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 $\mathbb{Z}_n$.

   (a) $13, 18, 23$ (answers may vary).
   (b) $13 + 5n$ for $n \in \mathbb{Z}$.
   (c) 7, by long division.
   (d) True! We just often prefer to call it $[1]$ instead.
   (e) $[a] = [b]$.

(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 $\mathbb{Z}_4$).

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

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

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

$$x^2 + 3x \equiv 6 \pmod{n}. \tag{†}$$

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

$$y^2 + [3]y = [6] \tag{‡}$$

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

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

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

(a) Suppose that $x = a$ is a solution of (†). Then $[a]^2 + 3[a] = [a^2 + 3a] = [6]$ in $\mathbb{Z}_n$, since $a^2 + 3a \equiv 6 \pmod{n}$, so $y = [a]$ is a solution of (‡). Suppose that $y = [a]$ is a solution of (‡). Then $[a^2 + 3a] = [a]^2 + 3[a] = [6]$ in $\mathbb{Z}_n$, so $a^2 + 3a \equiv 6 \pmod{n}$. Thus, a is a solution of (†).
(b) This worked because everything was make out of $+$ and $\times$. If we have any polynomial congruence equation modulo n, then it corresponds to an actual equation in $\mathbb{Z}_n$, and the solution set over $\mathbb{Z}$ is the union of congruence classes corresponding to the solutions in $\mathbb{Z}_n$.

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.

(a) $4 \cdot 16 = 64 \equiv 1 \pmod{21}$, since $21|63$. Also $25, 46$. (Answers may vary.)
(b) As above $ab \equiv 1 \pmod{K}$ if and only if $[a][b] = [1]$ in $\mathbb{Z}_K$.
(c) a is a unit in $\mathbb{Z}_K$ if and only if there is a $b \in \mathbb{Z}$ that is an inverse mod K, if and only if there is a b such that $[b]$ is an inverse to $[a]$ in $\mathbb{Z}_K$, if and only if $[a]$ is a unit in $\mathbb{Z}_K$.
(d) If $[a][b] = [1] = [a][b']$, then $[b] = [b][a][b] = [b][a][b'] = [b']$.

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.

(a) $ax - 1 = bn$ for some b, so $ax - bn = 1$.
(b) We saw last time that this equation has a solution if and only if 1 is a multiple of $\gcd(a, b)$, i.e., a and b are coprime.
(c) We apply the Euclidean algorithm as last time.

$$149 = 6 \cdot 24 + 5$$
$$24 = 4 \cdot 5 + 4$$
$$5 = 1 \cdot 4 + 1$$
$$5 = 1 \cdot 149 - 6 \cdot 24$$
$$4 = 1 \cdot 24 - 4 \cdot 5 = 1 \cdot 24 - 4 \cdot (1 \cdot 149 - 6 \cdot 24) = -4 \cdot 149 + 25 \cdot 24$$
$$1 = 1 \cdot 5 - 1 \cdot 4 = (1 \cdot 149 - 6 \cdot 24) - (-4 \cdot 149 + 25 \cdot 24) = 5 \cdot 149 - 31 \cdot 24.$$

So -31 is 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 $x' \equiv x \pmod{m_1 m_2 \cdots m_k}$.

(a) If p is a common prime factor of m_i and m_i', then p must be a prime factor of one of the m_j with $j \neq i$, since m_i' is the product of these. But this would contradict that m_i and m_j are coprime.
(b) We know that m_i' has an inverse modulo m_i since these are coprime. Then $m_i' m_i^* \equiv 1 \pmod{m_i}$ by definition of inverse, and $m_i' m_i^* \equiv 0 \pmod{m_j}$ since m_j divides m_i'.
(c) Take $x = a_1 m_1' m_1^* + \cdots + a_k m_k' m_k^*$. Taken modulo m_i, this every term but the i-th is zero, and the i-th is congruent to $a_i \cdot 1 = a_i$, so $x \equiv a_i \pmod{m_i}$ for each i.
(d) We can write $x' = x + d m_1 m_2 \cdots m_k$. Then $x' \equiv a_i + d m_1 m_2 \cdots m_k \equiv a_i \pmod{m_i}$ for each i.
(e) Since $x' \equiv a_i \equiv x \pmod{m_i}$, then $m_i \mid (x' - x)$ for each i, and all m_i are coprime, the product divides $x' - x$. This means $x' \equiv x \pmod{m_1 m_2 \cdots m_k}$.

[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)

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

(1) We find 2 is an inverse of 17 modulo 11 and 14 is an inverse of 11 modulo 17. So

$$x = 4 \cdot 2 \cdot 17 + 3 \cdot 14 \cdot 11 = 598$$

is a solution, and $598 + 187n$ is the general solution.

(2) We start by finding inverses of 35 modulo 3, 21 modulo 5, and 15 modulo 7; the numbers 2, 1, and 1 work, respectively. Then

$$x = 1 \cdot 2 \cdot 35 + 2 \cdot 1 \cdot 21 + 3 \cdot 1 \cdot 15 = 157$$

works. Since $3 \cdot 5 \cdot 7 = 105$, every solution is of the form $157 + 105n$. The smallest positive solution is 52.

(3) We cannot apply the theorem yet! Let's start by breaking the congruences down. Since $4 \equiv 1 \pmod{3}$ and $4 \equiv 0 \pmod{2}$, we can rewrite the first equation as $x \equiv 0 \pmod{2}$ and $x \equiv 1 \pmod{3}$. Likewise, we can break the second down by writing $13 \equiv 3 \pmod{5}$ and $13 \equiv 1 \pmod{3}$, so $x \equiv 3 \pmod{5}$ and $x \equiv 1 \pmod{3}$. Thus, we can get the system

$$\begin{cases} x \equiv 0 \pmod{2} \\ x \equiv 1 \pmod{3} \\ x \equiv 3 \pmod{5}. \end{cases}$$

Now we can apply the CRT to solve. I got $28 + 30n$.

---

(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)!