Theorem. Let $B_1, B_2, \ldots$ be a partition of A.
Then there exists an equivalence relation R on A whose equivalence classes are exactly $B_1, B_2, \ldots$

Pf. We define R by

(*) xRy if $\exists\ B_i$ with $x \in B_i$, $y \in B_i$.

[We showed this is an equivalence relation (symmetric, transitive, reflexive)]

We need also to show the B_i's are the equiv. classes.

Let C be an equiv. class.

Let $a \in C$. Then $a \in B_i$ for exactly one B_i (since $B_i \cap B_j = \emptyset$).

① Show that $[a] = B_i$.

$y \in [a] \iff yRa$

$\iff y, a \in B_j$ for some j

$\iff y, a \in B_i$ ($j = i$ because $a \in B_i, B_j$ and $B_i \cap B_j = \emptyset$)

$\iff y \in B_i$.

Therefore, having chosen a different $a' \in C$ gives the same B_i.

Therefore we have a well-defined function

$$g : \{[a] : a \in A\} \longrightarrow \{B_i\}$$

We check that this is a bijection.

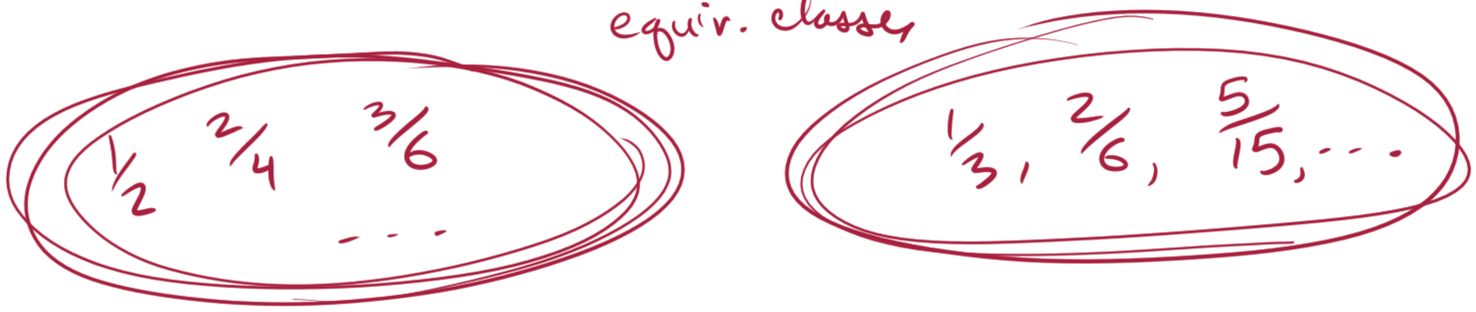
Injectivity: If $g([a]) = g([b])$ then $[a] = B_i = [b]$.

Surjectivity: For B_i, let $a \in B_i$.

Then $[a] = B_i$ and $g([a]) = B_i$.

Example. $\frac{1}{2} = \frac{3}{6}$ "=" on fractions

equiv. classes



$\mathbb{Z} \times \mathbb{Z}$

↓ equiv. relation

$\mathbb{Q}$

Define $\mathbb{Q}$ this way:

$\mathbb{Q}$ = the set of equivalence classes of pairs of integers (a,b) with $b \neq 0$

under the relation $(a,b) \sim (c,d)$ if $ad = bc$

Idea:

$\frac{a}{b} = \frac{c}{d}$

$\Leftrightarrow \quad ad = bc.$

Define $\mathbb{R}$.

Def^n We call a sequence a_n "Cauchy" if for every $\varepsilon > 0$, $\exists\ N \in \mathbb{N}$ s.t. $|a_n - a_m| < \varepsilon$ whenever $n, m > N$.

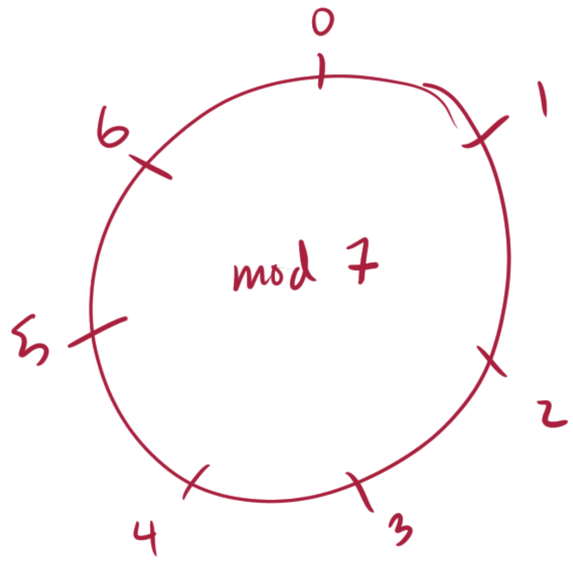
(Idea: these are sequences which "should" converge.)

Def^n We call two Cauchy sequences a_n and b_n equivalent if for every $\varepsilon > 0$, $\exists\ N \in \mathbb{N}$ s.t. $|a_n - b_n| < \varepsilon$ whenever $n > N$.

(Idea: such sequences go to same limit)

Def^n $\mathbb{R}$ is the set of equivalence classes of Cauchy sequences of rationals under equivalence.

Modular Arithmetic



$3+6 = 9 = 2$

$3 \cdot 6 = 18 = 4$

$\mathbb{Z}/7\mathbb{Z} = \{[0],[1],[2],[3],[4],[5],[6]\}$

Def^n. Let $n \in \mathbb{Z}$. Let $a, b \in \mathbb{Z}$.
Then $a \equiv b \pmod{n}$ if $n \mid a-b$.

Transitivity: Let $a,b,c,n \in \mathbb{Z}$. If $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$ then $a \equiv c \pmod{n}$.

Pf. Suppose $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$.
Then $n \mid a-b$ and $n \mid b-c$. So $n \mid (a-b)+(b-c) = a-c$. So $a \equiv c \pmod{n}$.

Q: Is this an equivalence relation? **YES**

Reflexivity:

Thm. Let $n, a \in \mathbb{Z}$.
Then $a \equiv a \pmod{n}$.

Pf. $n \mid 0$ so $n \mid a-a$.
So $a \equiv a \pmod{n}$. ∎

Symmetry: For $a,b,n \in \mathbb{Z}$, if $a \equiv b \pmod{n}$ then $b \equiv a \pmod{n}$.

Pf. Suppose $a \equiv b \pmod{n}$.
Then $n \mid a-b$.
So $n \mid b-a$.
So $b \equiv a \pmod{n}$.

Theorem. Let $a, b, c, d \in \mathbb{Z}$. Let $n \in \mathbb{Z}$.

If $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$.

Then $a+c \equiv b+d \pmod{n}$

and $ac \equiv bd \pmod{n}$.

The "well-defined"ness of addition and multiplication modulo n.

Ex. $\mathbb{Z}/7\mathbb{Z}$

$$[2] + [3] = [5]$$
$$\| \quad\quad \| \quad\quad \|$$
$$[9] + [3] = [12]$$

Mod 5.

Multipl.

	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1