Modular arithmetic and Equivalence Relations

CSC 1300 – Discrete Structures
Villanova University
If $a$ and $b$ are two integers and $m$ is a positive integer, then $a$ is congruent to $b$ modulo $m$, denoted $a \equiv b \pmod{m}$, if $a$ and $b$ have the same remainder when divided by $m$.

Examples:
$15 \equiv 7 \pmod{2}$
$14 \equiv 2 \pmod{12}$
$15 \equiv 95 \pmod{10}$
$-6 \equiv 24 \pmod{2}$
$8 \equiv -4 \pmod{12}$
Equivalent formulations of congruence modulo $m$

- **$a$ is congruent to $b$ modulo $m$**
- $a ≡ b \pmod{m}$
- $a$ and $b$ have the same remainder when divided by $m$
- $a − b$ is divisible by $m$
- $m$ divides $a − b$ \ (denoted $m | (a − b)$ )
- $a − b = km$ for some $k ∈ \mathbb{Z}$
Equivalence Relations

\[ a \equiv b \pmod{m} \] is an **equivalence relation**.

A relation on a set \( A \) is called an *equivalence relation* if it is
(i) reflexive,
(ii) symmetric,
(iii) transitive.

Formalizes the notion of “equivalence” or “sameness”.

Examples of equivalence relations:
- “to be equal” (for numbers or sets)
- “to have the same age”
- “to have the same remainder after division by 2” (i.e., parity)
- “to have the same first 3 bits” (for bit strings)
Let $R$ be an equivalence relation on a set $X$, and let $a$ be an element of $X$. The set of all elements of $X$ that are related to $a$ by $R$ is called the *equivalence class* for $a$ and is denoted by $[a]$. Any element $b \in [a]$, $b$ is called a *representative* of $[a]$.

**Example:** Consider the relation “… is congruent to … modulo 2” on the set $\mathbb{Z}$. What is $[4]$?

**Example:** Let $X$ be the set of all bit strings of length at least 3, and $R$ be the relation “agree in the first three bits”. Find

- $[001]$
- $[1101101]$
- $[0011]$
**Theorem.** Let $R$ be an equivalence relation on a set $X$. Then the equivalence classes of $R$ form a partition of $X$.

A *partition* of a set $X$ is a collection of disjoint nonempty subsets of $X$ that have $X$ as their union.

The collection $X_1, X_2, X_3, X_4$ is a partition of $X$. 

Villanova CSC 1300 - Dr Papalaskari
Partitions

What is the partition of $\mathbb{Z}$ formed by the relation “... is congruent to ... modulo 4”?
Useful facts about congruences

The following hold for \( n \geq 1 \):

• \( a \equiv a \pmod{n} \)

• \( a \equiv b \pmod{n} \) \( \Rightarrow \) \( b \equiv a \pmod{n} \)

• \((a \equiv b \pmod{n} \text{ } \& \text{ } b \equiv c \pmod{n})\) \( \Rightarrow \) \( a \equiv c \pmod{n} \)

• \( a \equiv b \pmod{n} \) \( \Rightarrow \) \( a + c \equiv b + c \pmod{n} \)

• \( a \equiv b \pmod{n} \) \( \Rightarrow \) \( ac \equiv bc \pmod{n} \)

• \((a \equiv b \pmod{n} \text{ } \& \text{ } c \equiv d \pmod{n})\) \( \Rightarrow \) \( a + b \equiv c + d \pmod{n} \)

• \((a \equiv b \pmod{n} \text{ } \& \text{ } c \equiv d \pmod{n})\) \( \Rightarrow \) \( ab \equiv cd \pmod{n} \)