# Number Theory Chapter 4.1-4.3

Section 4.1

## Divisibility

### Divison

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

Integer

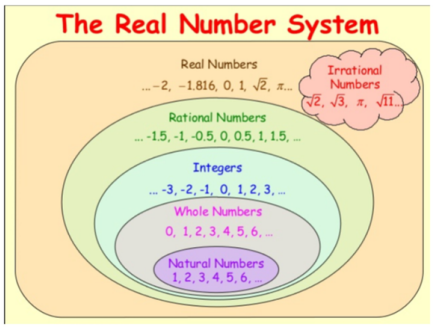
$a|b$: a divides b

$\exists c : ac = b$: Some Value of C

$3|15$ $\quad 3c = 15$

$c = 5 \in \mathbb{Z}^+$

Since that # goes in evenly.




Another Example: $3|22$ $\quad 3c = 22$

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

Not an Integer

**DEFINITION 1** If $a$ and $b$ are integers with $a \neq 0$, we say that $a$ *divides* $b$ if there is an integer $c$ such that $b = ac$, or equivalently, if $\frac{b}{a}$ is an integer. When $a$ divides $b$ we say that $a$ is a *factor* or *divisor* of $b$, and that $b$ is a *multiple* of $a$. The notation $a \mid b$ denotes that $a$ divides $b$. We write $a \nmid b$ when $a$ does not divide $b$.

## Properties of Divisibility

$a|b \quad ac = b$

$at = c$

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

"a divides into both"

Example: $3|15 \quad 3|6 \quad 3|(15+6)$ or $3|21$ ✓ Shown it's true

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

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

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

Equivalent

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

$\therefore a|(b+c)$ ← Proof

**COROLLARY 1** If $a$, $b$, and $c$ are integers, where $a \neq 0$, such that $a \mid b$ and $a \mid c$, then $a \mid mb + nc$ whenever $m$ and $n$ are integers.

## Properties of Divisibility

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

$3|15$ $3|30$ $3|45$ $3|60$

$15=2$ $15=3$ $15=4$ ~ if $b=15$, $c=\mathbb{Z}$

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

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

$bc = a(tc)$ ← Regroup
Associated Property

$\therefore a|bc$ 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 by substitution:

Then $c=(at)s$, or $c=a(ts)$

$\therefore a|c$

## Division Algorithm:

**THEOREM 2** **THE DIVISION ALGORITHM** Let $a$ be an integer and $d$ a positive integer. Then there are unique integers $q$ and $r$, with $0 \leq r < d$, such that $a = dq + r$.

$d|a \quad a = dq$

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

Example:

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

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

$21 = 4(5) + 1$ $\leftarrow 0 \leq r < d$ Important

**Examples:**

Give the quotient and remainder for each.

a) $7|18$ $\quad a = dq + r$

$d \quad a$

$18 = 7(2) + 4 \qquad 0 \leq r < 7$

Notation:

quotient: $q = a \text{ div } d$ — remainder: $r = a \bmod d$

$2 = 18 \text{ div } 7 \qquad 4 = 18 \bmod 7$

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

b) $10|-112 \qquad -112 = 10(-11) + -2 \quad \not\rightarrow \quad 0 \leq r < 10$ · negative two is not b/w 0 and 10!

$-112 = 10(-12) + 8$

$a = dq + r$

Correct Way to Write

quotient: $-12 = -112 \text{ div } 10$ — remainder: $8 = -112 \bmod 10$

c) $14|0 \qquad 0 = 14(0) + 0$

$a = dq + r$

quotient: $0 = 0 \text{ div } 14$ — remainder: $0 = 0 \bmod 14$

## Modular Arithmetic

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

Remainders

$\frac{-4}{4} \to 0$

$\frac{-3}{4} \to 1$

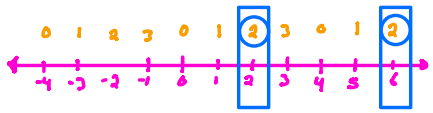
$\frac{-2}{4} \to 2$

$\frac{-1}{4} \to 3$

Mod 4 = {0, 1, 2, 3}

possible remainders

pattern




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

- is 2 congruent to 6 in mod 4?

