Equivalence Relation

Recall congruence

$$a \equiv b \pmod{n} \iff n \mid a-b$$

Why is congruence an <u>equivalence relation</u>?

Some numbers in $\mathbb{N}$ become "equivalent" modulo n.

Example : $n=7$

$$\left.\begin{array}{l}
\{\ldots, -14, -7, 0, 7, 14, \ldots\} \\
\{\ldots, -13, -6, 1, 8, 15, \ldots\} \\
\{\ldots, -12, -5, 2, 9, 16, \ldots\} \\
\quad\vdots \\
\{\ldots, -8, -1, 6, 13, 20, \ldots\}
\end{array}\right\} \text{7 classes of equivalence}$$

Given a set S, Consider $S \times S$

A relation R is a subset of $S \times S$

$$a R b \iff (a,b) \in R$$

An equivalence relation R (denoted by $\equiv$) satisfies

1. Reflexive. $\forall a \in S, \quad a \equiv a$ $\qquad (a,a) \in R$
2. Symmetric. $\forall a, b \in S, \quad a \equiv b \iff b \equiv a$ $\qquad (a,b) \in R \iff (b,a) \in R$
3. Transitive. $\forall a, b, c \in S, \ (a \equiv b \wedge b \equiv c) \Rightarrow a \equiv c$

'$=$' is an equivalence relation.

An equivalence relation on S partitions S into classes of equivalence

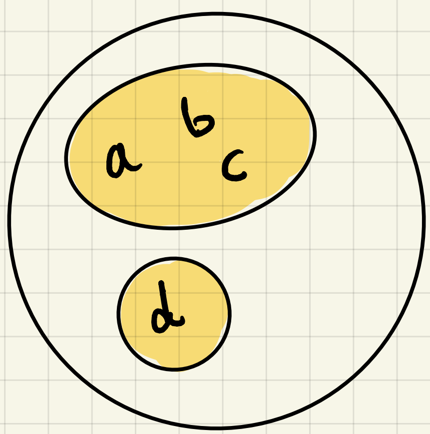
$$C_a = \{x \in S : a \equiv x\}$$

Example: $S = \{a, b, c, d\}$

$$R = \{(a,a), (b,b), (c,c), (d,d), (a,b), (b,c), (a,c), (b,a), (c,b), (c,a)\}$$

$C_a = \{a, b, c\}$ $\quad C_b = \{a, b, c\}$ $\quad C_c = \{a, b, c\}$ $\quad C_d = \{d\}$

S



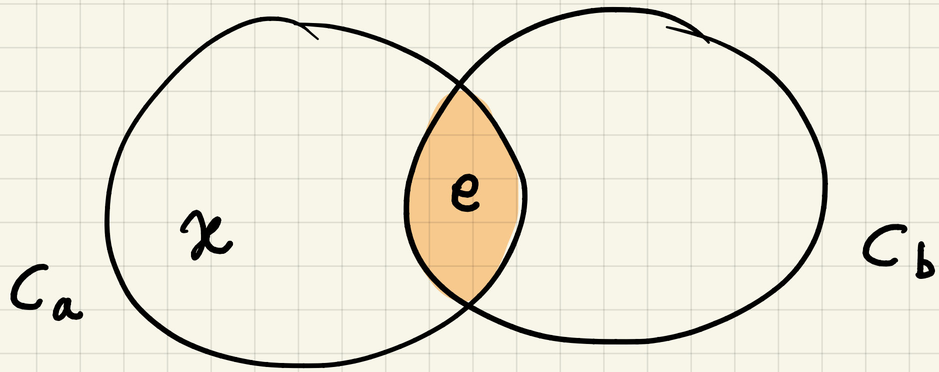
In general: 1) $\bigcup_{a \in S} C_a = S$

2) $C_a \cap C_b \neq \phi \Rightarrow C_a = C_b$

(either disjoint or the same)

1) By reflexivity: $\forall a \in S$, $a \in C_a$ because $a \equiv a$

Can't have



$e \in C_a \Rightarrow a \equiv e$

$e \in C_b \Rightarrow b \equiv e$

Proof: $x \in C_a \Rightarrow \begin{matrix} a \equiv x \\ a \equiv e \end{matrix} \Rightarrow x \equiv e$

symmetry & transitivity

$\begin{matrix} b \equiv e \\ x \equiv e \end{matrix} \Rightarrow b \equiv x \Rightarrow x \in C_b$. Therefore $C_a \subset C_b$

Similarly, we can show $C_b \subset C_a$. Therefore $C_a = C_b$