I often say "equivalence" instead of congruence — or even "equals".

Congruences are an equivalence relation.

Eq. rels. have 3 properties:

Let $a, b, c, m \in \mathbb{Z}$. $(m \geq 2)$

1. Reflexivity

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

Compare with other relations: $\leq$ is reflexive
$a \leq a$ always, but $<$ is not.

2. Symmetry

if $a \equiv b \pmod{m}$, then $b \equiv a \pmod{m}$.

Compare with $\le$ and $<$.

3. Transitivity.

if $a \equiv b \pmod{m}$ and $b \equiv c \pmod{m}$, then $a \equiv c \pmod{m}$.

Both $\le$ and $<$ are transitive.

Why do congruences satisfy these?

1. $a \equiv a \pmod{m}$: $a - a = k \cdot m$ find $k \in \mathbb{Z}$. $\boxed{k = 0}$.

2. $a - b = k \cdot m$, we have some $k \in \mathbb{Z}$.

Want to write $\underline{b - a} = (-1) \cdot (a - b) = (-1)(km) = \underline{(-k)} m$

3. Assume $a-b=k\cdot m$, and $b-c=\ell\cdot m$ for some $k,\ell\in\mathbb{Z}$.

$$\begin{aligned} a-c &= a-b+b-c \\ &= k\cdot m+\ell\cdot m \\ &= (k+\ell)m. \end{aligned}$$

Since $k,\ell\in\mathbb{Z}$, so is their sum $k+\ell$. Hence

$$a\equiv c \pmod m.$$

Connection with remainders

Bring in the Remainder Theorem.

Claim: Integers a and b are congruent mod m if and only if they have the same remainder upon (multiple) divison(s) by m.

By Remainder Theorem,

$$a = q_1 \cdot m + r_1 \qquad b = q_2 \cdot m + r_2$$

where $0 \le r_1 < m$ and $0 \le r_2 < m$.

Assume that $a \equiv b \pmod{m}$. There is a $k \in \mathbb{Z}$

$$a - b = k \cdot m.$$

$$k \cdot m = a - b$$
$$= (q_1 m + r_1) - (q_2 m + r_2)$$
$$= (q_1 - q_2) m + (r_1 - r_2)$$

So we have
$$k \cdot m = (q_1 - q_2) m + (r_1 - r_2).$$

We know LHS is a multiple of m, so the RHS must also be a multiple of m. Since $m \mid (q_1 - q_2) m$ (recall: m divides $(q_1 - q_2) m$), we must have that $m \mid (r_1 - r_2)$. But $0 \leq r_1, r_2 < m$, so $r_1 - r_2 = 0$.

Try other direction!

Equivalence classes.

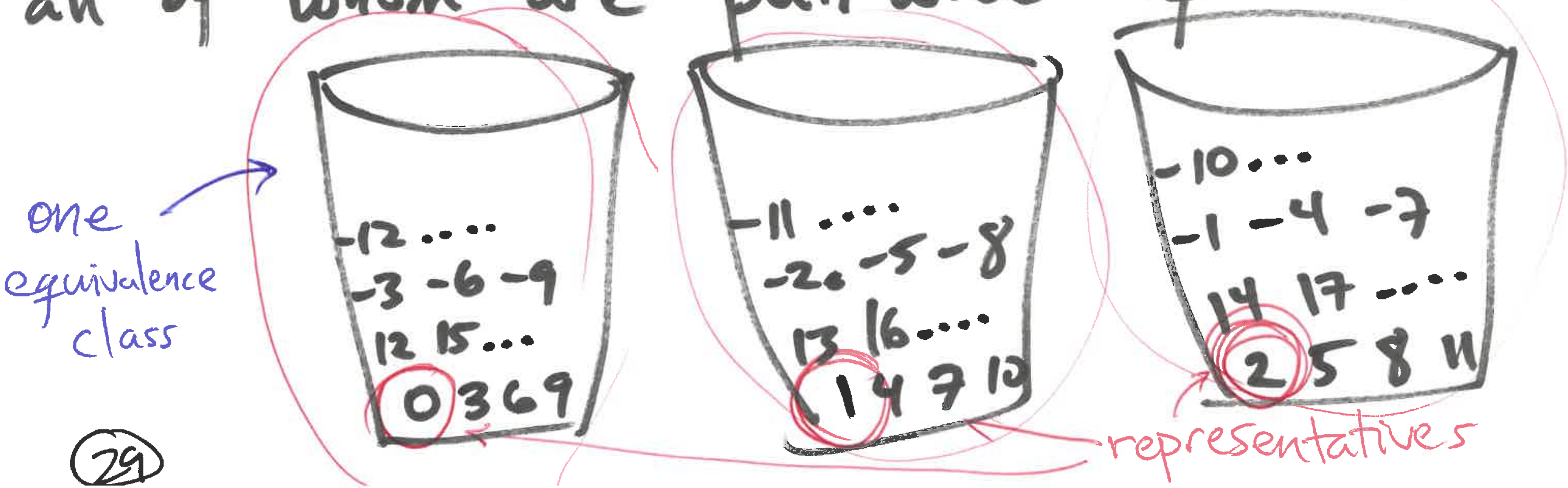
Congruence classes

Ex: $m = 3$: modulus is 3.

We have three possible remainders:

$$0 \qquad 1 \qquad 2$$

An <u>equivalence class</u> is a set of integers all of whom are pairwise equivalent.



This applies to general modulus m except the numbers change accordingly.

In general: we have m equivalence classes with representatives $\underbrace{0, 1, 2, \ldots, m-1}$.

$\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$.

$$\mathbb{Z}_m = \{0, 1, 2, \ldots, m-1\}.$$

Actually: we work with equivalence classes not just reps. but this good enough for us.