§ 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 exists a unique"

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 $b \div a \in \mathbb{Z}$

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) $3 \nmid 5$
$5 = 3 \cdot k \quad \Rightarrow \quad k = \frac{5}{3} \notin \mathbb{Z}$
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 $1 \to 9$ 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:

(i) $a + b$ by definition, $b = a \cdot k$ where $k \in \mathbb{Z}$. Similarly a | c, then $c = a \cdot q$ where $q \in \mathbb{Z}$.

Hence, $b + c = a \cdot k + a \cdot q$

$\Rightarrow b + c = a(k + q)$ where $(k + q) \in \mathbb{Z}$

$\Rightarrow a|(b + c)$ ✓

Consider $3|9$, $3|12$, then $3|(9 + 12) \Rightarrow 3|21$

$12 + 9 = 3 \cdot 3 + 3 \cdot 4 = 3(3 + 4) = 3 \cdot 7$

Answer: $3 \cdot 7$

(ii) If $a|b$, then by definition $b = a \cdot k$, where $k \in \mathbb{Z}$

GOAL: $b \cdot c = a \cdot integer$

From definition, $b \cdot c = a \cdot k \cdot c \Rightarrow b \cdot c = a \cdot u$ where $u = k \cdot c \in \mathbb{Z}$

$\Rightarrow a|b \cdot c$

(iii) By assumption

$b = a \cdot k$ where $k \in \mathbb{Z}$

$c = b \cdot q$ where $q \in \mathbb{Z}$

$\Rightarrow c = a \cdot u$ where $u = k \cdot q \in \mathbb{Z} \Rightarrow a|c$

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,

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

i.e. Any integer divided by positive integer d will result in quotient q and remainder r.

PROOF:

Case 1: $d|a$ if $d|a$ then $\exists q \in \mathbb{Z}$ such that:

$a = d \cdot q \Rightarrow ad = d \cdot q + 0$

$\Rightarrow a = d \cdot q + r$ where $r = 0$ ✓

Case 2: $d \nmid a$

If $d \nmid a$, then mod can subtract an integer in the range $(0, d)$ such that the result is divisible by d. (i.e. d = 4, a = 10)

**Note we are making the assumption that $d < a$.

Let such a number be r. Then:

$d|a - r \Rightarrow a - r = d \cdot q$, where $q \in \mathbb{Z}$

$\Rightarrow n = d \cdot q + r$ ✓

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.

i.e. $a \mod d$ is the remainder of $a \div d$

Example 3. Which of the following are true?

(a) $101 \mod 11 = 2$

$101 = 11 \cdot 9 + 2$

Answer: True

(b) $101 \mod 2 = 11$

$101 = 2 \cdot 50 + 1$

Answer: False

(c) $11 \mod 2 = 101$

$11 = 2 \cdot 5 + 1$

Answer: False

(d) $101 \mod 2 = 1$

$101 = 2 \cdot 50 + 1$

Answer: True

Example 4. What are the quotient and remainder when -11 is divided by 3?
$-11 = 3(-4) + 1$ where $3(-4) = q$ and $1 = r$
Answer: q = quotient = -4; r = remainder = 1

DEF | div

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

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

to express that q is the quotient of $a \div d$.
i.e. if a div d, it returns the quotient of $a \div d$.

Example 5. Evaluate each of the following:

(a) 101 div 11 =
$101 = 9 \cdot 11 + 2$
Answer: 9

(b) -11 div 3 =
$-11 = 3(-4) + 1$
Answer: -4

Modular Arithmetic

DEF | Congruent to b modulo m

if $m|a - b$ where $a, b, m \in \mathbb{Z}$ 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) $7 \equiv 3 \pmod 4$
$4|(7 - 3) = 4|4$
Answer: True

(b) $7 \equiv 4 \pmod 3$
$3|(7 - 4) = 3|3$
Answer: True

(c) $15 \equiv 3 \pmod 5$
$5|(15 - 3) = 5|12$
Answer: False

(d) $15 \equiv 5 \pmod 2$
$2|(15 - 5) = 2|10$
Answer: True

THM 4.1.3 |

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

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

if and only if

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

i.e. if dividing a by m produces the same remainder as dividing b by m, then a will be congruent to b modulo m and vice versa because it's (if and only if) bi-conditional.

