RELATION CONGRUENCE MODULO m
(Sec. 3.2)

Very important example of equivalence relation is arithmetic.

In the quiz: $R = \{(a,b) \in \mathbb{Z}^2 : 3 \mid (a-b)\}$

$\uparrow$
$m \in \mathbb{N}$

Given $m \in \mathbb{N}$, let us consider more in general

$R = \{(a,b) \in \mathbb{Z}^2 : m \mid (a-b)\}$: relation congruence modulo m

If $(a,b) \in R$, we say that a is congruent to b modulo m and we write $a \equiv b \pmod{m}$.

Def: Let $m \in \mathbb{N}$. For $a, b \in \mathbb{Z}$, we say that a is congruent to b modulo m and we write

$$a \equiv b \pmod{m}$$

if $m \mid (a-b)$.

The number m is called the modulo of the congruence.

Examples: $m = 3$.

- $(23, 17) \in R$, equivalently $23 \equiv 17 \pmod{3}$
  because $3 \mid (23-17) = 6$.
- $(17, 23) \in R$.
  Indeed in this case $17 - 23 = -6$ and $3 \mid -6$
  $(-6 = 3 \cdot (-2))$
- $(18, 17) \notin R$ because $3 \nmid (18-17) = 1$.
- $(17, 17) \in R$ because $3 \mid (17-17) = 0$
  $(0 = 3 \cdot 0)$

Recall $m \mid (a-b) \iff \exists\, k \in \mathbb{Z}$ s.t. $a - b = m \cdot k$.

Proposition: $\forall\, m \in \mathbb{N}$ the congruence modulo m is an equivalence relation.

Proof: We have to prove that it is reflexive, symmetric and transitive.

- Reflexive: $\forall\, a \in \mathbb{Z},\ (a,a) \in R\ (a \equiv a \pmod m)$

  because $m \mid (a-a) = 0\ \ (0 = m \cdot \underset{k}{0})$

- Symmetric: Let $a, b \in \mathbb{Z}$ s.t. $(a,b) \in R$ $(\Leftrightarrow\ a \equiv b \pmod m \Leftrightarrow m \mid (a-b))$,

  Then $\exists\, k \in \mathbb{Z}$ s.t. $a-b = m \cdot k$

  $\Rightarrow (-1)\cdot(a-b) = (-1)\, m \cdot k \Rightarrow$

  $\Rightarrow\ b-a = m \cdot (\underbrace{-k}_{\in \mathbb{Z}}) \Rightarrow m \mid (b-a)$

  $\Rightarrow (b,a) \in R.$

- transitive: Let $a, b, c \in \mathbb{Z}$ s.t. $(a,b) \in R$ and $(b,c) \in R \Rightarrow$

  $$\begin{cases} m \mid (a-b) \Leftrightarrow \exists\, k \in \mathbb{Z} \text{ s.t. } (a-b) = km \quad ① \\ m \mid (b-c) \Leftrightarrow \exists\, h \in \mathbb{Z} \text{ s.t. } (b-c) = hm \quad ② \end{cases}$$

  $$\Rightarrow a-c = \underbrace{a-b}_{} + \underbrace{b-c}_{} \overset{①}{\underset{②}{=}} \underbrace{km}_{} + \underbrace{hm}_{} =$$

  $$= m(\underbrace{k+h}_{\in \mathbb{Z}}) \Rightarrow m \mid (a-c)$$

  $\Rightarrow (a,c) \in R.$

So now let's describe the classes of equivalence:

$$\bar{0} = \{a \in \mathbb{Z} : (a,0) \in R\} = \{a \in \mathbb{Z} : \overbrace{a \equiv 0 \bmod m}^{m \mid (a-0)}\} =$$

$$= \{a \in \mathbb{Z} : \exists\, k \in \mathbb{Z} \text{ s.t. } a = m \cdot k\} = m\mathbb{Z}.$$

when $m = 3$: $\bar{0} = \{\ldots, -6, -3, 0, 3, 6, 9, \ldots\} = 3\mathbb{Z}.$

$$\overline{1} = \{a \in \mathbb{Z} : (a,1) \in R\} = \{a \in \mathbb{Z} : \underset{}{\overset{m \mid (a-1)}{a \equiv 1 \bmod m}}\} =$$

$$= \{a \in \mathbb{Z} : \exists\, k \in \mathbb{Z} \text{ s.t. } a-1 = m \cdot k\} =$$

$$= \{a \in \mathbb{Z} : \exists\, k \in \mathbb{Z} \text{ s.t. } a = \underline{m}\,k + \underline{1}\}$$

In the quiz you proved that if $a \in \overline{1} \iff \exists\, k \in \mathbb{Z}$ s.t. $a = 3k+1$.

$$\overline{2} = \{a \in \mathbb{Z} : \exists\, k \in \mathbb{Z} \text{ s.t. } a = mk + \underline{2}\}$$

$$\vdots$$

$$\overline{m-1} = \{a \in \mathbb{Z} : \exists\, k \in \mathbb{Z} \text{ s.t. } a = mk + \underline{(m-1)}\}$$

$$\overline{m} = \{a \in \mathbb{Z} : \exists\, k \in \mathbb{Z} \text{ s.t. } a = \underbrace{mk + m}_{m(k+1)}\} = m\mathbb{Z} = \overline{0}$$

clock arithmetic