§ 4.1 Divisibility & Modular Arithmetic

Jessica Wei

Introduction

One of the goals of this course is to equip you with the mathematical tools necessary to understand encryption methodologies and systems. The aim of this section of to introduce you to the underlying, basic math of some of the most widely used cryptosystems.

Notations

SYMBOL REFERENCE

$\mathbb{R}$ = set of real numbers and any number that is not complex.
$\mathbb{Z}$ = set of integers.
$\mathbb{Z}^-$ = set of negative integers.
$\mathbb{Z}^+$ = set of positive integers.
$\in$ = "in"
$\exists$ = "there exists"
$\exists!$ = "there does not exist"

Divisibility

DEF | DIVIDES

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

Example 1. Determine whether each of the following statements are true.

(a) $3 \mid 6$
$6 = 3 \cdot k \quad \Rightarrow \quad k = 2 \in \mathbb{Z}$
Answer: $True$

(b) $6 \mid 3$
$3 = 6 \cdot k \quad \Rightarrow \quad k = \frac{1}{2} \notin \mathbb{Z}$
Answer: $False$

(c) $3 \not| 5$
$5 = 3 \cdot k \quad \Rightarrow \quad k = \frac{5}{3} \notin \mathbb{Z}$
Answer: $True$

Example 2 Let $n, d \in \mathbb{Z}^+$. How many positive integers not exceeding n are divisible by d?
$Consider : n = 21, d = 2$. How many integers in the range of $1 \rightarrow 9$ are divisible by 2?
(2k = multiple of 2)
$\Rightarrow \quad 2k \leq 21 \quad \Rightarrow \quad k \leq 10$
$\therefore$ k = 2, 4, 6, 8, 10, 12, 14, 16, 18, 20

In general, $kd \leq$ n $\quad \Rightarrow \quad$ k $\leq \lfloor \frac{n}{d} \rfloor$

Answer: $\therefore$ There are $\lfloor \frac{n}{d} \rfloor$ positive integers not exceeding n that are divisible by d.

THM 4.1.1 |
Let $a, b, c \in \mathbb{Z}$ and $c \neq 0$.

(i) If $a \mid b$ and $a \mid c$, then $a \mid (b + c)$.

(ii) If $a \mid b$, then $a \mid bc \; \forall c \in \mathbb{Z}$.

(iii) If $a \mid b$ and $b \mid c$, then $a \mid c$.

PROOF:

THM 4.1.2 | Division Algorithm

Let $a \in \mathbb{Z}, d \in \mathbb{Z}^+$. Then, $\exists!\; q, r \in \mathbb{Z}$ satisfying $0 \leq r < d$ such that,

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

DEF | mod
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) $101 \mod 11 = 2$

(b) $101 \mod 2 = 11$

(c) $11 \mod 2 = 101$

(d) $101 \mod 2 = 1$

Example 4. What are the quotient and remainder when -11 is divided by 3?

DEF | div
If $a = d \cdot q + r$, then we write

$$q = a \text{ div } d$$

to express that q is the quotient of $a \div d$.

Example 5. Evaluate each of the following:

(a) $101 \text{ div } 11 =$

(b) $-11 \text{ div } 3 =$

Modular Arithmetic

DEF | Congruent to b modulo m

We say a is congruent to b modulo m, denoted,

$$a \equiv b \pmod{m}$$

if $\exists k \in \mathbb{Z}$ such that $a - b = m \cdot k$, i.e. $m \mid a - b$.

Example 6. Determine which of the following are true:

(a) $7 \equiv 3 \pmod{4}$

(b) $7 \equiv 4 \pmod{3}$

(c) $15 \equiv 3 \pmod{5}$

(d) $15 \equiv 5 \pmod{2}$

THM 4.1.3 |

Let $a, b \in \mathbb{Z}, m \in \mathbb{Z}^+$. Then,

$$a \equiv b \pmod{m}$$

if and only if

$$a \bmod m = b \bmod m$$

PROOF:

THM 4.1.4 |

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

(i) $a + c \equiv b + d \pmod{m}$

(ii) $ac \equiv bd \pmod{m}$

PROOF:

COROLLARY 4.1.4 |

Let $m \in \mathbb{Z}^+$.

(i) $(a + b) \mod m = [(a \mod m) + (b \mod m)] \mod m$

(ii) $(ab) \mod m = [(a \mod m) \cdot (b \mod m)] \mod m$

PROOF: TFYOG Example 7. Find each of the following without the aid of a

calculator.

(a) $(3^4 \mod 17)^2 \mod 11$

(b) $(99^2 \mod 32)^3 \mod 15$

DEF | Integers modulo m, $\mathbb{Z}_m$

The integers modulo m, denoted $\mathbb{Z}_m$, are defined as

$$\mathbb{Z}_m = \{0, 1, 2, 3, \ldots, m-1\}$$

Operations on $\mathbb{Z}_m$:

$a +_m b = (a + b) \mod m$

$a \cdot_m b = (ab) \mod m$

Example 8. Find the following:

(a) $7 +_{11} 9 =$

(b) $7 \cdot_{11} 9 =$