 \underset{3}{\equiv} 4 \underset{3}{\equiv} 7 \underset{3}{\equiv} \cdots$

$\cdots -1 \underset{3}{\equiv} 2 \underset{3}{\equiv} 5 \underset{3}{\equiv} 8 \underset{3}{\equiv} \cdots$

Properties

$a \underset{n}{\equiv} b \qquad c \underset{n}{\equiv} d$

$$a + c \underset{n}{\equiv} b + d$$

$$ac \underset{n}{\equiv} bd$$