DEFINITION: A **congruence class** modulo K is a set of the form

$$[a] := \{n \in \mathbb{Z} \mid n \equiv a \pmod{K}\}$$

for some $a \in \mathbb{Z}$. We might also write $[a]_K$ to make clear what K is. A **representative** for a congruence class is an element of the congruence class.

PROPOSITION: Given $K > 0$, the set of integers $\mathbb{Z}$ is the disjoint union of K congruence classes:

$$\mathbb{Z} = [0] \sqcup [1] \sqcup \cdots \sqcup [K-1]. \qquad \square$$

The ring $\mathbb{Z}_K$ is the set of congruence classes modulo K:

$$\{[0], [1], \ldots, [K-1]\}$$

equipped with the operations

$$[a] + [b] = [a+b] \quad \text{and} \quad [a][b] = [ab].$$

(1) Warmup with congruence classes:
   (a) Find three distinct representatives of the congruence class $[13]$ in $\mathbb{Z}_5$.
   (b) Write a formula for all of the elements in the congruence class $[13]_5$.
   (c) Find the smallest nonnegative representative of the congruence class $[228]_{13}$.
   (d) True or false: $[5]_4$ is an element of $\mathbb{Z}_4$.
   (e) Fill in the blank: $a \equiv b \pmod{n}$ if and only if ________________ in $\mathbb{Z}_n$.

(2) Fill out the following $+$ and $\times$ table for $\mathbb{Z}_4$. Write all of your entries in the form $[0], [1], [2]$, or $[3]$:

$+$	$[0]$	$[1]$	$[2]$	$[3]$
$[0]$				
$[1]$				
$[2]$				
$[3]$				

$\times$	$[0]$	$[1]$	$[2]$	$[3]$
$[0]$				
$[1]$				
$[2]$				
$[3]$				

Explain the entry in the $[3]$ row and $[2]$ column of each table as a statement about integers and congruence modulo 4 (instead of about elements of $\mathbb{Z}_4$).

(3) Translating between congruence equations in $\mathbb{Z}$ and literal equations in $\mathbb{Z}_K$: Consider the equation

$$(\dagger) \qquad x^2 + 3x \equiv 6 \pmod{n}.$$

   (a) Since we can add and multiply elements of $\mathbb{Z}_n$, the equation

$$(\ddagger) \qquad y^2 + [3]y = [6]$$

   makes sense in $\mathbb{Z}_n$. Show that $x = a$ is a solution of (†) if and only if $y = [a]$ is a solution of (‡). Conclude that the set of solutions to (†) is the union of the congruence classes

$$\{[a] \mid y = [a] \text{ is a solution of } (\ddagger)\}.$$

   (b) What was special about the equation (†)? Formulate a general principle.

DEFINITION: We say that a number a is a **unit modulo** K if there is an integer solution x to $ax \equiv 1 \pmod{K}$, and we say that such a number x is an **inverse modulo** K to a.

We say that a congruence class $[a]$ is a **unit in** $\mathbb{Z}_K$ if there is a congruence class $x \in \mathbb{Z}_K$ such that $[a]x = [1]$, and we say that such a class x is an **inverse** to $[a]$ in $\mathbb{Z}_K$.

(4) Warmup with units and inverses:
  (a) Check that 4 is an inverse for 16 modulo 21. Find two more inverses for 16 modulo 21.
  (b) Explain the following: b is an inverse for a modulo K if and only if $[b]$ is an inverse for $[a]$ in $\mathbb{Z}_K$.
  (c) Explain the following: a is a unit modulo K if and only if $[a]$ is a unit in $\mathbb{Z}_K$.
  (d) Show that if x has an inverse in $\mathbb{Z}_K$ then this inverse is unique.

THEOREM: Let a and n be integers, with n positive. Then a is a unit modulo n if and only if a and n are coprime.

(5) Proof of the Theorem / how to find inverses.
  (a) Use the definition of congruent modulo n to rewrite the statement $ax \equiv 1 \pmod{n}$ as a statement just about integers.
  (b) Prove the Theorem above.
  (c) Find an inverse for 24 modulo 149.

THEOREM (THE CHINESE REMAINDER THEOREM): Given $m_1, \dots, m_k > 0$ integers such that m_i and m_j are coprime for each $i \neq j$, and $a_1, \dots, a_k \in \mathbb{Z}$, the system of congruences

$$\begin{cases} x \equiv a_1 & \pmod{m_1} \\ x \equiv a_2 & \pmod{m_2} \\ \quad \vdots & \quad \vdots \\ x \equiv a_k & \pmod{m_k} \end{cases}$$

has a solution $x \in \mathbb{Z}$. Moreover, the set of solutions forms a unique congruence class modulo $m_1 m_2 \cdots m_k$.

(6) Proof of CRT:
  (a) Set $m_i' = m_1 \cdots m_{i-1} m_{i+1} \cdots m_k$ to be the product of all of the m's except the i-th. Explain why m_i and m_i' are coprime.
  (b) Let m_i^* be an inverse of m_i' modulo m_i. (Why does one exist?) Show that

$$m_i' m_i^* \equiv 1 \pmod{m_i} \quad \text{and} \quad m_i' m_i^* \equiv 0 \pmod{m_j} \ \text{ for } j \neq i.$$

  (c) Find a solution in terms of $a_1, \dots, a_k$ and $m_1' m_1^*, \dots, m_k' m_k^*$.
  (d) Show that if $x' \equiv x \pmod{m_1 m_2 \cdots m_k}$, then x' is a solution as well.
  (e) Show[1] that if x' is another solution, then $x' \equiv x \pmod{m_1 m_2 \cdots m_k}$.

[1] The following LEMMA may be useful: if a and b are coprime, and a and b both divide c, then ab divides c.

(7) Solve the following systems:

(a)

$$\begin{cases} x &\equiv 4 \pmod{11} \\ x &\equiv 3 \pmod{17} \end{cases}$$

(b) Find[2] a number that leaves remainder 1 when divided by 3, a remainder of 2 when divided by 5, and a remainder of 3 when divided by 7.

(c)

$$\begin{cases} x \equiv 4 \pmod{6} \\ x \equiv 13 \pmod{15} \end{cases}$$

---

(8) Let a, b, n be integers, with $n > 0$.

(a) When does the equation $[a]x = [b]$ have a solution in $\mathbb{Z}_n$? Give an answer in terms of properties of the integers a, b, and n that we have discussed in class.

(b) How many solutions does the equation $[a]x = [b]$ have a solution in $\mathbb{Z}_n$? Give an answer in terms of properties of the integers a, b, and n that we have discussed in class.

Key Points:

- Definition of congruence classes and $\mathbb{Z}_n$.
- Relationship between solving congruences and solving equations in $\mathbb{Z}_n$.
- A number is a unit modulo n if and only if a and n are coprime.
- How to find inverses modulo n.
- Using CRT to solve multiple congruences.

[2] Real problem from Master Sun's Mathematical Manual (fourth century AD)!