Both are two

If I take $\frac{2}{4}$ or $\frac{6}{4}$ my remainder is 2, which is exactly the same, so yes, they're Equivalent.

- Can do it w/o number line by seeing if the difference b/w the two values is divisible by 4

$2 \equiv 6 \pmod{4}$ $\quad 4 \mid (2-6)$

$4 \mid (-4)$ ✓ yes is congruent

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

$6 \mid (24-14)$

$6 \mid 10$ X

Not Equivalent

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

^if the remainders are equal to one another then they're congruent

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

$2 \bmod 4 = 6 \bmod 4$

$4|2 = 4(0) + 2$

$2 = 2 \bmod 4$

$4|6 = 4(1) + 2$

$2 = 6 \bmod 4$

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

$24 \bmod 6 \neq 14 \bmod 6$

$6|24 = 6(4) + 0$

$0 = 24 \bmod 6$

$6|14 = 6(2) + 2$

$2 = 14 \bmod 6$

**Theorem:**

$a \equiv b \pmod m$

P — The integers $a$ and $b$ are congruent modulo $m$ iff there is an integer $k$ such that $a = b + km$ — Q

Assuming → Let $a \equiv b \pmod m$

Then $m \mid (a-b)$ by defin of congruence

Then $a - b = km$ for some $k \in \mathbb{Z}$, by defin of divisibility.

By addition of $b$, then $a = b + km$.

Proved in both directions

Assume $a = b + km$.

Then $a - b = km$ by subtraction.

Then $m \mid (a-b)$, so $a \equiv b \pmod m$.

**Theorem**

Let $m \in \mathbb{Z}^+$. If $a \equiv b \pmod m$ and $c \equiv d \pmod m$ then $a + c \equiv b + d \pmod m$ and $ac \equiv bd \pmod m$.

Assume $a \equiv b \pmod m$. Then $a = b + km$ for some $k \in \mathbb{Z}$.

Assume also, $c \equiv d \pmod m$. Then $c = d + lm$ for some $l \in \mathbb{Z}$.

$a + c = (b + km) + (d + lm) = (b+d) + (km + lm) = (b+d) + m(k+l)$

$a + c = (b+d) + m(k+l)$ so $(a+c) - (b+d) = m(k+l)$ so

$m \mid (a+c) - (b+d)$ so $a + c \equiv b + d \pmod m$.

$ac = (b + km)(d + lm) = bd + blm + kdm + klm^2 = bd + m(bl + kd + klm)$

So $ac - bd = m(bl + kd + klm)$ so $m \mid ac - bd$ so $ac \equiv bd \pmod m$

Let $m \in \mathbb{Z}^+$. If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$ then $a + c \equiv b + d \pmod{m}$ and $ac \equiv bd \pmod{m}$.

Find $7 + 11 \pmod 5$ and $7 \cdot 11 \pmod 5$

$7 + 11 \pmod 5$ and $7 \cdot 11 \pmod 5$

$7 + 11 = 18 \equiv 3 \pmod 5$

(18 congruent to 3)

$7 \cdot 11 = 77 \equiv 2 \pmod 5$

$7 \cdot 11 = 2 \cdot 1 = 2 \pmod 5$

$7 \equiv 2 \pmod 5$

$11 \equiv 1 \pmod 5$

$7 + 11 = 2 + 1 = 3 \pmod 5$

## Arithmetic modulo m

- We can define operations on $\mathbb{Z}_m$, the set of non-negative integers less than m, $\{0, 1, 2, \ldots, m-1\}$.

Addition (denoted $+_m$): $a +_m b = (a + b) \bmod m$

Multiplication (denoted $\cdot_m$): $a \cdot_m b = (a \cdot b) \bmod m$

**Example:**

Find $4 +_3 5$ and $4 \cdot_3 5$

$4 + 5 = 9 \equiv 0 \pmod 3$

3 goes into 9 evenly

$4 \cdot 5 = 20 \equiv 2 \pmod 3$

# Decimal Expansions from Binary, Octal and Hexadecimal

Section 4.2