Divisibility and Modularity

Divisibility

- Definition: Let $a, b \in \mathbb{Z}$ with $a \neq 0$. We say that a divides b, denoted $a|b$, if $\exists k \in \mathbb{Z}$ such that $b = a \cdot k$. In such case, we can also express this as $b \div a \in \mathbb{Z}$

Example 1

- Determine whether each of the following statements are true

  $a)$ $3|6$

  - Solution: $6 = 3 \times 2$, where 2 is an integer $\Longrightarrow TRUE$

  $b)$ $6|3$

  - Solution: $3 = 6 \times \frac{1}{2}$, where $\frac{1}{2}$ is not an integer $\Longrightarrow FALSE$

  $c)$ $3 \nmid 5$

  - Solution: $5 = 3 \times \frac{5}{3}$, where $\frac{5}{3}$ is not an integer $\Longrightarrow TRUE$

Example 2

- Let $n, d \in \mathbb{Z}^+$. How many positive integers not exceeding n are divisible by d
- e.g. $\rightarrow n = 9, d = 4$
- How many positive integers from 1-9 are divisible by 4?
  - 4 and 8 (2 integers)
- Notice: $4K$ describes a number divisible by 4, if $K \in \mathbb{Z}$. We can find all integers divisible by 4 not exceeding 9 by placing the following condition:
- $4K \leq 9$
- $K \leq \left\lfloor \frac{9}{4} \right\rfloor = 2$ (floor function forces and integer)
- $K \leq 2 \rightarrow K = 1{,}2$ (2 integers)
- $\Longrightarrow$ Any integer divisible by d, must have the form $d \times k,\ k \in \mathbb{Z}$
- $d \times k \leq h \rightarrow k \leq \left\lfloor \frac{h}{d} \right\rfloor \Longrightarrow$ Hence, there are $\left\lfloor \frac{h}{d} \right\rfloor$ many integers exceeding n that are divisible by d

Theorem 4.1.1

- Let $a, b, c \in \mathbb{Z}$ and $c \neq 0$
  i. If $a|b$ and $a|c$, then $a|(b + c)$
  ii. If $a|b$, then $a|bc\ \forall c \in \mathbb{Z}$
  iii. If $a|b$ and $b|c$, then $a|c$
- Proof:
  i. If $a|b$ and $a|c$, then $\exists k, q \in \mathbb{Z}$ such that $\mathrm{b} = a \times k$ and $c = a \times q$
     $b + c = ak + aq$
     $b + c = a(k + q)$
     $b + c = a \times u$, where $u = k + q \rightarrow u \in \mathbb{Z}$
     By definition, $a|(b + c)$

Theorem 4.1.1

- Let $a, b, c \in \mathbb{Z}$ and $c \neq 0$
  i. If $a|b$ and $a|c$, then $a|(b+c)$
  ii. If $a|b$, then $a|bc\ \forall c \in \mathbb{Z}$
  iii. If $a|b$ and $b|c$, then $a|c$
- Proof:
  ii. If $a|b$, then $\exists k \in \mathbb{Z}$ such that $\mathrm{b} = a \times k$
  $bc = a \times k \times c$
  $bc = a \times u$, where $u = k \times c \rightarrow u \in \mathbb{Z}$
  By definition, $a|bc$

Theorem 4.1.1

- Let $a, b, c \in \mathbb{Z}$ and $c \neq 0$
  i. If $a|b$ and $a|c$, then $a|(b+c)$
  ii. If $a|b$, then $a|bc \; \forall c \in \mathbb{Z}$
  iii. If $a|b$ and $b|c$, then $a|c$
- Proof:
  i. If $a|b$ and b$|c$, then $\exists k, q \in \mathbb{Z}$ such that $\mathrm{b} = a \times k$ and $c = b \times q$
     $c = b \times q$
     $c = a \times k \times q$
     $c = a \times u$, where $u = k \times q \rightarrow u \in \mathbb{Z}$
     By definition, $a|c$

Theorem 4.1.2 Division Algorithm

- Let $a \in \mathbb{Z}$ and $d \in \mathbb{Z}^+$, then $\exists!\, q, r \in \mathbb{Z}$ satisfying $0 \leq r < d$ such that
$$a = d \cdot q + r$$
- Proof:
   i. Let $d|a \to \exists q \in \mathbb{Z}$ such that $a = d \times q + r$
   In such a case, $a = d \times q + r$, where $r = 0$
   ii. Let $d \nmid a \to$ if a $d \nmid a$ $\exists r \in \mathbb{Z}$ such that $r < d$ and $d|(a - r)$
   In such a case, $a - r = q \times d \Longrightarrow a = d \times q + r$

Modularity

- Definition: Let $a, q, r \in \mathbb{Z}$ and $d \in \mathbb{Z}^+$ such that $a = d \cdot q + r$. We define,

$$a \bmod d = r$$

- Whenever a divided by d results in remainder r

Example 3

- Which of the following are true?
  a) $101 \bmod 11 \ = \ 2$
     - $101 = 11 \times 9 + 2 \Longrightarrow TRUE$
  b) $101 \bmod 2 \ = 11$
     - $101 = 50 \times 2 + 1 \Longrightarrow FALSE$
  c) $11 \bmod 2 \ = \ 101$
     - $11 = 5 \times 2 + 1 \Longrightarrow FALSE$
  d) $101 \bmod 2 \ = \ 1$
     - $101 = 50 \times 2 + 1 \Longrightarrow TRUE$

Example 4

- What are the quotient and remainder when -11 is divided by 3?
- $-11 = -3 \times 3 + (-2)$
- $-11 = -4 \times 3 + 1$
- $\Longrightarrow q = -4, r = 1$

Quotient

- Definition: Definition: Let $a, q, r \in \mathbb{Z}$ and $d \in \mathbb{Z}^+$ such that $a = d \cdot q + r$.
$$a \bmod d = r$$
- Whenever a divided by d has a quotient q

Example 5

- Evaluate the quotient of the following:
- $101 \div 11$
  - $101 = 9 \times 11 + 2 \Rightarrow 9$
- $-11 \div 3$
  - $-11 = -4 \times 3 + 1 \Rightarrow -4$

Congruency

- Definition: Congruent to b modulo m. Let $a, b, m \in \mathbb{Z}$. We say that a is congruent to b modulo m denoted
$$a \cong b \bmod m$$
- iff $m|(a-b)$