Reading Summary 2.1-2.2

Evan Hughes

January 2023

2.1 Congruence and Congruence Classes

Definition: Let a, b, n be integers with $n > 0$. Then a is congruent to b modulo n. Written as $a \equiv b \pmod{n}$ if and only if $a - b$ is a multiple of n.

Example

: (from the book) $17 \equiv 5 \pmod{6}$ because 6 divides $17 - 5 = 12$. Also, $4 \equiv 25 \pmod{7}$ because 7 divides $4 - 25 = -21$.

reflexive: $a = a$ for all integers a.
symmetric: if $a = b$, then $b = a$.
transitive: if $a = b$ and $b = c$, then $a = c$.
Using these properties, we can prove that $a \equiv b \pmod{n}$ is reflexive, symmetric, and transitive.

Theorem 2.1

Let n be a postive integer. For all $a, b, c \in \mathbb{Z}$,

1. $a \equiv a \pmod{n}$;
2. if $a \equiv b \pmod{n}$, then $b \equiv a \pmod{n}$;
3. if $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$, then $a \equiv c \pmod{n}$.

Theorem 2.2

If $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$, then

1. $a + c \equiv b + d \pmod{n}$.
2. $ac \equiv bd \pmod{n}$.

Definition: Let a and n be integers with $n > 0$. The congruence class of a modulo n, $[a]$ is the set of all those integers that are congruent to a modulo n.

$$[a] = \{b \mid b \in \mathbb{Z} \text{ and } b \equiv a \pmod{n}\}$$

Example:

In congruence modulo 2:

$$[1] = \{\pm 1, \pm 3, \pm 5, \cdots\}$$

Theorem 2.3

$a \equiv c \pmod{n}$ if and only if $[a] = [c]$.

Corollary 2.4

Two congruence classes modulo n are either disjoint or identical.

Corollary 2.5

Let $n > 1$ be an integer and consider congruence modulo n.

1. If a is any integer and r is the remainder when a is divided by n, then $[a] = [r]$.
2. IThere are exactly n distinct congruence classes, $[0], [1], \cdots, [n-1]$.

Definition: The set of all congruence classes modulo n is denotes $\mathbb{Z}_n$.

2.2 Modular Arithmetic

The sum of the classes $[a]$ and $[b]$ is the class $[a+b]$. The product of the classes $[a]$ and $[b]$ is the class $[ab]$.

Theorem 2.6

If $[a] = [b]$ and $[c] = [d]$ in $\mathbb{Z}_n$, then $[a + c] = [b + d]$ and $[ac] = [bd]$.

$\oplus$	$[0]$	$[1]$
$[0]$	$[0]$	$[1]$
$[1]$	$[1]$	$[2]$