Divisibilty

Section 4.1

Divison

Integer

$a|b$ iff $\exists c : \boxed{ac = b}$ ($a, b, \in \mathbb{Z}$, $c \in \mathbb{Z}^+$)

a divides b   Some Value of C

$3|15$ $3c = 15$
$C = 5 \in \mathbb{Z}^+$ Since that # goes in evenly.

$3|22$ $3c = 22$
$c = \frac{22}{3} \notin \mathbb{Z}^+$

Properties of Divisibility

$a|b$ $ac = b$
$at = C$

a) if $a|b$ and $a|c$, then $a|(b+c)$

$3|15$ $3|6$ $3|(15+6)$ or $3|21$ ✓   Shown its true

Start Proof: There exists two integers s and t such that

$b = as$ and $C = at$ from defin. of divisibility.

Subsition

$b + c = as + at = a(s+t)$

$b + c = a(s+t)$

$\therefore a|(b+c)$ ← Proof

Properties of Divisibility

b.) iff $a|b$ then $a|bc$ for all $c \in \mathbb{Z}$

$3|15 \quad 3|10 \quad 3|45 \quad 3|60$

If $a|b$ then $b = at$ for some $t \in \mathbb{Z}$

$$bc = (at)c = a(tc)$$

$\therefore\ a|bc$ by defin. of divisibility

c.) If $a|b$ and $b|c$, then $a|c$

$3|6$ and $6|18$, then $3|18$ ✓

Since $a|b$ then $b = at$ for some $t \in \mathbb{Z}$
Since $b|c$ then $c = bs$ for some $s \in \mathbb{Z}$.
Then $c = (at)s$, or $c = a(ts)$

$\therefore\ a|c$

Division Algorithm:

$d \mid a \quad a = dq$

Let $a \in \mathbb{Z}$ and $d \in \mathbb{Z}^+$. $\exists!\, q, r : a = dq + r$.

remainder

quotient

divisor

Example:

$4 \mid 21 \qquad 21 = 4q + r$

$4\overline{)21}$ = 5 R 1; -20, 1

$21 = 4(5) + \underline{\underline{1}} \qquad 0 \le r < d$

Give the quotient and remainder for each.

$a = dq + r$

$7 \mid 18$ (d, a) $\qquad 18 = 7(2) + 4 \qquad 0 \le r < 7$

quotient: $q = a \text{ div } d$, $2 = 18 \text{ div } 7$

remainder: $r = a \underline{\underline{\text{mod}}}\ d$, $4 = 18 \text{ mod } 7$

If we took 18 divided by 7 our remainder would be 4

$10 \mid -112 \qquad -112 = 10(-11) + -2 \qquad 0 \le r < 10$

$\boxed{-112 = 10(-12) + 8}$

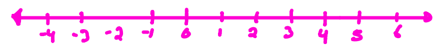
quotient: $-12 = -112 \text{ div } 10$

remainder: $8 = -112 \text{ mod } 10$

$14 \mid 0 \qquad 0 = 14(0) + 0 \qquad 0 = 0 \text{ div } 14 \quad 0 = 0 \text{ mod } 14$

Modular Arithmetic

If $a, b \in \mathbb{Z}$ and $m \in \mathbb{Z}^+$, then $a \equiv b \pmod{m}$ iff $m \mid a-b$.



Determine if $2 \equiv 6 \pmod{4}$

Determine if $24 \equiv 14 \pmod{6}$

Let $a, b, \in \mathbb{Z}$ and $m \in \mathbb{Z}^+$. Then $a \equiv b \pmod{m}$ iff $\boxed{a \bmod m = b \bmod m}$

Determine if $2 \equiv 6 \pmod{4}$

Determine if $24 \equiv 14 \pmod{6}$