An equivalence relation R on a set A partitions the set into *equivalence classes*.

An equivalence class is a subset of A so that every pair of elements from the class is in the relation, while any pair of an element in the class and an element outside the class is not in the relation.

Every element in A is in exactly one of the equivalence classes.

Notation: $[x]$ denotes the equivalence class of which x is a member. Note that $[x] = [y]$ if and only if xRy.

Examples:

Let R be the relation on the set $A = \{1, \ldots, 16\}$ where xRy if $\lceil \log_2(x) \rceil = \lceil \log_2(y) \rceil$.

Equivalence classes:

$[1] = \{1\}$
$[2] = \{2\}$
$[4] = \{3, 4\}$
$[8] = \{5, 6, 7, 8\}$
$[16] = \{9, 10, 11, 12, 13, 14, 15, 16\}$

Let R be the relation on the set $\{0, 1, \ldots, 20\}$ where xRy if x and y, divided by 5, have the same remainder.

Equivalence classes:

$[0] = \{0, 5, 10, 15, 20\}$
$[1] = \{1, 6, 11, 16\}$
$[2] = \{2, 7, 12, 17\}$
$[3] = \{3, , 8, 13, 18\}$
$[4] = \{4, 9, 14, 19\}$.

The Integers Modulo n

For each positive integer n, the following is an equivalence relation on $\mathbb{Z}$: xRy if x and y, divided by n, have the same remainder.

Alternative definitions:

xRy **if** $x - y$ **is divisible by** n**.** $(n|(x-y))$

xRy **if** $\exists_k x = y + kn$**.**

This relation R is called: Congruence modulo n.

Notation: $x \equiv y \bmod n$**.**

Modular Arithmetic

$\mathbb{Z}_n$ is the set of *integers modulo* n**:**

$$\mathbb{Z}_n = \{[0], [1], \ldots, [n-1]\},$$

where $[0]$, $[1]$ etc. are the equivalence classes of the relation "congruence modulo n". So $[0] = \{x \mid \exists_k x = kn\}$, $[1] = \{x \mid \exists_k x = kn + 1\}$ etc.

Addition and multiplication on $\mathbb{Z}_n$ are defined as follows:

$[x] + [y] = [x + y]$
$[x][y] = [xy]$