PROOF:

($\rightarrow$) Assume that $a \equiv b(\mod m)$. By the division algorithm, dividing a by m will result in $a = m \cdot q + r$ where $q, r \in \mathbb{Z}$. Similarly, dividing b by m will result in $b = m \cdot k + s$ where $k, s \in \mathbb{Z}$.

Hence, $a - b = (m \cdot q + r) - (m \cdot k + s) = (m \cdot q - m \cdot k) + (r - s)$

(*) $a - b = m(q - k) + (r - s)$

Since $a \equiv b(\mod m)$, m divides $a - b$, so the remainder portion of (*) must be 0.

i.e. $r - s = 0 \Rightarrow r = s$

$\Rightarrow a \mod m = b \mod m$

($\leftarrow$) Now suppose $a \mod m \equiv b \mod m$.

By the division algorithm:

$a = m \cdot q + 3$, $b = m \cdot k + r$ (notice remainder are the same the same by assumption)

$\Rightarrow a - b = (m \cdot q + r) - (m \cdot k + r)$

$\Rightarrow m \cdot q - m \cdot k + r - r$

$\Rightarrow a - b = m \cdot q - m \cdot k = m(q - k)$

$\Rightarrow a - b = m \cdot u$ where $u = q - k \in \mathbb{Z}$

$\Rightarrow a \equiv b(\mod m)$

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:

$a \equiv b(\mod m)$ and $c \equiv d(\mod m)$
$a \equiv b(\mod m) \Rightarrow m|(a - b)$
$c \equiv d(\mod m) \Rightarrow m|(c - d)$
$\Rightarrow m|((a - b) + (c - d))$
$\Rightarrow m|(a - b + c - d)$
$\Rightarrow m|((a + c) + (-b - d))$
$\Rightarrow m|((a + c) - (b + d))$
$\Rightarrow a + c \equiv b + d(\mod m)$ ✓

i.e. Given $15 \equiv 5(\mod 2)$ is true and $7 \equiv 5(\mod 3)$ is true,
$\Rightarrow 15 + 7 \equiv 5 + 5(\mod 2) \Rightarrow 22 \equiv 10(\mod 2)$
$\Rightarrow 15 \cdot 7 \equiv 5 \cdot 5(\mod 2)$
$\Rightarrow 105 \equiv 25(\mod 2)$ ✓

COROLLARY 4.1.4 |

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

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

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

i.e. $33 + 5 \mod 2$
w/o: $33 + 5 \mod 2 = 32 mod 2 = 0$
w/: $[(33 \mod 2) + (5 \mod 2)] \mod 2 = [1 + 1] \mod 2 = 2 \mod 2 = 0$

PROOF: TFYOG

Example 7. Find each of the following without the aid of a calculator.

(a) $(3^4 \mod 17)^2 \mod 11$
Let $B = 34 \mod 17$
Simplify $B = 3^4 \mod 17$
$B = 3^3 \cdot 3 \mod 17$
$= (3^3 \mod 17)(3 \mod 17) \mod 17$
$= 10 \cdot 3 \mod 17$
$= 30 \mod 17$
$\Rightarrow 30 = 1 \cdot 17 + 13$
$\therefore B = 13$
Goal: $B^2 \mod 11$
$= 13^2 \mod 11$
$= (13 \mod 11)(13 \mod 11) \mod 11$
$= 2 \cdot 2 \mod 11$
$= 4 \mod 11 = 4$
Answer: 4

(b) $(99^2 \mod 32)^3 \mod 15$
Let $B = 99^2 \mod 32$
Simplify B
$B = (99 \mod 32)(99 \mod 32) \mod 32$
$= 3 \mod 32$
$\therefore B = 3$
$Goal: B^3 \mod 15$
$= 3^3 \mod 15$
$= 27 \mod 15$
Answer: 12

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) $7 +_{11} 9 =$
$= 7 + 9 \mod 11$
$= 16 \mod 11$
Answer: 5

(b) $7 \cdot_{11} 9 =$
$= 7 \cdot 9 \mod 11$
$= 63 \mod 11$
Answer: 8